IFIP AICT 328

Jacques Berleur
Magda David Hercheui
Lorenz M. Hilty
(Eds.)

What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience

9th IFIP TC 9 International Conference, HCC9 2010
and 1st IFIP TC 11 International Conference, CIP 2010
Held as Part of WCC 2010
Brisbane, Australia, September 2010
Proceedings

Springer

IFIP Advances in Information and Communication Technology 328

IFIP – The International Federation for Information Processing

IFIP was founded in 1960 under the auspices of UNESCO, following the First World Computer Congress held in Paris the previous year. An umbrella organization for societies working in information processing, IFIP's aim is two-fold: to support information processing within its member countries and to encourage technology transfer to developing nations. As its mission statement clearly states,

> *IFIP's mission is to be the leading, truly international, apolitical organization which encourages and assists in the development, exploitation and application of information technology for the benefit of all people.*

IFIP is a non-profitmaking organization, run almost solely by 2500 volunteers. It operates through a number of technical committees, which organize events and publications. IFIP's events range from an international congress to local seminars, but the most important are:

- The IFIP World Computer Congress, held every second year;
- Open conferences;
- Working conferences.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is small and by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is less rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

Any national society whose primary activity is in information may apply to become a full member of IFIP, although full membership is restricted to one society per country. Full members are entitled to vote at the annual General Assembly, National societies preferring a less committed involvement may apply for associate or corresponding membership. Associate members enjoy the same benefits as full members, but without voting rights. Corresponding members are not represented in IFIP bodies. Affiliated membership is open to non-national societies, and individual and honorary membership schemes are also offered.

Jacques Berleur Magda David Hercheui
Lorenz M. Hilty (Eds.)

What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience

9th IFIP TC 9 International Conference, HCC9 2010
and 1st IFIP TC 11 International Conference, CIP 2010
Held as Part of WCC 2010
Brisbane, Australia, September 20-23, 2010
Proceedings

Springer

Volume Editors

Jacques Berleur
University of Namur, Faculty of Informatics
61, rue de Bruxelles, 5000 Namur, Belgium
E-mail: jberleur@info.fundp.ac.be

Magda David Hercheui
Westminster Business School
35 Marylebone Road, London NW1 5LS, UK
E-mail: m.hercheui@westminster.ac.uk

Lorenz M. Hilty
University of Zurich, Department of Informatics
Binzmuehlestr. 14, 8050 Zurich, Switzerland
E-mail: hilty@ifi.uzh.ch

Library of Congress Control Number: 2010933097

CR Subject Classification (1998): C.2, K.6.5, D.4.6, E.3, H.4, J.1

ISSN 1868-4238
ISBN-10 3-642-15478-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-15478-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

IFIP World Computer Congress 2010 (WCC 2010)

Message from the Chairs

Every two years, the International Federation for Information Processing (IFIP) hosts a major event which showcases the scientific endeavors of its over one hundred technical committees and working groups. On the occasion of IFIP's 50th anniversary, 2010 saw the 21st IFIP World Computer Congress (WCC 2010) take place in Australia for the third time, at the Brisbane Convention and Exhibition Centre, Brisbane, Queensland, September 20–23, 2010.

The congress was hosted by the Australian Computer Society, ACS. It was run as a federation of co-located conferences offered by the different IFIP technical committees, working groups and special interest groups, under the coordination of the International Program Committee.

The event was larger than ever before, consisting of 17 parallel conferences, focusing on topics ranging from artificial intelligence to entertainment computing, human choice and computers, security, networks of the future and theoretical computer science. The conference History of Computing was a valuable contribution to IFIPs 50th anniversary, as it specifically addressed IT developments during those years. The conference e-Health was organized jointly with the International Medical Informatics Association (IMIA), which evolved from IFIP Technical Committee TC-4 "Medical Informatics".

Some of these were established conferences that run at regular intervals, e.g., annually, and some represented new, groundbreaking areas of computing. Each conference had a call for papers, an International Program Committee of experts and a thorough peer reviewing process of full papers. The congress received 642 papers for the 17 conferences, and selected 319 from those, representing an acceptance rate of 49.69% (averaged over all conferences). To support interoperation between events, conferences were grouped into 8 areas: Deliver IT, Govern IT, Learn IT, Play IT, Sustain IT, Treat IT, Trust IT, and Value IT.

This volume is one of 13 volumes associated with the 17 scientific conferences. Each volume covers a specific topic and separately or together they form a valuable record of the state of computing research in the world in 2010. Each volume was prepared for publication in the Springer IFIP Advances in Information and Communication Technology series by the conference's volume editors. The overall Publications Chair for all volumes published for this congress is Mike Hinchey.

For full details of the World Computer Congress, please refer to the webpage at http://www.ifip.org.

June 2010

Augusto Casaca, Portugal, Chair, International Program Committee
Phillip Nyssen, Australia, Co-chair, International Program Committee
Nick Tate, Australia, Chair, Organizing Committee
Mike Hinchey, Ireland, Publications Chair
Klaus Brunnstein, Germany, General Congress Chair

Preface

The present book contains the proceedings of two conferences held at the World Computer Congress 2010 in Brisbane, Australia (September 20–23) organised by the International Federation for Information Processing (IFIP). In the first part, the reader can find the proceedings of the 9th Human Choice and Computers International Conference (HCC9) organised by the IFIP Technical Committee TC9 on the Relationship Between ICT and Society. The HCC9 part is subdivided into four tracks: Ethics and ICT Governance, Virtual Technologies and Social Shaping, Surveillance and Privacy, and ICT and Sustainable Development. The second part consists of papers given at the Critical Information Infrastructure Protection Conference (CIP) organized by the IFIP Technical Committee TC11 on Security and Privacy Protection in Information Processing Systems.

The two parts of the book are introduced by the respective Conference Chairs. Chapter 1 introduces HCC9, providing a short summary of the HCC conference series, which started in 1974, and explaining the overview of HCC9, detailing the rationale behind each of the tracks in this conference. The details related to the papers of each track are discussed by the Track Chairs in the respective introductions to the specific tracks of HCC9 (Chaps. 2, 10, 16 and 22). Finally, Chap. 22 introduces the CIP part.

The papers selected for this book cover a variety of relevant subjects, drawing upon high-quality research and experience from professionals working in various parts of the world. It is our intention that academics, practitioners, governments and international organisations alike will benefit from these contributions. We hope readers will engage in the debate, pushing forward the collective work we present here.

July 2010

Jacques Berleur
Magda David Hercheui
Lorenz M. Hilty

HCC9 2010

Organization

HCC9 Chairs

Jacques Berleur	University of Namur, Belgium
Magda Hercheui	Westminster Business School, UK London School of Economics, UK
Lorenz M. Hilty	University of Zurich, Switzerland Empa, Swiss Federal Laboratories for Materials Science and Technology, Switzerland

HCC9 Track Chairs and Program Committee

Track 1: Ethics and ICT Governance

Chairs

Jacques Berleur	University of Namur, Belgium
Catherine Flick	University of Namur, Belgium
Philippe Goujon	University of Namur, Belgium
Diane Whitehouse	The Castlegate Consultancy, UK

Program Committee

Julie Cameron	Info. T.EC Solutions Pty Ltd., Australia
Annemieke Craig	Deakin University, Australia
Richard Delmas	EC, Belgium
Penny Duquenoy	Middlesex University, UK
Françoise Massit-Folléa	Vox Internet, France
Marc van Lieshout	TNO, The Netherlands
John Weckert	Charles Sturt University, Australia
Gunnar Wenngren	AB Wenngrens i Linköping, Sweden
Chris Zielinski	WHO, Congo

Track 2: Virtual Technologies and Social Shaping

Chairs

David Kreps	Salford Business School, Salford University, UK
Martin Warnke	Computer Science & Culture, Leuphana University, Germany

Program Committee

Oliver Burmeister	University of Wollongong, Australia
Niki Panteli	School of Management, University of Bath, UK
Erika Pearson	Otago University, Dunedin, New Zealand
Lin Yan	Greenwich University, UK
Sean Westwood	Stanford University, USA

Track 3: Surveillance and Privacy

Chairs

Simone Fischer- Hübner	Karlstad University, Sweden
Yola Georgiadou	Geo-information Science and Earth Observation (ITC), University Twente, The Netherlands

Program Committee

Roger Clarke	Xamax Consultancy Pty Ltd., Australia
George Danezis	Microsoft Research, UK
Marit Hansen	Independent Centre for Privacy Protection, Germany
Francis Harvey	University of Minnesota, USA
JAN Holvast	Holvast & Partner, The Netherlands
David-Olivier Jaquet-Chiffelle	University of Lausanne, Switzerland
Eleni Kosta	KU Leuven, Belgium
Ronald Leenes	Tilburg University, The Netherlands
Andreas Pfitzmann	TU Dresden, Germany
Kai Rannenberg	Goethe University Frankfurt, Germany
Morton Swimmer	John Jay College of Criminal Justice, CUNY, USA
Jozef Vyskoc	VaF, Slovakia
Diane Whitehouse	The Castlegate Consultancy, UK
Louise Yngström	Stockholm University/KTH, Sweden

Track 4: ICT and Sustainable Development

Chairs

Lorenz M. Hilty	University of Zurich, Switzerland Empa, Swiss Federal Laboratories for Materials Science and Technology, Switzerland
Magda Hercheui	Westminster Business School, UK London School of Economics, UK

Program Committee

Gunilla Bradley	Royal Institute of Technology, Sweden
Vlad Coroama	Empa, Switzerland
Mihaly Csoto	ITTK, Hungary
Lorenz Erdmann	IZT, Germany
Klaus Fichter	Borderstep Institute, Germany
Roland Geyer	University of California Santa Barbara, USA
Wolfgang Hofkirchner	University of Salzburg, Austria
Shirin Madon	London School of Economics, UK
William McIver	National Research Council, Canada
Bernd Page	University of Hamburg, Germany
Tony Vetter	International Institute for Sustainable Development, Canada
Eric Williams	Arizona State University, USA
H. Scott Matthews	Green Design Institute, Carnegie Mellon University, USA

Reviewers

Track 1

Jacques Berleur	University of Namur, Belgium
Julie Cameron	Info. T.EC Solutions Pty Ltd., Australia
Penny Duquenoy	Middlesex University, UK
Richard Delmas	EC, Belgium
Catherine Flick	University of Namur, Belgium
Philippe Goujon	University of Namur, Belgium
Françoise Massit-Folléa	Vox Internet, France
Marc Griffiths	The Castlegate Consultancy, UK
Marc van Lieshout	TNO, The Netherlands
Gunnar Wenngren	AB Wenngrens i Linköping, Sweden
Diane Whitehouse	The Castlegate Consultancy, UK
Chris Zielinski	WHO, Congo

Track 2

Niki Panteli	School of Management, University of Bath, UK
Martin Warnke	Computer Science & Culture, Leuphana University, Germany
Claus Pias	University of Vienna, Austria

Track 3

Roger Clarke	Xamax Consultancy Pty Ltd., Australia
George Danezis	Microsoft Research, UK
Marit Hansen	Independent Centre for Privacy Protection, Germany
Francis Harvey	University of Minnesota, USA

David-Olivier Jaquet-Chiffelle	University of Lausanne, Switzerland
Eleni Kosta	KU Leuven, Belgium
Andreas Pfitzmann	TU Dresden, Germany
Kai Rannenberg	Goethe University Frankfurt, Germany
Morton Swimmer	John Jay College of Criminal Justice, CUNY, USA
Jozef Vyskoc	VaF, Slovakia
Diane Whitehouse	The Castlegate Consultancy, UK
Matthias Kirchner	TU Dresden, Germany

Track 4

Gunilla Bradley	Royal Institute of Technology, Sweden
Katharina Bunse	ETH Zurich, BWI Center for Enterprise Sciences, Switzerland
Vlad Coroama	Empa, Switzerland
Lorenz Erdmann	IZT, Germany
Wolfgang Hofkirchner	University of Salzburg, Austria
John Houghton	Centre for Strategic Economic Studies, Victoria University, Australia
Shirin Madon	London School of Economics, UK
H. Scott Matthews	Green Design Institute, Carnegie Mellon University, USA
William McIver	National Research Council, Canada
Andreas Möller	Leuphana University Lueneburg, Germany
Bernd Page	University of Hamburg, Germany
Thomas Ruddy	Empa, Switzerland
Eric Williams	Arizona State University, USA

CIP 2010

CIP Chair

William Caelli	Information Security Institute, Queensland University of Technology, Australia

Table of Contents

Section 2: Virtual Technologies and Social Shaping

Section 3: Surveillance and Privacy

Section 4: ICT and Sustainable Development

Part 2: Critical Information Infrastructure Protection Conference (CIP 2010)

Part 1

Human Choice and Computers International Conference (HCC9)

What Kind of Information Society? Introduction to the HCC9 Conference Proceedings

Jacques Berleur[1], Magda David Hercheui[2,3], and Lorenz M. Hilty[4,5]

[1] University of Namur, 61, rue de Bruxelles, 5000 Namur, Belgium
[2] Westminster Business School, 35 Marylebone Road, London, United Kingdom, NW1 5LS
[3] London School of Economics, Houghton Street, London, United Kingdom, WC2A 2AE
[4] University of Zurich, Department of Informatics, Binzmuehlestr. 14, CH-8050 Zurich, Switzerland
[5] Empa, Swiss Federal Laboratories for Materials Science and Technology, Lerchenfeldstr. 5 CH-9014 St.Gallen, Switzerland
jberleur@info.fundp.ac.be, m.hercheui@lse.ac.uk, lorenz.hilty@empa.ch

1 The HCC Conference Series

The Human Choice and Computers (HCC) conferences organized by the IFIP Technical Committee 9 (TC9)[1] have been important fora for discussing the impact of Information and Communication Technology (ICT) on society, ranging from the way ICT affect our lives at home and at the workplace to the impact that they have in institutions and communities. These conferences have permitted scholars and practitioners to discuss technology from a social perspective: once we understand that artefacts are not neutral, it becomes necessary to explore their economic, political, cultural, and social implications. In this introduction we recount briefly the history of the HCC conferences, in order to contextualise the contribution made by the HCC9 and the papers published in this book, a topic discussed in section 2.

The first world conference Human Choice and Computers was held in 1974 (April 1-5) in Vienna [8]. The initiative came from Heinz Zemanek, President of IFIP (1971-1974), who at the time was also president of IBM Austria. He was supported by Fred Margulies, Secretary of IFAC (International Federation of Automatic Control) who was a main lead in the reflection process launched by trade unions on the computerization of working life. The success of HCC1 was such that IFIP-TC9 henceforth considered it the TC's founding event, if not birthplace. TC9 was conceived in 1976, two years after HCC1. Its creation was fortunate: having a technical committee reflecting on the issues raised by the nascent Information Technology (IT) was a blessing.

Kelly Gotlieb (CDN) was the first TC9 Chair, and organized HCC2 with Fred Margulies, which took place in Baden (Austria) in 1979 (June 4-8) [7]. It was the first attempt to clarify the field of "Computers and Society". In the proceedings, Abbe Mowshowitz attempted to list the main social issues in computing.

The third world conference HCC3 was held in Stockholm from 2 to 5 September 1985 [10]. Comparative Worldwide National Computer Policies was chosen as its main theme in an attempt to go further in the direction of how various nations were

[1] The IFIP Technical Committee 9 (TC9) is dedicated to the study of the relationship of Computers and Society (http://www.ifiptc9.org/).

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 3–9, 2010.

designing policies on ICT in domains such as working life, public policy, culture, etc. TC9 was chaired at that time by Harold Sackman.

HCC4 took place from 6 to 12 June 1990 in Dublin [2]. It was prepared by TC9, under the chairmanship of Klaus Brunnstein and the European FAST Programme led by Riccardo Petrella. The concept of Technology Assessment applied to the field of Information Technology was surely the first attempt to consolidate the main reflection on social aspects of science in the field of ICT.

The fifth world conference HCC5 was organised in Geneva (August 25-28, 1998) with the help of Silvio Munari and the HEC of the University of Lausanne [9]. It was the first time that TC9 addressed the role of ICT in the context of globalization. Pertti Järvinen was the TC9 Chair.

HCC6 was held in Montreal (August 25-30, 2002) as a track of the 17th IFIP World Computer Congress [5]. The main theme concerned the scope of TC9 as stated in its Aims and Scope: "Issues of Choice and Quality of Life in the Information Society." Klaus Brunnstein and Jacques Berleur, TC9 Chair, were the fathers of that worldwide initiative, organizing as well the IFIP-WG 9.2 Namur Award Ceremony in honour of Deborah Hurley, Director of the Harvard Information Infrastructure Project.

HCC7, the 7th conference on Human Choice and Computers "Social Informatics: An Information Society for all?", was held in Maribor (Slovenia) on September 21-23, 2006 [3]. This conference focused on the concept of social informatics, its methodology and practice, in remembrance of Rob Kling (August 1944 - May 2003). The participants debated this field defined by Rob Kling as the discipline which examines social aspects of computerization – including the roles of information technology in social and organizational change and the ways that the social organization of information technologies are influenced by social forces and social practices.

Participants from all continents gathered at the conference, with speakers coming from 17 different countries. Work was organized in six plenary sessions, nine sessions in five tracks and two panel discussions. A separate part of the conference was the Student forum on Fair Globalisation and ICT based on the syntegration method and created by our Danish colleagues from the Copenhagen Business School (CBS).

The 8th Human Choice and Computers conference, hosted by the University of Pretoria, South Africa (September 25-27, 2008), focused on the social dimensions of ICT policy [1]. Policy plays a major role in the advancement of ICT and the shaping of ICT-mediated socio-economic practice. It also provides mechanisms for addressing potentially undesirable effects of ICT innovation and influences ethical conduct in modern society.

This conference was intended to explore the theoretical justification of policy action concerning ICT and socio-economic change and to discuss particular policies through which various institutions of contemporary governance have sought to promote ICT, to achieve specific socio-economic changes, or to address undesirable effects of ICT diffusion in contemporary society.

Lastly, the 9th Human Choice and Computers International Conference, which is embedded in the 21st World Computer Congress (WCC 2010), is to take place in Brisbane, Australia between 20 and 23 September 2010. In this conference, scholars and practitioners will meet again to discuss what kind of information society we want to strive for. Organized in four tracks, HCC9 will focus on topics related to ethics,

governance, virtuality, surveillance, privacy, and sustainable development. The section below explains in detail the four tracks of HCC9.

2 Overview of HCC9

HCC9 chapters in this book explore topics in relation to the impact of ICTs on society and the importance of the discussion on the right of human choice in developing and adopting technology. The contributions explore theories and perspectives in a variety of domains, pointing out that ICTs are affecting the way we live in society, changing our understanding of identity, our relationships within communities and groups, our interaction with institutions and work places, and our expectations about the future of technology and its impact on societies.

The contributions show we must explore how technology is shaping our lives, and how we as societies want to shape technology and the governance structures related to the development, regulation and use of ICTs. The ethics of the development and use of ICTs continues to be a major area, and one intertwined with the debates on surveillance and privacy. The recent attention Facebook and Google have received from the media and society on related topics shows there is still much to be explored before arriving at a clear norm on how users' privacy should be respected during the handling of their data. Indeed, societies are coming up with new understandings of surveillance and privacy almost every day, either before or after the implementation of technology which changes the status quo. Security issues have been strong arguments for adopting surveillance technologies, but we must also take a critical look at the impact of such choices in society and individuals, in order to be sure we are making informed decisions.

Lastly, ICTs may have a role to play in fostering international development and sustainable development, but this expectation has to be verified in practice. In other words, ICTs have the potential to bring such benefits, but we have to consider the contexts in which such technologies are developed and diffused, in order to ensure we will be able to extract their potential benefits.

In the subsections below we introduce the rationale of each HCC9 track. These introductions are intended to serve the reader as a starting point to understand the selection of articles which contribute to part 1 in this volume.

2.1 Ethics and ICT Governance

Governance is an old word that goes back to Plato. The concept disappeared for a while, and was replaced by ideas like government, and government policy. Governance has now returned to the scene. Today, it is focussed on issues like participative democracy and transparency.

The state is no longer a unique partner in regulating systems. Other actors take part at the local, regional, national, and international levels. New means of regulating scientific, technical, and other subsystems, and new ways of communicating, are possible among a variety of actors and subsystems.

Internet governance has been a highly debated issue throughout the early part of the first decade of the twenty-first century, particularly at the World Summit on

Information Systems (WSIS), held in Geneva in 2003 and in Tunis in 2005. The proposal to set up a Working Group on Internet Governance (WGIG) was adopted by government negotiators in Tunis. It put forward a multi-stakeholder approach to Internet governance. Stakeholder engagement has since become increasingly strong.

These debates raised other questions, particularly with regard to the role of business as a stakeholder. Even if the word "government" seems familiar, "civil society" and the "private sector" are perhaps less well defined. "Civil society" can be defined rather simply in the spirit of the philosopher Jürgen Habermas. Alternatively, it may be given more extensive definitions that invite discussions on precisely which kinds of organisations should be among the participants in civil society, and the extent to which business should be involved.

The main goal of the track Ethics and ICT Governance is to offer a forum to establish ICT governance as a new field in the discourse on computing ethics. The track continues the work of IFIP's SIG 9.2.2 Ethics of Computing, which has been working in this domain for almost 20 years. The group has produced various books and monographs on the ethics of computing. Yet it recognises that the current literature and guidelines could be enhanced and expanded upon, which has been the motivation behind the organisation of this track.

The contributions selected for this book discuss piracy, community empowerment, the digital divide, public procurement, ICT standardisation, money laundering and ethical governance for emerging ICTs. Jacques Berleur, Diane Whitehouse, Philippe Goujon and Catherine Flick introduce the theme of these contributions in detail in chapter 2, embedding them in a broader debate on ethics and governance.

2.2 Virtual Technologies and Social Shaping

The track Virtual Technologies and Social Shaping, coordinated by the IFIP Working Group on Virtuality and Society (IFIF WG 9.5), focuses on the feedback loops between virtual technologies and the social groups who use them, how each of them shapes the other and in turn is shaped by them.

Social shaping, the sociology of technology, science studies and other approaches of cultural studies to the phenomenon of the information society, driven by such classics as those of Bijker and Law [4] and Mackenzie and Wajcman [6] are arguably now ready to be given a fresh look in the context of virtual environments and global social networking and gaming communities. The intervening years have additionally seen an explosion of digital and media arts interpretations, and explorations of the impact of virtual technologies upon society, and the social use of such technologies upon their design, and entrepreneurial trajectories of their appearance in the global market.

Virtual technologies, crucially, have moved very decisively from the workplace – whether corporate or home office – into the domestic sphere, into our living rooms, playrooms, our kitchens, and our bedrooms. Here the relationship between virtual technologies and society, and the mutual shaping processes each of them undergoes, are ripe for fresh study, insight, and exploration.

The track addresses the choices faced by an information society permeated by ubiquitous virtual technologies, in which technology shapes social interactions, and society shapes technology. New identities and organisational forms emerge, huge

volumes of information demand new strategies to cope with them, and issues of intellectual propriety rights become more important. In chapter 10, David Kreps gives a more detailed introduction to this track.

2.3 Surveillance and Privacy

New technical and legal developments are posing greater and greater privacy dilemmas. Governments have in the recent years increasingly established and legalised surveillance schemes in form of data retention, communication interception or CCTVs purportedly for fighting terrorism or serious crimes.

Surveillance monitoring of individuals is also a threat in the private sector: private organisations are, for instance, increasingly using profiling and data mining techniques for targeted marketing, analysing customer buying preferences or social sorting. Work place monitoring practices comprise surveillance of employees. Emerging pervasive computing technologies, where individuals are usually unaware of a constant data collection and processing in their surroundings, will further exacerbate the problem that individuals are effectively losing control over their personal spheres.

At a global scale, Google Earth and other corporate virtual globes may have dramatic consequences for the tracking and sorting of individuals. With CCTV, the controlling power of surveillance is in few hands. With live, high resolution imagery feeds from space in the near future, massive surveillance may soon be available to everybody, a development whose consequences we do not yet grasp. New means of surveillance are also enabled by social networks, in which individuals are publishing many intimate personal details about themselves and others. Such social networks are today already frequently analysed by employers, the marketing industry, law enforcement or social engineering.

The track Surveillance and Privacy, coordinated by the IFIP Working Groups on Computers and Social Accountability, and Information Technology Misuse and the Law (WG 9.2 and 9.6/11.7), aims to explore and analyse such privacy risks of surveillance for humans and society as well as countermeasures for protecting the individuals' rights to informational self-determination from multi-disciplinary perspectives. In chapter 16, Yola Georgiadou and Simone Fischer-Hübner highlight the main contributions of the articles in this track.

2.4 ICT and Sustainable Development

ICTs are perceived both as enablers of societal change towards sustainable development and as drivers of unsustainable resource consumption. How can we use ICTs to support management techniques which permit corporations, governments and societies to contribute to sustainable development?

Starting with ICT hardware, the relevant debates focus on the qualities and quantities of the material and energy flows caused by the life cycle of devices and how their relevance to sustainable development can be assessed. For example, there are increasing environmental and social implications of electronic waste (e-waste) building up in both industrialized countries and emerging economies. Since the production of an ICT device requires quantities of more than half the elements listed in the periodic system, the demand for scarce chemical elements for ICT is expected to grow. Assessing and

reducing the energy and materials demand of ICT infrastructures per unit of service (Green IT) is therefore an important topic.

Much greater impacts – both in the positive and negative senses – with regard to sustainability can be caused by using ICT as an enabling technology for optimizing or being substituted for other technologies and processes. Researchers and practitioners alike are looking for solutions to apply ICT for higher energy and materials efficiency in production and consumption processes. Which applications might trigger a structural change towards a sustainable economy in the long run, and under what conditions might this be possible? A major issue under investigation is the application of ICTs for a reduction in greenhouse gas emissions and to facilitate adaptation to climate change, a topic that demands coordination on the local, national and global levels. ICTs are to be involved in the development of sustainable production, the improvement of resource productivity and economic dematerialization (decoupling total material consumption from GDP).

This track, coordinated by the IFIP Working Group on ICT and Sustainable Development (WG 9.9), will explore how information technology may indeed contribute to sustainable practices and processes in contemporary societies. In chapter 22, Lorenz Hilty and Magda Hercheui introduce the current discussion on ICT and sustainable development, presenting different views and conceptual frameworks related to this debate in a broad arena, and positioning the contributions of HCC9 within the debate on the role of ICT in sustainable development.

References

1. Avgerou, C., Smith, M.L., Besselaar, P.v.d. (eds.): Social Dimensions of Information and Communication Technology Policy, Proceedings of the 8th International Conference on Human Choice and Computers (HCC8), IFIP TC 9, Pretoria, South Africa, September 25-26. Springer, New York (2008)
2. Berleur, J., Drumm, J. (eds.): Information Technology Assessment: Human Choice and Computers 4, Proceedings of the 4th IFIP-TC9 International Conference on Human Choice and Computers (HCC4), Dublin, July 8-12. Elsevier/North-Holland, Amsterdam (1991)
3. Berleur, J., Nurminen, M., Impagliazzo, J. (eds.): Social Informatics: An Information Society for All? Human Choice and Computers 7, Proceedings of the 7th IFIP-TC9 International Conference in Remembrance of Rob Kling, Maribor (Slovenia), September 21-23. Springer Science & Business Media, Heidelberg (2006)
4. Bijker, W., Law, J. (eds.): Shaping Technology / Building Society: Studies in Sociotechnical Change. MIT Press, Cambridge (1992)
5. Brunnstein, K., Berleur, J. (eds.): Human Choice and Computers, Issues of Choice and Quality of Life in the Information Society, Proceedings of the 6th IFIP-TC9 Conference HCC6, at the 17th World Computer Congress, Montreal. Kluwer Academic Publ., Dordrecht (August 2002)
6. Mackenzie, D., Wajcman, J. (eds.): The Social Shaping of Technology. Open University Press, Buckingham (1985)
7. Mowshowitz, A. (ed.): Human Choice and Computers 2, Proceedings of the 2nd IFIP-TC9 Human Choice and Computers Conference (HCC2), Baden (Austria), June 4-8, 1979. Elsevier/North-Holland, Amsterdam (1980)

8. Mumford, E., Sackman, H. (eds.): Human Choice and Computers, Proceedings of 1st Conference on Human Choice and Computers (HCC1), Vienna (Austria), April 1-5, 1974. Elsevier/North-Holland, Amsterdam (1975)
9. Rasmussen, L.B., Beardon, C., Munari, S. (eds.): Computers and Networks in the Age of Globalization, Proceedings of the 5th IFIP-TC9 Human Choice and Computers International Conference (HCC5). Kluwer Academic Publishers, Boston (2000)
10. Sackman, H. (ed.): Comparative Worldwide National Computer Policies, Proceedings of the 3rd IFIP-TC9 Conference on Human Choice and Computers (HCC3), Stockholm, Sweden, September 2-5, 1985. Elsevier/North-Holland (1986)

Section 1

Ethics and ICT Governance

Ethics and ICT Governance

Jacques Berleur[1], Diane Whitehouse[2], Philippe Goujon[1], and Catherine Flick[1]

[1] University of Namur, Namur, Belgium
[2] The Castlegate Consultancy, Malton, United Kingdom
[3] Institut d'Informatique, FUNDP, Namur, Belgium
jacques.berleur@info.fundp.ac.be,
info@thecastlegateconsultancy.com, philippe.goujon@fundp.ac.be,
catherine.flick@fundp.ac.be

Abstract. Human Choice and Computing is a longstanding series of conferences organised by the International Federation for Information Processing (IFIP)'s Technical Committee 9. This conference is the federation's ninth. One of its tracks concentrates on ethics and information and communication technologies (ICT) governance. A background explains why investigations of ethics and ICT governance are coming to the fore, and it shows how this has been tackled by IFIP's special interest group (SIG) 9.2.2 on a Framework for Ethics of Computing. On offer is an explanation of the purposes of the track – how to govern ICT ethically, a synthesis of its seven papers, and an overview of the results that the track is anticipated to achieve. It is hoped that, in an ever more global society, such a track and associated panel will enable a much more dynamic dialogue and exchange to take place among a wider diversity of cultures and countries, whether this is among academics, business executives, or policy-makers.

Keywords: Ethics, Governance, Information and Communication Technologies (ICT), Participative Democracy.

1 Background

Governance now includes a focus on participative democracy and transparency. The state is no longer the sole influence on the regulation of systems. Other actors take part at the local, regional, national, and international levels. New means of regulating scientific, technical, and other subsystems, and new ways of communicating are possible among a variety of actors.

This past decade has seen many attempts to highlight how top-down and bottom-up approaches to governance can be brought together in the ethics of computing and ICT governance. Traditional top-down forms of regulation are seen as unrepresentative by many thinkers, researchers, lobbyists, and activists. Societies' pluralism implies the growth of new forms of governance. Indeed, many international organisations are already exploring how this might take place [1]. High-level announcements on plans for a European digital agenda are anticipated by the time that Human Choice and Computing 9 takes place in September 2010.

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 13–21, 2010.

A multi-stakeholder approach to Internet governance, and to information and communications technologies (ICT) governance, and stakeholder engagement in the domain has become increasingly strong. However, what is meant precisely by Internet governance and a multi-stakeholder approach?

> *A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.* [2]

If the words "government" and "governance" contemporarily both seem familiar to researchers, "civil society" and the "private sector" are terms that have perhaps traditionally been less well defined, and will need more concerted efforts at determining concrete definitions. Discussions are more and more common about which kinds of organisations should be represented among the participants in civil society, and the extent to which business, business associations, and business systems are, or should be, involved in governance processes. Implicit in new forms of democracy and stakeholder involvement may be ethics that focus on fairness and justice.

Bottom-up approaches are often highly participatory in their underpinning theory, and hopefully too in their practice. Aspirations abound that the distance between rulers and the ruled, or those who govern and those who are governed, should be minimised.

In parallel with ICT governance, ethics and the ethics of computing are fields that are particularly worth deepening. A start to fundamental work along these lines already exists [3]. Descriptive approaches to the ethics of computing help to set the scene so that readers understand the context of the specific ethical dilemma and its challenges. Today, researchers and activists are seeking in a normative way to overcome these challenges. A critical approach to different sets of case studies and use-cases is under development. Participatory approaches to ICT governance are a well-known way of tackling these difficulties. They are becoming increasingly popular and widespread. At a more thoughtful ("epistemological") level, reflections on the ethics of governance are encouraged.

2 Ethics, Governance, and the Work of the International Federation for Information Processing

Over its fifty years of existence, the International Federation for Information Processing (IFIP) has worked to support information processing in its member countries and to encourage technology transfer to developing countries.

IFIP's special interest group (SIG) 9.2.2 focuses on a Framework on Ethics of Computing[1] is organising this particular track on ethics and ICT governance. It has been working in this domain for some twenty years, and has produced several books and monographs on the subject. As examples, we can especially cite the work of Pullinger [4], Berleur [5], Goujon et al. [3] and, more recently, Berleur et al. [6].

[1] http://www.info.fundp.ac.be/~jbl/IFIP/cadresIFIP.html/ (accessed on May 24, 1010).

Today, IFIP SIG9.2.2 is seeking to enhance and expand the available literature in this field from a wide variety of different perspectives and locations. As a result, it anticipates to be able to develop new guidelines.

3 Aims and Purpose of the Track

In today's global society, politics, context, and ethics are some of the major challenges that need to be faced in the process of developing sound ICT governance arrangements.

The main aim of the Human Choice and Computing (HCC) 9's track on ethics and ICT governance is to organise a discussion that will highlight two sets of important issues: on the one hand, challenges pertinent to new forms of ICT governance; and, on the other hand, ethics. ICT governance is a crucial component of the new, and developing, field of the ethics of computing, with everything that implies in terms of research, practice, and deployment.

The authors selected for this track all focus in some way on the subject of ICT governance. The papers build from the individual to the international. In an introductory paper, governance decisions take place at the level of personal, individual choices with regard to software piracy on which the behaviour of peers could nevertheless have a substantial influence. It is also important to consider the context and background of any governance decisions and their ethics. Associations, organisations, and countries have adopted very different ways of governing processes and technologies, although many aspire to greater commonality and consensus. In this track, the countries involve Bangladesh, China, and the Maldives[2]. Institutions and agencies of international stature include the European Commission and the Financial Action Task Force.

In their range across such differing societal levels, the papers in this track reflect what in sociological, and even philosophical, terms are referred to as *micro*, *meso*, and *macro* approaches or levels. The methodologies used by each of the seven papers in this track differ considerably. Many papers – although they identify cultural, organisational, or social challenges with regard to making decisions about ICT, and managing or governing it – do not cover the relevant ethical issues in detail. It is the programme committee's aspiration that these ethical issues will emerge much more strongly in the actual track presentations, and the ensuing panel discussion on the "Ethics of computing: insights into today's key issues", which will take place in Brisbane, Australia, on Wednesday September 22, 2010.

In this track, an emphasis has been placed on the internationalism of the setting – in Brisbane, Australia – in which the conference takes place, and the range of authors chosen to contribute to it. The track is characterised by the diversity of the sources of its papers. The authors focus on governance contexts that are experienced in Australia, Bangladesh, China, the Maldives, South Africa, the United Arab Emirates, the United States of America, and a variety of European countries. As a result, the track

[2] A much wider range of institutions and their role in governance and the ethics of computing is explored in [1]. The institutions and geographic coverage represented by the authors in this track are probably in that sense influenced by the membership organisations of IFIP, on the one hand, and by the location of the conference in the southern hemisphere, on the other.

brings to light the fact that various, different aspects of ICT governance and its ethical challenges have to be scrutinised carefully when we examine the character of globalism and the richness of multiculturalism.

4 The Individual Articles in the Track

These papers are presented in the order in which they will appear in the track on Wednesday September 22, 2010. They progress from a level which is individual to levels which are local/regional, national, European, and international. This ordering of the papers will enable HCC9 readers and attendees to understand in more depth the notions of *micro*, *meso*, and *macro* levels of sociology and philosophy. The track ends with a more reflective, and theoretical, paper that examines a possible framework for the assessment of ethics and ICT governance. A discussion panel will then facilitate a wider process of dialogue and discussion.

The Demographic Factors Affecting University Students' Intention to Pirate Software, Linda Spark

Pirating software is considered to be illegal in many countries. Convention n° 185 on Cybercrime of the Council of Europe[3] classifies it as such, at least in terms of the European Member States.

The author presents an extensive survey among South African undergraduate and graduate students on their intentions to pirate software. This study explores the demographic factors that affect the students' intentions. The students' gender and level of study appear to have the most significant effect, and their academic discipline and level of household income the least.

The author's investigation raises questions about the need for education about the ethics of software piracy, and the implications and consequences of any actions taken by them.

ICT Governance *versus* Community Empowerment: Grassroots Evidence from Bangladesh, Mizanur Rahman

Science, Technology and Society studies emphasise a need for multi-stakeholders, and community-led and participative approaches that strengthen the innovation process. However, contemporary surveys and benchmarking show that this ideal is not always reachable. This paper outlines three layers of community empowerment: informing, consulting and involving. ICT empowerment is said to include access, use, technological appropriation, "carrier of meaning", and social appropriation.

There are 2165 telecentres in Bangladesh for a total country population of about 120 million inhabitants, among whom 80% live in rural areas. The aim is to ensure that, by 2020, each Union Parishad (an administrative entity of about 25,000 inhabitants) should have at its disposal a Union Information Centre that enables the local citizens to access information.

The paper's conclusion with regard to ICT empowerment is realistic. It shows that, regardless of whether the local government authorities are using older or newer forms

[3] The Council of Europe. Action against Economic Crime (accessed on May 24, 2010), http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp/

of ICT, people's empowerment is far from being a reality. No ethical conclusion is derived in this paper, but a political challenge is surely open.

Exploring the Digital Divide in the Maldives, Mohamed Shareef, Adegboyega Ojo, and Tomasz Janowski

The Maldive Islands in the Indian Ocean constitute an archipelago of 26 natural coral atolls. There are around 1,192 small low-lying islands, of which 194 are permanently inhabited. Only four of these islands have a population of over 5,000. One hundred and thirty-one of them have a population which is below 1,000; seventy-two have a population below 500. The distance north-south is 823 kilometres, and west-east is 130 kilometres. The range is quite obvious.

The paper starts by defining rapidly, and with acuity and interest, the concept of the digital divide. It takes into account the different factors which enable people to benefit from digital technology, and those which do not. The paper answers two main questions: How are the atolls of the Maldives divided with respect to access to ICT, and how significant is the geographical distribution and demography of the atolls to the digital divide? Its results are convincing. The analysis shows clearly that there is no digital divide with respect to mobile phones. There is, however, a large difference in terms of the penetration of the household use of both Internet and personal computers. The difference between the capital city, Male', and the remainder of the Maldives' atolls is significant.

While the challenges of geographic dispersal and population density to ICT development are fairly well accepted, the analysis of the paper shows that the relationship between these characteristics and the creation of the digital divide are more complex.

The ethical issues which probably underlie the paper are not made explicit, however. An analysis of literacy as in the International Telecommunications Union's Digital Access Index could have helped to open up that discussion[4].

Balancing Public and Private Interests in ICT Standardisation: The Case of AVS in China, Junbin Su and Vladislav Fomin

This paper proposes a way to reconcile the vested interests of patent holders, intellectual property rights, and the public through a "Fair, rational and non-discrimination" (FRAND) and royalty-free standard-setting process. It focuses on the case of the Audio Video Coding Standard (AVS) established by the Ministry of Information Industry of China in 2002. The AVS example can be applied in other ICT standardisation processes. A more comprehensive model of committee standardisation called the "Public Dominated Model" has been derived from it.

The process to define the AVS has led to the development of a theoretical model that deals with the conflict of interests. The standard is protected from a kind of monopoly of rents by a few companies where the public interest is often neglected and where the holders of essential patents obey the FRAND. This presupposes a balanced representation of the stakeholders. AVS is inspired by the development of MPEG-family standards. What is different is the policy on intellectual property rights.

[4] International Telecommunications Union, Digital Access Index (accessed on May 24, 2010), http://www.itu.int/ITU-D/ict/dai/

The FRAND proposal belongs surely to the field of Science, Technology and Society studies. However, it is not yet entirely clear why the AVS model privileges public research institutes and universities among its various stakeholders. The authors explore the complexity of public-private dilemmas in ICT standardisation-setting.

The European VCD Service: Facilitating Public Procurement through Criteria to Evidence Mapping, Ansgar Mondorf and Maria A. Wimmer
This paper develops a model which favours interoperability among European interstate commissioning ("procurement"). One of the key building blocks which has emerged from the European Commission co-funded project on Pan-European Public Procurement On-Line (PEPPOL) is the Virtual Company Dossier (VCD). The idea of this model is to facilitate the appropriate mapping of national criteria in a common tendering process, and to support the mutual recognition – among Member States – of certificates and qualification documents which satisfy the appropriate legal, organisational, semantic and technical interoperability criteria in Europe. The paper makes explicit a set of specific rules to do this.

As an eCommerce or eGovernment paper, this paper falls in the governance domain. However, its purely technical approach does not immediately enable the identification of any underlying ethical principles.

Money Laundering and FATF Compliance by the International Community, Ali Alkaabi, George Mohay, Adrian McCullagh, and Nicholas Chantler
The International Financial Action Task Force (FATF) has established 40 recommendations against money laundering, and nine special recommendations for combating the financing of terrorism. In this paper, the authors examine how four countries have implemented those recommendations in their legal systems, preventive measures, and institutional and other measures. The four countries are: Australia, the United Arab Emirates (UAE), the United Kingdom (UK), and the United States of America (USA). The analysis of FATF compliance shows that the USA (with 34 implemented recommendations), followed by the UK (29) and Australia (21), are fully or largely compliant with the anti-money laundering recommendations; the UAE is the least compliant country (17). With regard to the nine specific recommendations, the order of compliance remains the same (in descending order, 9, 8, 5 and 3). In both cases, the UAE is the least compliant vis-à-vis the recommendations.

From a HCC9 viewpoint, it is interesting to try to understand the reasons why the situation is like this. A first explanation is that the founding members of the FATF like Australia, the UK and the USA – which did not include the UAE – have left their unavoidable, cultural imprints on the organisation and its operations. But there are other factors that appear to affect the degree of compliance. The authors offer examples such as culture, faith, and socio-economic elements. They note that:

> *… the culture and legal systems support each other and that economic development and financial structures are affected not only by a country's legal system but also by its culture and show that development of a country's legal and financial system is related to its religious beliefs.*

and,

> *Islam prohibits any activity funded by money derived from unlawful trade or ill-gotten property and prohibits using illegal money for charities. Money gained*

> *from gambling and bank interest is prohibited in Islam. This is in marked contrast to normal practice in Australia, the UK and the USA.*

There are also social, economic and financial factors:

> *The UAE is a cash-based economy: in it, carrying large cash amounts is a normal practice and this makes it more difficult to impose requirements concerning reporting large cash transactions. Imposing regulations (for instance, requiring all large transactions to be reported) in such circumstances is very difficult if not impossible.*

The authors conclude that these various factors present a challenge to the international community and to the FATF. These dilemmas can only be resolved by careful, country by country, consideration of local factors.

Ethical Governance for Emerging ICT: Opening Cognitive Framing and Achieving Reflexivity, Philippe Goujon and Catherine Flick

This paper's aim is to find new ways to address the ethical problems raised by ICT. The paper draws on examples of technological development projects supported by the European Commission's latest research and technological development Framework Programme (2007-2013).

Many such projects are subject to a strong push for technology development. It too often obscures the need for any deep form of ethical consideration prior to a technical project being funded, developed or deployed. Ethics can become an "add-on", a sort of accessory or instrumentalised guarantee.

> *In this context, expertise, whether it is philosophical or scientific, becomes the indisputable new source of normativity. The problems revealed are confined to a scientific perspective alone; this means that the challenges taken into account are confined to the realm of strict scientific rationality. Democracy is confiscated.*

The authors illustrate the limitations of technology assessment. They show that the cognitive framing of the assessment process is often biased by expertise. Thus, such assessments might simply represent, or remain, a means of designing the social acceptance or acceptability of a specific technology.

There is a variety of elements ("conditions") which need to be borne in mind. What is called in this paper, the "opening of the cognitive framing" is a preliminary condition for a real social and ethical approach. However, there are other conditions: norms and ways of life have to be addressed; dominant norms need to be challenged by minority norms; and a "second-order reflexivity" should encourage a testing of the governance process for its social legitimacy.

The authors introduce the theory and approach of Belgian theorists, Jacques Lenoble and Marc Maesschalck [7]. These philosophers advocate a form of "progressive reflexive governance". This kind of governance process enables the actors who are involved in any technological project or initiative to organise themselves in a way that would enable them to think about their own construction of the particular project's framing, context, and norms. The terms – such as framing, context, and norms – are explained in the paper. The track programme committee is interested to explore the appropriateness and application of these ideas in an international setting.

5 An Overview of the Track

These papers on ICT governance and the ethics of computing build from the individual to the international. They first investigate elements of self-governance at the individual level: for example, in terms of activity around software piracy and the degree of control that individuals may have on their own actions and peer groups on them. They progressively examine how associations, organisations, and countries can govern their choices with regard to computing and the Internet. Last but not least, a framework is provided for a way to look at ethics of computing cases, contexts, and ways of organising. To date, it has been tested largely only in the Benelux countries or in wider European settings. It is a considerable challenge to assess its application to a wider international context.

The panel will come at the end of the papers represented by this track. It is likely to concentrate even more on the ethical issues that surround computing than on the governance arrangements. It will deliberately expose in a more structured manner what are called the *micro-meso-macro* (bottom, middle, and high) levels of the ethics of computing. It will draw on a mix of voices and opinions which come from a diversity of geographic and cultural settings. In an ever more global society, it is hoped that such a track can help to explore more dynamic forms of dialogue and sharing among a wider diversity of cultures, communities, and countries.

The programme committee urges not only an enjoyment of the reading of these papers on ICT governance and the ethics of computing, but also quiet reflection on their meaning and more systematic application of that meaning in action.

Acknowledgments. As track programme chairs, we thank all the programme committee members for their efforts in supporting the organisation of this track. In this respect, we would especially like to acknowledge the following for their intellectual and organisational inputs: Julie Cameron, Penny Duquenoy, Richard Delmas, Françoise Massit, Marc Griffiths, Marc van Lieshout, Gunnar Wenngren, and Chris Zielinski. We are cognisant of the efforts of John Weckert in agreeing to co-chair the track's panel discussion on the "Ethics of computing: insights into today's key issues".

References

1. Berleur, J.: Governance Challenges: First Lessons from the WSIS – An Ethical and Social Perspective. In: Goujon, P., Lavelle, S., Duquenoy, P., Kimppa, K., Laurent, V. (eds.) IFIP International Federation for Information Processing. The Information Society: Innovation, Legitimacy, Ethics and Democracy, vol. 233, pp. 225–259. Springer, Boston (2007)
2. World Summit on the Information Society (WSIS), The Tunis Agenda. See especially articles §§29-82, and §34, `http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=22670` (accessed on May 24, 2010)
3. Goujon, P., Lavelle, S., Duquenoy, P., Kimppa, K., Laurent, V.: The Information Society: Innovation, Legitimacy, Ethics and Democracy. Springer, Boston (2007)

4. Pullinger, D.: Society, Religions and Information Technology. In: Berleur, J., Clement, A., Sizer, R., Whitehouse, D. (eds.) The Information Society: Evolving Landscapes, pp. 124–144. Springer-Verlag and Captus University Publications, New York (1990)
5. Berleur, J.: Culture and democracy revisited in the global information society: Summary of a position paper. In: Berleur, J., Whitehouse, D. (eds.) An Ethical Global Information Society: Culture and Democracy Revisited, pp. 3–11. Chapman & Hall, London (1997)
6. Berleur, J., Duquenoy, P., Gotterbarn, D., Goujon, P., Kimppa, K., Six, B., Weber-Wulff, D. (eds.): Ethics of Computing Committees: Suggestions for Functions, Form and Structure. On behalf of IFIP SIG9.2.2. IFIP, Laxenburg, Austria (2008)
7. Lenoble, J., Maesschalck, M.: Towards a Theory of Governance: The Action of Norms. Kluwer Law International, The Hague (2003)

The Demographic Factors Affecting University Students' Intention to Pirate Software

Linda Spark

University of the Witwatersrand, Johannesburg, South Africa
linda.spark@wits.ac.za

Abstract. As the requirement to use computers increases, software piracy is increasing, yet little research has been conducted in South Africa to investigate the reasons why students pirate software. This paper reports on a study on the demographic factors affecting students' intention to pirate software. The study was carried out on students at the University of the Witwatersrand using questionnaires. It was found that gender and an individual's level of study had the most significant effect on intention to pirate, with academic discipline and level of household income having the least significant effect. Educational campaigns on the ethics and consequences of piracy are recommended.

Keywords: Software Piracy, Demographics, Students, Ethics, South Africa.

1 Introduction and Background

The use of technology has become necessary for our everyday lives [1], resulting in an increasing demand to use software. As the technology needed to pirate software has become cheaper and more efficient, piracy is increasing [2]. Worldwide, the piracy rate has increased from 38% in 2007 to 41% in 2009 (South Africa's piracy rate is 35%) and losses for the software industry grew by 5% (US$ 50.2 billion) [3].

Although some research has indicated that piracy assists diffusion of software and therefore "levels the playing field" for developing countries [4], other research has shown that piracy inhibits diffusion and so obstructs emerging countries [5], cited by [6] and [7]. Gopal and Sanders [8] suggested that developing countries may encourage or ignore piracy to allow cheaper access to technology.

Piracy can be defined as the "unauthorized use of computer software or the unauthorized distribution of copies of software without permission given by the owner" [9, p. 34]. It is regarded as both an illegal activity [1, 10] – taking an individual's property without consent or compensation is stealing – and an ethical issue [11, 12] – piracy may be regarded as a victimless and/or harmless act, seen as less ethically serious than the theft of physical property. This view may result in the erosion of ethics and individuals may resort to other such victimless or harmless practices [13].

Governance of Information Technology (IT) requires that assets and resources are managed to ensure that business goals are met, yet the escalating dependence on IT can result in increased risks for business [14]. Unethical behaviour by employees can

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 22–32, 2010.

have serious outcomes for businesses – a critical issue for managers who are responsible for their employees' workplace behaviour [15].

Schilhavy and King [15] suggest that professional behaviour starts developing already in the educational system. As little piracy research has been done on students in South Africa, there is a need to investigate the factors that affect the intention to pirate software and whether the factors found overseas apply to South African students. In addition, as technology diffusion increases around the world, intellectual property rights for software are of increasing concern for both researchers and businesses [7].

As many courses require students to use computers, students' demand for software increases. However, students typically do not have much disposable income to acquire the software that they require; they may therefore resort to piracy as they often have the tools and know-how to do so [2]. Gan and Koh [16] and Van Belle, Macdonald and Wilson [17] suggested that piracy is highest among young people, with much of it happening at universities. In addition, Christensen and Eining [18] and Gattiker and Kelley [19] found that students pirate software because they believe it is reasonable or acceptable to pirate. Recent research has started to show that there are students who believe it is not illegal to make copies of software [6, 20], while there are others who believe it is acceptable to use "free" trial software versions for indefinite periods [16].

So, what are the factors behind this reasoning on the part of students? This paper reports on a study that explored the demographic factors that affect students' intention to pirate software.

1.1 Intention and Demographic Variables

Higgins [21] stated that intentions are an indication of how ready a person is to perform a specific behaviour. Ajzen [22] found that the greater the intention to perform an act, the greater was the probability of the behaviour actually taking place. Here, we examine six different variables and how they are treated in the literature in relation to software piracy.

Age. A large amount of research has looked at age and the effect it has on a person's acts of piracy. While Cronan, Leonard and Kreie [23] found that age was not a significant factor, Gopal and Sanders [24], Mishra, Akman and Yazici [25], Bhattacharjee, Gopal and Sanders [26] and Cronan, Foltz and Jones [27] found that younger students were more likely to pirate software than older students. In addition, Gan and Koh [16], Bachman [28], Seale, Polakowski and Schneider [29] and Kwong, Yau, Lee, Sin and Tse [30] found that age is inversely related to the amount an individual pirates software while Masrom, Ismail and Hussein [31] and Cronan and Al-Rafee [32] found a direct relationship between the age of a person and the extent to which that person may pirate.

Gender. Males are more likely to pirate software compared to females according to Chiang and Assane [2], Simpson, Banerjee and Simpson [10], Van Belle, Macdonald and Wilson [17], Siponen and Vartiainen [20], Bhattacharjee, Gopal and Sanders [26], Cronan, Foltz and Jones [27], Bachmann [28] and Kwong et al. [30]. However, Gopal and Sanders [24], Mishra, Akman and Yazici [25] and Al-Rafee and Cronan [33] found no correlation between gender and the decision to pirate software.

Price. The price of software is seen to be a major factor in determining a person's intention to pirate software [34, 35]. The higher the price, particularly if the gap between the price of legal and illegal software is great, the more individuals are likely to pirate rather than purchase software [11, 34, 35, 36, 37] especially when income levels are low [8].

Level of Household Income. Research into this determinant of intention to pirate has had mixed results. It is generally thought that as the level of household income increases, the amount of software pirated would decrease. However, Cheng, Sims and Teegen [36] and Rahim, Seyal and Rahman [38], cited by Liang and Yan [39], found only a weak relationship between household income and an individual's intention to pirate software. Gan and Koh [16], Kwong et al. [30], and Rahim, Seyal and Rahman [40] found no correlation between these variables. On the other hand, Lau [9], Mishra, Akman and Yazici [25] and Coyle, Gould and Gupta [41] found a significant relationship between income and the reasons for using pirated software. When software has a high price relative to income, it makes economic sense to purchase hardware and rely on pirated software [8].

Academic Discipline. This factor looks at the major subject or discipline that a student is studying. Wong, Kong and Ngai [42], cited by Liang and Yan [39], determined that students with majors in Science and Computer Studies were more likely to pirate software than students with business majors. However, no relationship between the courses studied and intention to pirate was found by Simpson, Banerjee and Simpson [10] and Gan and Koh [16].

Computer Ownership. Individuals who have their own computer spend more time using computers than those who do not. This allows those owners to become more knowledgeable about computers, including how to pirate software. Seale, Polakowski and Schneider [29] and Rahim, Seyal and Rahman [40] found that individuals who own a computer are more likely to use pirated software, but Kini, Ramakrishna and Vijayaraman [43] found that an individual who owned a computer had a higher level of moral intensity.

Personal Computer Experience. This variable looks at a student's familiarity with a computer (measured in the number of years of use). Students who do not have much experience of computer use are more likely to use a computer only for what their tasks and assignments require [40]. Cronan, Foltz and Jones [27], Malin and Fowers [44], and Seyal and Rahman [45] found that the more familiar a student is with a computer, the more likely the student will be to pirate software. In contrast, Kini, Ramakrishna and Vijayaraman [43] found that the relationship between experience and piracy was insignificant.

As a result of these conflicting findings about the impact of a variety of variables on a student's intention to pirate software, and the increasing software needs of "dishonest" students, it is deemed important to undertake research into the reasons why students pirate software. Little research has been done on the impact of ranges of variables on students' intention to pirate software in a South African context. Understanding the determinants of piracy may help to identify the target audience(s) for educational campaigns (which may assist in curbing software piracy) and assist employers in understanding the graduates that they employ.

2 Methodology

Approximately 400 questionnaires were distributed to university students at University of the Witwatersrand, via an online posting and handouts. Participation was voluntary and anonymous. The questionnaire targeted both undergraduate and postgraduate students, across the university's five faculties (Commerce, Law and Management, Humanities, Science, Engineering and the Built Environment and Health Sciences). Students were excluded if they were first-time computer users; the remaining respondents were students who may or may not have pirated software before. A total response rate of 62% was achieved, with the majority of respondents being undergraduate (90.7%) males (53.7%). The age of respondents varied from 18 to 25 for undergraduates (118 males and 104 females) and 21 to 31 for postgraduate students (13 males and 9 females). The majority of the respondents (88.2%) owned a computer or laptop and 51.4% had used a computer for 10 to 18 years. The majority of students (43.6%) responded that their total household income was R100 000 or more and 12.8% were in the range of less than R20 000, which showed a diversity of economic backgrounds (this represents monthly income)[1].

Besides the demographic questions, the questionnaire contained five questions which tested the respondent's intention to pirate software, namely: I intend to copy software in the near future; I will try to copy software in the near future; I will not make an effort to copy software in the near future; If I had the opportunity, I would commit software piracy; I would never commit software piracy. The questions were adapted from Goles et al. [13], Cronan and Al-Rafee [32], Peace, Gallette and Thong [46], and Limayem, Khalifa and Chin [47]. These were measured using a 7 point Likert scale from Strongly Disagree to Strongly Agree. Pearson's correlation coefficient analysis, an independent samples t-test and a one-way ANOVA were used to explore the relationships between the demographic factors and the intention to pirate.

3 Findings and Discussion

Here we explore the questionnaire findings in relation to the appropriate variables indicated in the literature.

Age. Pearson's correlation coefficient analysis was used to look at the relationship between age (M=20.24, SD=1.945) and the intention to pirate (M=4.2057, SD=1.51321). The correlation was statistically significant ($r=0.356$, $p<0.01$), showing a strong positive relationship between age and intention to pirate. A scatter plot is shown in Figure 1.

Past research has yielded contradictory findings on the effect that age has on a student's intention to pirate software. The findings of this study are consistent with the results of Gan and Koh [16], Bachman [28], Cronan, Foltz and Jones [27], and Kwong et al. [30], which suggested that age has a significant impact on an individual's intention to behave ethically or unethically. Specifically, the findings suggest

[1] At the time of writing there are around eight South African rand to the American dollar, nine to the euro, and seven to the Australian dollar.

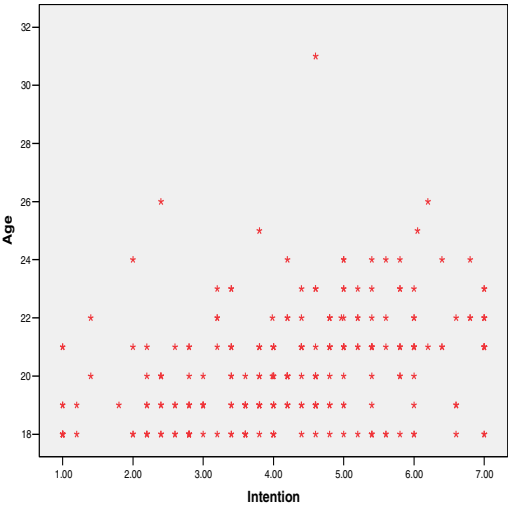


Fig. 1. Relationship between Age and Intention to Pirate

that age has an inverse direct effect on a student's intention to pirate software. The results were confirmed by an independent samples t-test that was carried out to compare the effect of level of study (undergraduate vs postgraduate) on intention to pirate. It was found that there was a significant difference in the scores for undergraduate students (M=4.1187, SD=1.49772) and postgraduate students (M=5.2091, SD= 1.39588); t=3.277, $p<0.05$. These findings suggest that as students mature, their level of moral intensity increases and perhaps they are more aware of the effects and consequences of pirating software. It would also suggest that younger students should be the target of educational campaigns.

Gender. An independent samples t-test was carried out to compare the effect of gender on intention to pirate. There was a significant difference in the scores on intention to pirate for males (M=4.9001, SD=1.36831) and females (M=3.4243, SD=1.28455); t=8.678, $p<0.05$.), suggesting that gender does have a significant effect on intention to pirate. The relationship is shown in Figure 2.

The findings of this study which show a significant relationship between gender and intention to pirate software are consistent with prior research by Chiang and Assane [2], Simpson, Banerjee and Simpson [10], Siponen and Vartiainen [20], Bhattacharjee, Gopal and Sanders [26], Cronan, Foltz and Jones [27], Bachmann [28], and Kwong et al. [30]. Specifically, the results reveal that males are more likely to pirate than females, which would suggest that males should be targeted in any anti-piracy education campaign.

Price of Software. An independent samples t-test was carried out to compare the effect of price of software on intention to pirate. There was a significant difference in the scores for respondents who believe that the price of software affects their decision about original software (M=4.4507, SD=1.44571) and those who do not (M=3.3623,

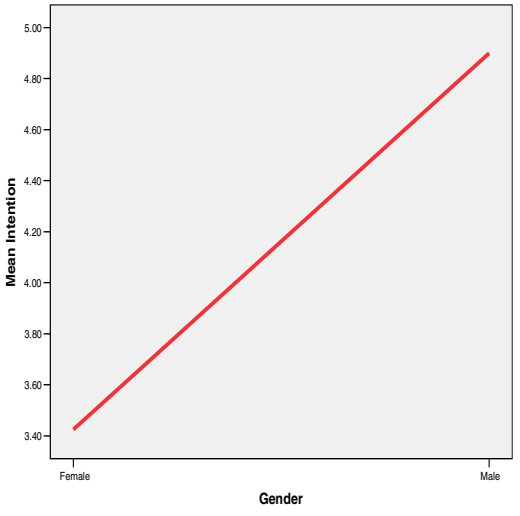


Fig. 2. Relationship between Gender and Intention to Pirate

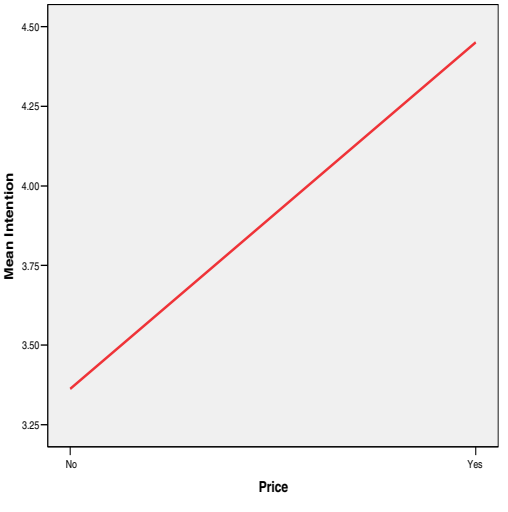


Fig. 3. Relationship between Price of Software and Intention to Pirate

SD=1.4827); t=4.828, p<0.05, which suggests that price does have a significant effect on intention to pirate. The relationship is shown in Figure 3.

The results of this study are consistent with the findings of Hsu and Shiue [34], Moores and Dhaliwal [35], Tan [11], Cheng, Sims and Teegen [36], and Miyazaki, Rodriguez and Langenderfer [37], which suggest that the price of software is a determinant in an individual's decision whether or not to pirate software. In order to succeed educationally, a student may need to work with various software packages. On a

limited income, he or she may turn to piracy as a way of obtaining the software required. To curb software piracy which takes place for this reason, software development companies should consider lowering the price of software, and/or increasing the software's perceived value by marketing the product better, and/or insuring a better product so the student perceives value for money. Alternatively, cheaper student versions of software could be made available, while retaining the various capabilities that students require. This would be particularly important in developing economies where cheaper access to technology is needed.

Level of Household Income. A one-way ANOVA between subjects was explored to compare the effect of income on intention to pirate at different income levels. There was no significant effect of income on intention to pirate at the $p>0.05$ level for the different levels of income. The findings were consistent with those of Gan and Koh [16], Kwong et al. [30], and Rahim, Seyal and Rahman [40] who found no correlation between income and pirating of software, yet they were expected to be similar to the findings of Lau [9], Mishra, Akman and Yazici [25], and Coyle, Gould and Gupta [41] who did find a significant relationship. It is important to note that students may not have known the answer to this particular question; as they were not given the opportunity to ask their parents for financial information, some students may have guessed or estimated the answer about the level of their household income.

Academic Discipline. A one-way ANOVA between subjects was explored to compare the effect of academic discipline on intention to pirate in Commerce, Engineering and the Built Environment, Health Sciences, Humanities and Science which represent the different faculties at the University of the Witwatersrand. There was no significant effect at the $p>0.05$ level for the different faculties. The study expected to find results consistent with those of Wong, Kong and Ngai [42], cited by Liang and Yan [39], who found a relationship between the major discipline of study and intention to pirate, but instead the findings were consistent with Simpson, Banerjee and Simpson [10] and Gan and Koh [16]. Irrespective of their choice of faculty, students are required to be familiar with computers and are required to use software. Although it might be believed that students in Engineering, Science and perhaps Commerce (doing courses that require software for systems design or programming, for example) may be more likely to pirate (since their courses demand more software to be used), an interesting finding of this study was that the Humanities faculty respondents had the greatest intention to pirate software. (The results, however, could be skewed due to the smaller number of student respondents from the university's Humanities faculty.)

Computer Ownership. An independent samples t-test was carried out to determine the effect of computer ownership on intention to pirate. There was a significant difference in the scores on intention to pirate for students who own a computer ($(M=4.2939, SD=1.49392)$ and students who do not own a computer ($M=3.6345$, $SD=1.60095$); $t=2.214$, $p<0.05$. This suggests that ownership of a computer has a greater influence on students to pirate software. The relationship is shown in Figure 4.

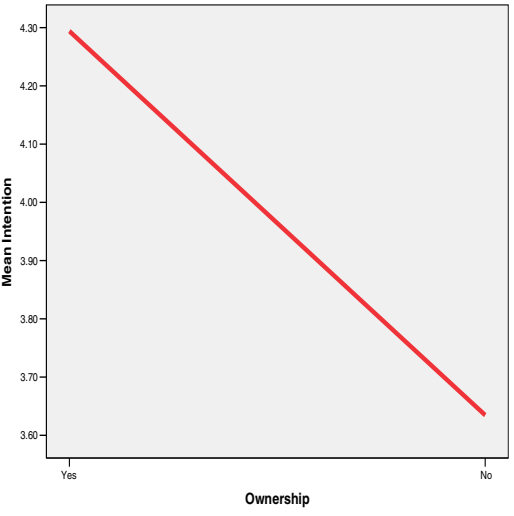


Fig. 4. Relationship between Computer Ownership and Intention to Pirate

The findings of this study are consistent with the results of studies done by Seale, Polakowski and Schneider [29] and Rahim, Seyal and Rahman [40]. They indicate that individuals who have their own computers are more likely to pirate software. Students would want their own copies of software and the mechanisms to monitor the actions of individuals on their own computers are inadequate. As the price of computers decreases, more people will purchase their own computers which may result in a need to educate computer owners about the effects and consequences of piracy. Once again, this would suggest that education about software piracy should start earlier as individuals would start using home computers at an earlier age.

Personal Computer Experience. Pearson's correlation coefficient analysis was used to look at the relationship between the number of years a student has used a computer (M=9.07, SD=4.815) and intention to pirate (M=4.2057, SD=1.51321). The correlation was found to be statistically significant ($r=0.232$, $p<0.01$), which suggests a strong positive relationship between personal computer experience and intention to pirate. A scatter plot is shown in Figure 5.

The results are consistent with the findings of Cronan, Foltz and Jones [27], Malin and Fowers [44], and Seyal and Rahman [45]. They reveal that the longer a student has used a computer, the greater his/her intention to pirate software. This could be a consequence of the student being more familiar with how to pirate and/or increasing needs for software. As young people will increasingly be using computers from a younger age, there will be an increase in piracy: this suggests that perhaps education on computer-related ethics and the effects and consequences of piracy should begin even earlier than at the tertiary level.

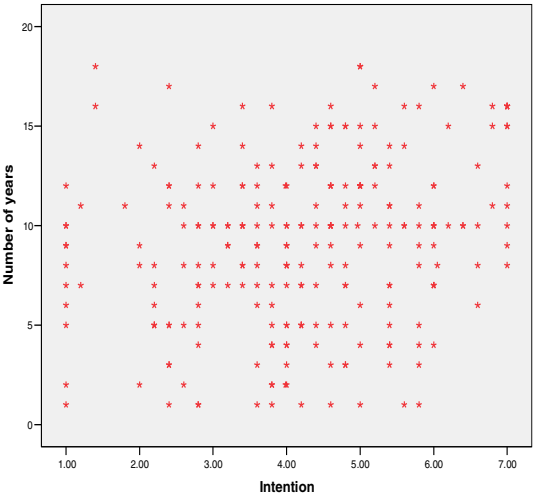


Fig. 5. Relationship between PC Experience and Intention to Pirate

4 Conclusion

Software piracy is increasing and is of great concern. Students need more software at a life stage when they usually cannot afford it. This study has explored the demographic factors that affect University of the Witwatersrand's students' intention to pirate software, with gender and level of study having the most significant effect and academic discipline and level of household income having the least significance.

This study measured intention to pirate as opposed to actual piracy behaviour, although intention is seen to be a good predictor of behaviour. Although measurement of piracy acts may be more accurate, it could raise the challenge of underreporting of piracy due to the illegal nature of that piracy. The accuracy of the variable relating to the level of household income, which some students may have guessed, is a further limitation of this study.

One of the strongest recommendations that can be taken from this study is the need for students in developing economies (including South Africa) to be educated in and become aware of the ethical norms expected of them, as they move from tertiary education into the business world that operates globally. This includes understanding and respecting intellectual property rights and the ethics of software piracy. Such an understanding would enable students to understand clearly the implications and consequences of pirating software and why piracy is regarded as unethical. Similarly, businesses need to know the standard of graduate who is entering the workplace, as part of the management of their IT assets and resources. This study would suggest that educational campaigns should target younger people who own computers, particularly males.

References

1. Hinduja, S.: Trends and patterns among online software pirates. Ethics Inform. Tech. 5(1), 49–61 (2003)
2. Chiang, E.P., Assane, D.: Music piracy among students on the university campus: Do males and females react differently? J. Socio. Econ. 37(4), 1371–1380 (2008)
3. Business Software Alliance (2007), http://www.bsa.org
4. Shoham, A., Ruvio, A., Davidow, M. (Un)ethical consumer behaviour: Robin Hoods or plain hoods? J. Consum. Mark. 25(4), 200–210 (2008)
5. Piatkowski, M.: The Institutional Infrastructure of the 'New Economy' and Catching-up Potential of Post-Socialist Countries. TIGER Working Paper Series 16, 1–28 (2002)
6. Rawlinson, D.R., Lupton, R.A.: Cross-National attitudes and perceptions concerning software piracy: A comparative study of students from the United States and China. J. Educ. Bus. 83(2), 87–93 (2007)
7. Marron, D.B., Steel, D.G.: Which countries protect intellectual property? The case of software piracy. Econ. Inq. 38(2), 158–174 (2000)
8. Gopal, R.D., Sanders, G.L.: Global software piracy: you can't get blood out of a turnip. ACM Commun. 43(9), 82–89 (2000)
9. Lau, E.K.-W.: Interaction effects in software piracy. Bus. Ethics: Eur. Rev. 16(1), 34–47 (2007)
10. Simpson, P.M., Banerjee, D., Simpson, C.L.: Softlifting: A model of motivating factors. J. Bus. Ethics 13(6), 431–438 (1994)
11. Tan, B.: Understanding consumer ethical decision making with respect to purchase of pirated software. J. Consum. Mark. 19(2), 96–111 (2002)
12. Gupta, P.B., Gould, S.J., Pola, B.: "To pirate or not to pirate": A comparative study of the ethical versus other influences on the consumer's software acquisition-mode decision. J. Bus. Ethics 55(3), 255–274 (2004)
13. Goles, T., Jayatilaka, B., George, B., Parsons, L., Chambers, V., Taylor, D., Brune, R.: Softlifting: Exploring determinants of attitude. J. Bus. Ethics 77(4), 481–499 (2008)
14. Pye, G., Warren, M.J.: Striking a balance between ethics and ICT governance. Australas. J. Inform. Syst. 13(2), 201–207 (2006)
15. Schilhavy, R.A.M., King, R.C.: The virtuous and the vicious: The effects of professionalism and Machiavellianism on ethical IT decision making. In: Proceedings of the 15th Americas Conference on Information Systems, California, USA, Paper 627, August 6-9 (2009)
16. Gan, L.L., Koh, H.C.: An empirical study of software piracy among tertiary institutions in Singapore. Inform. Manage. 43(5), 640–649 (2006)
17. Van Belle, J.-P., Macdonald, B., Wilson, D.: Determinants of digital piracy among youth in South Africa. Commun. IIMA 7(3), 47–64 (2007)
18. Christensen, A.L., Eining, M.M.: Factors influencing software piracy: Implications for Accountants. J. Inform. Syst. 5(1), 67–80 (1991)
19. Gattiker, U.E., Kelley, H.: Morality and computers: attitudes and differences in moral judgements. Inform. Syst. Res. 10(3), 233–254 (1999)
20. Siponen, M.T., Vartiainen, T.: Attitudes to and factors affecting unauthorized copying of computer software in Finland. Behav. Inform. Technol. 24(4), 249–257 (2005)
21. Higgins, G.E.: Digital Piracy: An examination of low self-control and motivation using short-term longitudinal data. CyberPsych. Behav. 10(4), 523–529 (2007)
22. Ajzen, I.: Theory of Planned Behavior. Organ. Behav. Hum. 50, 179–211 (1991)
23. Cronan, T.P., Leonard, L.N.K., Kreie, J.: An empirical validation of perceived importance and behaviour intentions in IT ethics. J. Bus. Ethics 56(3), 231–238 (2005)

24. Gopal, R.D., Sanders, G.L.: International software piracy: Analysis of key issues and impacts. Inform. Syst. Res. 9(4), 380–397 (1998)
25. Mishra, A., Akman, I., Yazici, A.: Software piracy among IT professionals in organizations. Int. J. Inform. Manage. 26(5), 401–413 (2006)
26. Bhattacharjee, S., Gopal, R.D., Sanders, G.L.: Digital music and online sharing: Software piracy 2.0? ACM Commun. 46(7), 107–111 (2003)
27. Cronan, T.P., Foltz, C.B., Jones, T.W.: Piracy, computer crime, and IS misuse at the University. ACM Commun. 49(6), 85–90 (2006)
28. Bachmann, M.: Lesson spurned? Reactions of online music pirates to legal prosecutions by the RIAA. Int. J. Cyber. Criminol. 1(2), 213–277 (2007)
29. Seale, D.A., Polakowski, M., Schneider, S.: It's not really theft!: Personal and workplace ethics that enable software piracy. Behav. Inform. Technol. 17(1), 27–40 (1998)
30. Kwong, K.K., Yau, O.H.M., Lee, J.S.Y., Sin, L.Y.M., Tse, A.C.B.: The effects of attitudinal and demographic factors on intention to buy pirated CDs: The case of Chinese consumers. J. Bus. Ethics 47(3), 223–235 (2003)
31. Masrom, M., Ismail, Z., Hussein, R.: Ethical awareness of computer use among undergraduate students. ACM SIGCAS Comput. Soc. 39(1), 27–40 (2009)
32. Cronan, T.P., Al-Rafee, S.: Factors that influence the intention to pirate software and media. J. Bus. Ethics 78(4), 527–545 (2008)
33. Al-Rafee, S., Cronan, T.P.: Digital piracy: Factors that influence attitude toward behavior. J. Bus. Ethics 63(3), 237–259 (2006)
34. Hsu, J.L., Shiue, C.W.: Consumers' willingness to pay for non-pirated software. J.Bus. Ethics 81(4), 715–732 (2008)
35. Moores, T.T., Dhaliwal, J.: A reversed context analysis of software piracy issues in Singapore. Inform. & Manage. 41(8), 1037–1042 (2004)
36. Cheng, H.K., Sims, R.R., Teegen, H.: To purchase or to pirate software: An empirical study. J. Manage. Inform. Syst. 13(4), 49–60 (1997)
37. Miyazaki, A.D., Rodriguez, A.A., Langenderfer, J.: Price, scarcity, and consumer willingness to purchase pirated media products. J. Public Policy Mark. 28(1), 71–84 (2009)
38. Rahim, M.M., Seyal, A.H., Rahman, M.N.: Factors affecting softlifting intentions of computing students: An empirical study. J. Educ. Comput. Res. 24(4), 385–405 (2001)
39. Liang, Z., Yan, Z.: Software piracy among College students: A comprehensive review of contributing factors, underlying processes and tackling strategies. J. Educ. Comput. Res. 33(2), 115–140 (2005)
40. Rahim, M.M., Seyal, A.H., Rahman, M.N.A.: Software piracy among computing students: a Bruneian scenario. Comput. Educ. 32(4), 301–321 (1999)
41. Coyle, J.R., Gould, S.J., Gupta, R.: "To buy or to pirate": The matrix of music consumers' acquisition-mode. J. Bus. Res. 62(10), 1031–1037 (2009)
42. Wong, G., Kong, A., Ngai, S.: A study of unauthorized software copying among post-secondary students in Hong Kong. Aust. Comput. J. 22(4), 114–122 (1990)
43. Kini, R.B., Ramakrishna, H.V., Vijayaraman, B.S.: An exploratory study of moral intensity regarding software piracy in Thailand. Behav. Inform. Technol. 22(1), 63–70 (2003)
44. Malin, J., Fowers, B.J.: Adolescent self-control and music and movie piracy. Comput. Hum. Behav. 25(3), 718–722 (2009)
45. Seyal, A.H., Rahman, M.N.: Student use of the Internet: An extension of TAM in technical and vocational institutions in Brunei Darussalam. Aust. J. Inform. Syst. 10(2), 91–104 (2003)
46. Peace, A., Gallette, D., Thong, J.Y.L.: Software piracy in the workplace: A model and empirical test. J. Manage. Inform. Syst. 20(1), 153–177 (2003)
47. Limayem, M.L., Khalifa, M., Chin, W.W.: Factors motivating software piracy: A longitudinal study. IEEE T. Eng. Manage. 51(4), 414–425 (2004)

ICT Governance versus Community Empowerment: Grassroots Evidence from Bangladesh

Mizanur Rahman

Development Research Network, Bangladesh,
6/8 Humayun Road, Block B, Mohammadpur, Dhaka 1207, Bangladesh
mizanur.rahman@dnet.org.bd

Abstract. Information and Communication Technologies (ICT) is a catalyst to enhance the level of community empowerment – with this motivation, this paper reports on a research study on "Community Empowerment Through ICTs: Evidence from Grassroots in Bangladesh and India". The evidence from an early benchmark study from Bangladesh shows that ICT penetration on its own is not proportionately related with community empowerment. Rather, ICT penetration with a precise application of ICT governance, strengthens community empowerment. The evidence also shows that if ICT penetration is high, but ICT governance is low, ICT does not remain as high a catalytic factor for community empowerment.

Keywords: ICT Governance, ICT Penetration, Ethics of Computing, Community Empowerment, Bangladesh, New and Traditional ICT, Local Government.

1 Introduction

Year after year, the global budget for information and communication technologies (ICT) penetration is increasing, with a maximisation of multi-dimensional benefits that result from the use of various ICT resources. ICT is used as a catalyst to minimise the activation time towards the community, improving individual development, and hence, strengthening community empowerment. The new ruling political party of the Bangladesh government[1] is also committed to establish "Digital Bangladesh" by the end of 2021. With this global trend, the Bangladesh government also has been increasing its national budget on ICT year after year on the basis of the notion that it will enhance community empowerment, accelerate the establishment rate of the Millennium Development Goals, and eventually eradicate poverty. Under-developed and developing countries have been travelling the same route. Therefore it is very significant to figure out whether there is any correlation between ICT and community empowerment. The Development Research Network (D.Net)[2] has started a new research

[1] Centre-left Awami League.

[2] D.Net is a premier research institution in Bangladesh which is very popular for its Pallitathya Model, a realistic telecentre paradigm that includes infomediary, info-lady and mobile-lady models.

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 33–50, 2010.

study with the title of "Community Empowerment Through ICTs: Evidence from Grassroots in Bangladesh and India" which is funded by the IdeaCorp[3] and reports to the IDRC[4] over a duration of two years. This paper shows the analytical consequences, with raw research evidence which has been drawn from the benchmarking study in Bangladesh, in relation with ICT penetration, governance and community empowerment.

2 Literature Review

The standard of ICT governance is now an integral part of the successful operation of all organisations, whether public or private, for profit or not-for-profit, and large or small. One of its important goals is to create a common platform so that all parties understand their responsibilities and obligations [1]. Within the last decade, many public sector strategists have acknowledged the strategic value of e-technology. They also recognise the need for the improved efficiency of business processes, enhanced citizens' access to information and services, and productive relationships with citizens and private sector agencies alike. Consequently, many innovative public sector agencies worldwide (in e.g. Australia, Canada, Hong Kong, New Zealand, Singapore, the United Kingdom (UK), among many others) have had to create new ways in which to use e-business and e-service solutions[5] so as to respond to the need for change [5].

Governance is a system of power within and by which organisations and other entities are controlled and directed, whereas "corporate governance" is the wealth creation and distribution system of such power. It concerns a whole host of issues surrounding and emanating from the requirement of management to ensure that an organisation or organisational units are efficient and effective in carrying out their proper functions [2, 8]. Local, regional and national governments throughout the world are attempting to broaden service delivery and citizen involvement by providing effective e-services. e-Technology has become a catalyst for enabling more effective government through better access to services and the democratic process. As public interest in the internet and e-technology solutions continues to grow, there is an increasing expectation that these solutions will be used in national and local governments for not only more efficient governance, but also to improve public access to information and services [4].

e-Government has been a priority for administration, with expectation of gains in services to citizens and performance of government processes which have acted as strong drivers for significant investments, focused managerial and political actions, and which have led to new services for corporations and citizens' live-events. These highly visible front-end interfaces require the support of effective and integrated back-office process and informed management. Therefore e-government management has to be

[3] IdeaCorp is an independent, non-profit organization in the Philippines that is devoted to research, training, and advocacy on development issues, particularly on the use of ICT for development (ICT4D).

[4] The International Research Development Centre (IDRC) is a Canadian Crown corporation that works in close collaboration with researchers from the developing world in their search for the means to build healthier, more equitable, and more prosperous societies.

[5] Known as electronic or digital government.

considered in the context of the agency's global ICT activities. The relationship between ICT use, growth stages, governance, ICT budget participation, and growth can be used as indirect and robust measures for the effectiveness of ICT governance and as indications to managers of a governance pre-condition for the generation in government [6].

At the beginning of the twenty-first century, the average number of mobile phones per 100 inhabitants in Asia, Africa, Latin America, and the Caribbean has risen by 100-400% in a span of just five years [12]. Using mobile phones was appreciated by rural communities as an easy, fast and convenient way to communicate and get prompt answers to their respective problems. Farmers were more excited about the use of the mobile phone than other forms of ICT. The governance of mobile phones to access information differed from one parish to another. Information on marketing is in high demand (100%) [13]. Accurate and timely market information, particularly of perishable items, can reduce transaction and travel costs significantly. There have been quite a few studies that explored how mobile phones impact the livelihoods of farmers [14]. Studies by de Silva [15] and Ashraf et al. [16] assert that mobile phones can facilitate a greater export orientation in agricultural practices and marketing, potentially bringing higher incomes to rural farmers. Thus ICT penetration is not much more important than how ICT is used by the community people.

Development interventions that have evolved in response to ground requirements have been multi-stakeholder and community-led, and have pursued inclusive and participative approaches: they have been shown to be far more sustainable than others that have been imposed from above. Although these insights are well documented, they are yet to be fully integrated into many large ICT for development (ICT4D) projects and programmes these have tended to focus on the technology rather than on the capacity building and empowerment aspects of the ICT [7]. There is a reasonable volume of literature on the impact of ICT on communities [9, 11].

3 Subject Matter and Conceptual Dimensions

The project "Community Empowerment Through ICTs: Evidence from Grassroots in Bangladesh and India" is an empirical research study. This study is not related with any dimension of action research. To detect the relationship between community empowerment and ICT is the core subject matter of this research study. The impact of ICT penetration at the community level, and its relation with community empowerment, with or without precise ICT governance, is another of the study's focii. ICT governance plays an important role in establishing productive and maximum utilisation of ICT penetration. ICT penetration is not fruitful, without a proper application of ICT governance, in acting as a catalyst for community empowerment. In this study, the Union Parishad[6] is considered as the community. Various types of models of ICT penetration are identified in finalising the appropriate type of community from where the final evidence would be collected to draw the most feasible study outcomes.

[6] The lowest government unit of Bangladesh is known as local government and governs by the Union Parishad Act 2009.

4 Methodology

The entire research study is divided into two major segments. Quantitative and qualitative approaches to data collection have been used during the completed portion of the study.

The first segment consisted of a benchmarking study which was completed by January 2010. The 30 Union Parishads covered by the study have been selected by a comprehensive desk research and direct communication with different government departments, especially the Local Government and Rural Development Ministry of Bangladesh (LGRD), and the Bangladesh Telecentre Network (BTN)[7] which theoretically represents a total around 4,500 Union Parishads in Bangladesh. Participatory Research Appraisal[8] was the methodological research tool during the benchmarking study which consisted of four unstructured interviews[9] and three focal group discussions[10] including Stakeholder Mapping and ICT Mapping. During this study two local Key Informants provided intensively all kinds of local assistance to the researchers.

The second segment of the study will consist of a comprehensive survey at 12 selected Union Parishads out of the 30 Union Parishads. The survey will be conducted twice. The first survey will be completed by May 2010 and then a second survey will be completed by the beginning of 2011. During the survey periods, simultaneous Participatory Research Appraisal will also be conducted so as to draw the final outcomes.

For this paper, we have used raw evidential information from 11 Union Parishads that are involved with different models of ICT penetration. This evidence was collected using Participatory Research Appraisal during the benchmarking study.

5 Theoretical Debate

The depth of the relationship between community empowerment and ICT-based information systems that are available in the community is one of the key investigation agendas of this empirical research. There is no literature available to measure the community empowerment through any unique set of principle-based standards. With this apprehension, the study team revisited the theoretical underpinnings of the debate so as to understand the relationship of ICT with community empowerment. The team discussed the models offered by different stages of community empowerment through ICT which was developed by Daniel Pimienta[11] [18], and the community engagement framework proposed by the Association of Ontario Health Centres [9].

---

[7] The Bangladesh Telecentre Network (BTN) is a coalition of organisations for fostering a telecentre movement in Bangladesh.

[8] Participatory Research Appraisal is distinguished at its best by the use of local graphic representations created by the community that legitimise local knowledge and promote empowerment.

[9] Unstructured interviews: two unstructured interviews were with power in people and other two unstructured interviews were with people not in power.

[10] Focal Group Discussion (FGD): one discussion was with a group of poor people of the community, another was with a group of non-poor people of the community; and the last was with a group of politically influential people in the community.

[11] In 2008, Daniel Pimienta was the ninth Namur Award winner, an award allocated by the International Federation for Information Processing working group on social accountability and computing that is helping to organise this track. See http://www.info.fundp.ac.be/~jbl/IFIP/winners.html/

The team thought that some combination of both would be explored through a new model. The new model articulates that the value of community empowerment is not only due to having access to, and utilisation of, information, rather it is directly and indirectly related with ICT. Therefore the new model has two dimensions:

- Community empowerment through access to, and utilisation of, information which is comprised of seven layers: inform, consult, involve, collaborate, partner, delegate authority, and autonomy and empowerment.
- Community empowerment through ICT which consists of six layers: access, use, technological appropriation, carrier of meaning, social appropriation and empowerment.

When a community reaches the stage of delegating authority due to access to and utilisation of all of their required multi-dimensional information through using ICT, the community crosses the stage of "carrier of meaning" and enters into the stage of "social appropriation". At the stage of social appropriation of ICT, the maximum number of community people doing daily life activities using ICT is reached. This eventually makes the community's people autonomous and then empowered. To achieve community autonomy and empowerment, the practice of using ICT at the social appropriation level is not merely related with either the level of ICT penetration or the percentage of community people who get access to ICT: rather, it is strongly associated with ICT governance. The evidence shows the ICT governance is much more fundamental than ICT penetration for community empowerment and the ethics of the various agents of ICT applications (like InfoLady[12], MobileLady, Infomediary), computing, mobile usage and other resources of ICT.

6 Local Government of Bangladesh: Status of ICT Penetration and Community Empowerment

This section has four parts. These parts outline the basic statistics in relation to Bangladesh's local governments, ICT penetration in the Union Parishads, the status of community empowerment in the Union Parishads, and a comparative study among several of them.

6.1 Basic Statistics of Local Government of Bangladesh

Bangladesh's population is almost evenly distributed throughout its 64 districts except for the three Hill Tracts districts which are rather sparsely inhabited. On average, a district has a population of about 1.8 million, a Thana 230,000, a union 25,000 and a village has 2,000. There are 490 thanas, 4,451 unions and 59,990 villages. The number of households is about 20 million. On average, a household consists of 5.6 persons. There are four metropolitan cities and 119 municipalities in the country.

The level of urbanisation in Bangladesh is low at 20%. This means that 80% of the country's total population of about 120 million lives in rural areas and depends

[12] An informative newspaper article on the first of these three initiatives is described by Davinder Kumar. Two-wheel triumph. The Guardian, 23 November, 2009. See http://www.guardian.co.uk/journalismcompetition/professional-two-wheel-triumph.

primarily on a poorly developed agriculture for livelihood. The annual growth rate of the population has come down to 1.75% with the acceptance of family planning practices rising to 48.7%. The sex ratio is 106 males for every 100 females. The density of population per square kilometre is 800. Some 44.3% of the people are literate: about five million have passed secondary school level and another 1.27 million are graduates. The primary school enrollment rate has risen to 86% and the rate for secondary school enrollment to 33%. According to the 2007 statistics, there are 450,000 internet users in Bangladesh[13].

There are 2,165 telecentres in Bangladesh (see table 1). Among them, the Dhaka division has the highest number with 615 telecentres and Barisal has the lowest at 94 telecentres. The Local Government and Rural Development Ministry has initiated a project for infrastructural capacity-building of the Local Government Unit, the Union Parishad, in collaboration with the United Nations Development Programme (UNDP). Already 30 Union Information Centres[14] have been set up, and more than 100 Union Information Centres are going to be installed in the timeline of 2010-11[15].It has now been established in the mindset of national policy makers and development activities that telecentres have the highest possibility of impact in enhancing community empowerment and hence on eliminating poverty from the community.

Table 1. Division Wise Telecentre Distribution

Division of Bangladesh	Number of Telecentres
Barisal	94
Chittagong	495
Dhaka	615
Khulna	284
Sylhet	127
Rajshahi	549
Total	2165

By the year 2020, each Union Parishad will have one Union Information Centre to ensure the access of information by citizens. Recently, the Bangladesh government has enacted four laws to strengthen the decentralisation of power and authority through local government activities. The Acts are called the Union Parishad Act 2009, Upazilla Parishad Act 2009, City Corporation Act 2009, and Paurashava Act 2009. At the same time, the Right To Information Act 2009 also came into force. There are many provisions relating to ICT among these Acts. The Bangladesh national budget of 2009-10 has also emphasised ICT investments under Private Public Partnership projects.

[13] Bangladesh Bureau of Statistics, http://www.bbs.gov.bd/, and local government division of Bangladesh, http://www.lgd.gov.bd/

[14] The Union Information Centre (UIC) is a Public-Private-People's Partnership (PPPP) model. The PPPP idea comes from the successful Community e-Centre (CeC) experiences.

[15] Bangladesh Telecentre Network, http://www.mission2011.net.bd/

6.2 Status of ICT Penetration in 11 Selected Union Parishads of Bangladesh

In this research study, two types of ICT have been involved: traditional or old ICT like phone, radio, and television, and new ICT such as the computer and internet. To measure the ICT penetration level into the root community in a realistic manner, the types of ICT penetration have been detected initially in conjunction with different models of ICT penetration. The types of ICT penetration and their related models used in this research paper are discussed below:

- **None:** it is really very difficult to find a Union Parishad where there is no existence of traditional ICT. The evidence from the Participatory Research Appraisal shows that this presumption is correctly identified. However, there are a great number of places where there is no existence of new ICT such as computer or internet connectivity; in this study, those types of ICT penetration are considered as None).
- **Only Community:** there are many Union Parishads or communities where there is the presence of various types of traditional and new ICT but ICT does not exist at the local government premises. Different kinds of model of ICT penetration also have been detected: a few communities have only ICT but no telecentre, a few communities have a telecentre but no ICT, and a few communities have both a telecentre and ICT.
- **Only Local Government:** there are many Union Parishads or communities where there is no existence of new ICT at the community level, whereas local government possesses new ICT. Under this type of model, there are also a few local governments which have only ICT but no telecentre or Union Information Centre, a few local governments have only a telecentre but no other ICT at any branch of the office, and a few local governments have both ICT at the office as well as at the telecentre.
- **Both in Local Governments and Communities:** there are also a few Union Parishads where new ICT is located at both the community and the local government level including different models of ICT penetration and accessibility.

As Figure 1 shows, there are few Union Parishads where there is the presence of new ICT at local government and community level but no telecentre, a few Union Parishads have new ICT and a telecentre at the local government level and only new ICT at community level but no telecentre, and few Union Parishads have only new ICT at the local government level but no telecentre. At the community level, the presence of new ICT and a telecentre is very sound. This is the most ICT-penetrated form of community where generally all types of ICT resources are available.

The ICT penetration level has been divided into two broad categories. One is a private place of ICT penetration where only the household and individual access is guaranteed and public access is denied; the second is a public place of ICT penetration where public access is welcomed and which has more comparative impacts over the community empowerment. The evidence in Figure 1 shows that ICT penetration in

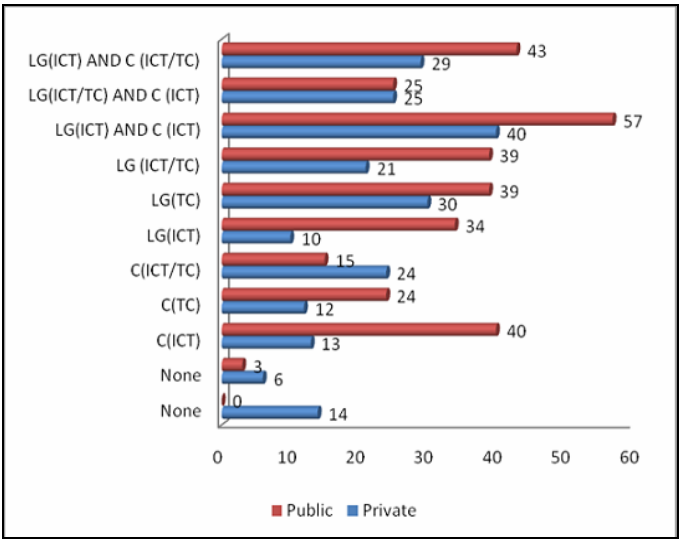


Fig. 1. ICT Penetration in 11 selected Union Parishads

public places is more than in private places. There are few Union Parishads where ICTs penetration in a public place is zero. The Union Parishads where the community has only new ICT and a telecentre have good ICT penetration. Generally, in Union Parishads, where new ICT penetration is high at both local government and community levels, new ICT penetration occurs more in the public places than private places. This indicates that new ICT are not yet cost-effective and cost-friendly for the poor citizens of Bangladesh.

Table 2 shows the ICT penetration score in Hathazari Union Parishad which is located at Chittagong division: there, possession of old ICT is remarkable. The evidence shows that 90% of households use phones whereas only 10% use the internet on their mobile. Among the public places where any person from the community has access to the ICT, 95% possess a phone but no public place uses the internet connection in it; 40% of public places use a computer whereas only 20% use internet in it.

The evidence also shows that 80% of public places use a television, which is 5% more than exists in private possession as a catalytic factor to maximise business outcomes. In this ICT penetration score, the weight of private access is given less concentration than the weight of public access. This is because private access to ICT is only concerned with individual empowerment, whereas public access to ICT is associated with community empowerment due to the accessibility of a large percentage of the population at a point that can enhance mass communication. Table 3 also shows all the scores of ICT penetration together. The status of the ICT penetration is detected by the relative scoring system: 0 to 15 indicates Low, 16 to 30 indicates Medium and above 30 indicates high status.

Table 2. ICT Penetration Score of Hathazari Union Parishad, Chittagong, Bangladesh

LG(ICT) AND C (ICT) : Hathazari Union Parishad, Hathazari, Chittagong						
ICT Penetration Scoring						
	Private Access weight	Percentage of penetration at household level	Weighted Average	Public Access Weight	Percentage of penetration (public places)	Weighted Average
Radio	10	60%	6	10	80%	8
Television	20	75%	15	20	80%	16
Phone (without Internet connection)	15	90%	14	20	95%	19
Computer (without Internet connection)	15	20%	3	20	40%	8
Mobile Phone (with Internet connection)	20	10%	2	0	0%	0
Computer (with Internet connection)	20	1%	0	30	20%	6
Total	100		39.7	100		57
Weight for Private Access			35%			65%
Overall Weight	50.95					

6.3 Status of Community Empowerment in 11 Selected Union Parishads of Bangladesh

To measure the eight components of community empowerment, questionnaires have been designed in relation with the core objectives of the research. The scoring rule for Community Empowerment is crucial to the observation of the differences of empowerment status between communities (table 3). The status of community empowerment in 11 of the country's Union Parishads is shown in appendix 1.A and 1.B.

Table 3. Scoring Guideline of Community Empowerment

Stages of Community Empowerment	Scoring points
Autonomy & empowerment	91 to 100
Delegate Authority	81 to 90
Partner	71 to 80
Collaborate	61 to 70
Involve	41 to 60
Consult	21 to 40
Inform	1 to 20

Seven stages of community empowerment are totally absent. Those components are described below in brief:

- **Participatory Democracy Vs ICT:** is intended to measure the appreciation level of participatory democracy in the community and the impact of ICT over it. Appendix 1.A and 1.B show Fathepur Union Parishad, where local government has new ICT and the community has new ICT as well as a telecentre. PurbaCharbata Union Parishad (where local government has new ICT including a telecentre but there is no existence of new ICT at the community level) has the highest score of 35. This indicates that both Union Parishads are at the "Consult" stage of community empowerment.
- **Rights-based Knowledge Vs ICT:** is intended to measure the people's knowledge of their entitlements and the exercise of their rights, and the role of ICT over this. Hathazari Union Parishad[16], where local government and the community both have new ICT, scored 45: this expresses the "Involve" stage of community empowerment. Balukhali Union Parishad, where there is no presence of new ICT, scored only 20 which indicates the "Inform" stage of community empowerment.
- **Social Violation Vs ICT:** is intended to identify the depth of social violation and how ICT affects these issues. Kohalong Union Parishad, where there is no new ICT, has scored only 15. This means that this community is still at the "Inform" stage of community empowerment. PurbaBirgong Union Parishad, where there is no presence of new ICT but there is a telecentre in the community and no ICT at the local government level, scored 30. Two other locations where ICT penetration is high at both the community and the local government level – like the Hathazari Union Parishad and the Shapara Union Parishad – indicate that they are at the "Consult" stage of community empowerment.
- **Community Involvement Vs ICT:** is intended to measure the community involvement in the roles and responsibilities of the local government and the role of ICT in this. The Nila Union Parishad, where only the community has new ICT, has a score of 25 which indicates the "Consult" stage of community empowerment. It therefore has the same status as the Shapara Union Parishad which is a highly ICT-penetrated community at both the community and local government premises.
- **Knowledge of Community Vs ICT:** to measure the level of the knowledge of the community people about the local, national and international issues and the role of ICT in this. Kohalong Union Parishad , with a very low level of ICT penetration, has scored 35: this indicates a "Consult" stage of community empowerment. The Shapara Union Parishad, with a high ICT penetration, has scored below the Kohalong Union Parishad .The Hathazari Union Parishad, with the highest ICT penetration, has the same empowerment status as Kohalong Union Parishad.

[16] This is the place where of the first Micro Credit revolution started under the initiative of Muhammed Yunus. More than 80% of women from the poor community are involved in it. There is also evidence that women obtain Micro Credit to start computer shops in public places where people can use computers in the presence of other family members in a group.

- **Resource Mobilization Vs ICT:** to measure the community involvement towards the annual activity plan and resource mobilisation plan of the Local government and the role of ICT in it. A highly ICT-penetrated area like Shapara Union Parishad has the same status of empowerment as a poorly ICT-penetrated area like Joyga Union Parishad.
- **Good Governance Vs ICT:** to measure the transparency and accountability of Local Government towards the community and the role of ICT in it. A highly ICT-penetrated Union Parishad, like Hathazari, has the same status of empowerment as a poorly ICT-penetrated area, like Nila Union Parishad.
- **Public and Private Collaboration Vs ICT:** to measure the presence of the collaboration between the local government institution and local community organisation regarding access to information through ICT. Basically this indicator focuses on the presence of the telecentre. If a telecentre exists in the local government, the indicator assumes that it can have the highest impact over empowerment due to the people of the Union Parishad having mass access to their required information easily and in a friendly environment; therefore its weight is the highest at 80. Only two Union Parishads have a telecentre that maximises the e-services to the citizens of the community. If the telecentre exists in the community only, it presumes that it also has impact over community empowerment, but the impact is not higher than that of the local government telecentre due to public accessibility and cost efficiency.

6.4 Comparative Study of Status of Community Empowerment in 11 Selected Union Parishads of Bangladesh

This last section explores a number of basic comparisons among Union Parishads and the need for proper ICT governance.

6.4.1 Basic Comparisons

Early evidence collected during the benchmarking study produced the following general outcomes (which are outlined in Appendix 2):

- Where ICT penetration is low, the overall status of empowerment is at the "Inform" stage.
- Where ICT penetration is only at the community level, the overall status of the empowerment is at the "Consult" stage.
- Where the ICT penetration level is only at the local government, and there is no presence of new ICT at the community level, the overall status of empowerment is at the "Consult" level like the overall empowerment status of an ICT-penetrated community. One exception is the Purba Charbata Union Parishad where the overall empowerment status is at the "Involve" stage.
- Where ICT penetration level is high at both local government and community level, the overall community empowerment is at the "Consult" level like the empowerment status of an ICT-penetrated local government and community separately.

6.4.2 Need to Apply Proper ICT Governance

Evidence shows that the level of ICT penetration is not proportionally related to community empowerment. High ICT-penetrated Union Parishads do not have a higher status of empowerment. With either community or local government-penetrated levels, a Union Parishad has the same empowerment status as a high-penetrated area. At the same time, evidence indicates that traditional ICT-penetrated Union Parishads have a lower status of empowerment.

In comparison with other ICT-penetrated Union Parishads, ICT has a very positive impact on overall empowerment status. During the benchmarking study, it has also been noted that ICT-penetrated areas have been facing very serious crises due to them not having applied proper ICT governance. In the maximum ICT-penetrated areas, there are many traditional and new ICT resources but none where there is a proper application of ICT governance.

7 Findings

Early findings from the benchmarking study are outlined below:

- In the Participatory Democracy Vs ICT component of the empowerment measurement, it is noticed that people highly appreciated ICT over the dialogue correspondence of elections. Figure 2 (which follows) shows that this applies to 20% people in Hathazari, which is a highly ICT-penetrated Union Parishad; the lowest score is 1.5% at Kohalong, which is most poorly ICT-penetrated Union Parishad. It also is also important to note that an informed decision-making process, sound pluralism, and other important features of participatory democracy, is not yet exercised through ICT. No single Union Parishad informs its final decisions through ICT.
- In the Good Governance Vs ICTs component of community empowerment, evidence shows that only 7% of people are being informed about the annual budget of the local government in Joyga Union Parishad, which is the only community to have new ICT and a telecentre. In BaluKhali Union Parishad only 0.5% of people are being informed about annual plan of the local government: in this Union Parishad, there is no presence of new ICT either at local government of community levels. It is also very important to note the percentage of people who use ICT to correspond about the annual budget of the local government, a maximum proportion of them are related with the leading political party. Therefore, this is potentially a threat to community empowerment.
- In the Community Involvement Vs ICT component of the community empowerment measurement, evidence shows that only 3% people in Kholang Union Parishad, where there is no presence of new ICT and a telecentre, use ICT to know about the Social Safety Net Programme, which is run by the local government and is a part of Annual Development Programme nationwide. In Hathazari Union Parishad, 5% of people correspond about the Social Safety Net Programme through ICT. The alarming point is that only those people who are directly and indirectly related with the leading political party use ICT to have communication on the Social Safety Net Programme.

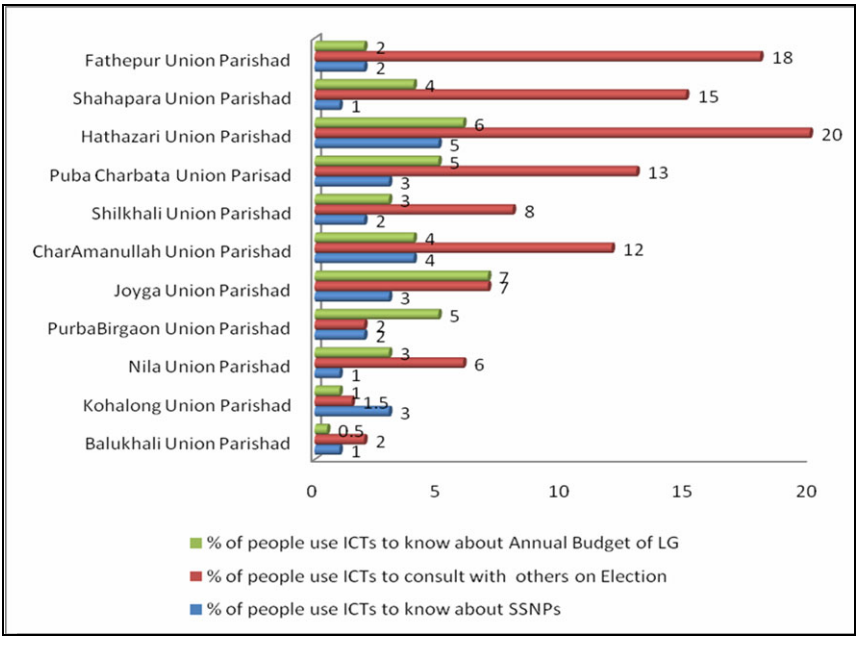


Fig. 2. ICT penetration and its role over community

- Where there is a telecentre, the following problems are detected from voices at the grassroots:
  - The local non-government organisations use the telecentre to promote their activities towards the national and international funding organisations.
  - Infomediary or Mobile-Lady or Info-Lady does not work due to a lack of financial supply.
  - ICT Governance for the telecentre is not maintained by the Infomediary or Mobile-Lady or Info-Lady. In a few cases, ICT Governance for the telecentre is not realistic enough to influence the work of the Infomediary.
- In general, around 85% of people inclusively use traditional ICT to communicate with their relatives, and to maintain domestic relationships. More than 90% of political people use traditional ICT to gain their personal political goals, and around 90% of businesses use traditional ICT to maintain their business activities.
- Evidence from the benchmarking study shows that there is a good relationship between ICT penetration and ICT governance towards the community empowerment. Table 4 shows that where ICT penetration and ICT governance is high, the status of community empowerment is high. Where ICT penetration and ICT governance is low, the status of community empowerment is low. The evidence directly shows that community empowerment is more related with ICT governance rather than ICT penetration.

Table 4. ICT Penetration, Governance and Community Empowerment

ICT Penetration	ICT Governance	Community Empowerment
High	High	High
High	Low	Low
Low	Low	Low
Low	High	High

- There is also evidence of a strong link between the ethics of computing and ICT penetration towards community empowerment. Table 5 (below) shows that, if ICT penetration and ethics of computing is high, the community has a raised level of empowerment. If ICT penetration and the ethics of computing is low then the community has a low status of empowerment. If ICT penetration is low but ethics of computing is high, then the community has the status of raising empowerment.
- In the case of the Union Information Centre, there is no presence of ICT governance. It may be there on paper, but not in application.

Table 5. ICT Penetration, Ethics of computing and Community Empowerment

ICT Penetration	Ethics of Computing	Community Empowerment
High	High	Raised Empowerment
High	Low	Disempowerment
Low	Low	Low Empowerment
Low	High	Raising Empowerment

8 Conclusions

Evidence from the benchmarking study initially shows why ICT governance and the ethics of computing are necessary to functionalise ICT penetration effectively and efficiently towards community empowerment. Observations include the a) lack of establishment of having clearly understood responsibilities for ICT at all levels; b) lack of having a plan to best support the local government and telecentre where, organisationally, ICT penetration is high; c) lack of acquiring ICT validly through evaluating the risks of the investment, making sure that it adds value, and monitoring the extent to which it performs as proposed; d) lack of the quality of ICT required to supply adequate data quality, security, privacy; e) lack of ICT performance when it is required; f) lack of usage of ICT without disrespecting human factors; g) lack of measurement of status of the ethics of computing as well as mobile usage. All these limitations show the lack of efficient ICT governance and the establishment of an ethics of computing and mobile usage. The evidence also shows that when ICT penetration is high, but with a low level of application of ICT governance, the status of empowerment is lower. When ICT penetration is high with a high level of application of ICT governance, the status of empowerment is higher.

References

1. Feld, C.S., Stoddard, D.B.: Fixing the Corporation-IT. In: Disconnect, Working Knowledge, Harvard Business School Newsletter, Harvard Management Communication letter (Online): A Newsletter from Harvard Business School Publishing. Harvard Business School Publishing, Boston
2. Ziolkowski, R., Clark, E.: Standards of ICT Governance: The Need for Stronger Epistemological Foundations in Shifting Sands. The Asia Pacific Journal of Public Administration 26(1), 77–90 (2005)
3. Taifur, S., Chowdhury, M.: Problems of E-Governance in Bangladesh and Possible Steps Towards Solutions. In: Seminar Paper: Road Map for ICT Development in Bangladesh, IDB Bhaban (2003)
4. Asgarkhani, M.: The Effectiveness of e-Service in Local Government: A Case Study. The Electronic Journal of e-Government 3(4), 157–166 (2005), http://www.ejeg.com
5. Heeks, R.: Software Strategies in Developing Countries. Development Informatics Working Paper Series, Paper No. 6. Institute for Development Policy and Management (June 1999)
6. Reinhard, N., Sun, V., Meizi, R.: ICT Spending and Governance in Brazilian Public Administration. In: 19th Bled eConference, Slovenia (2006)
7. Gurumurthy, A.: Promoting gender equality? Some development-related uses of ICTs by women, Development in Practice (2006)
8. Mingers, J., Wilkocks, L. (eds.): Social Theory and Philosophy for Information Systems. John Wiley & Sons, West Sussex (2004)
9. AOCH: A Review of the Trends and Benefits of Community Engagement and Local Community Governance in Health Care, prepared by Ktpatzer Consulting, Community Centered Primary Health Care, Ontario, Canada (2006)
10. Khelladi, Y.: The Infocentros Telecentre Model. World Resources Institute, Washington (2001)
11. Raihan, A., Mahmud, H., Uddin, F., Billah, M., Das, N., Sarker, T.: Pallitathya: An Information and Knowledge System for the Poor and Marginalized Experience from Grassroots in Bangladesh, D.Net, Dhaka (2007)
12. Orbicom: Emerging Development Opportunities: The Making of Information Societies and ICT Markets. IDRC, Ottawa (2007)
13. Masuki, K.F.G., Kamugisha, R., Mowo, J.G., Tanui, J., Tukahirwa, J., Mogoi, J., Adera, E.O.: Role of mobile phones in improving communication and information delivery for agricultural development: Lessons from South Western Uganda. In: Workshop at Makerere University, Uganda, March 22-23 (2010)
14. Rashid, A.T., Elder, L.: Mobile Phones and Development: An Analysis of IDARC-Supported Projects. The Electronic Journal on Information Systems in Developing Countries (EJISDC) 36(2), 1–16 (2009)
15. De Silva, H.: Using ICTs to Create Efficiencies in Agricultural Markets: Some Findings from Sri Lanka. Paper Presented to IDRC, Ottawa (2008)
16. Ashraf, N., Gine, X., Karlan, D.: Growing Export Oriented Crops in Kenya: An Evaluation of DrumNet Services. IDRC, Ottawa (2005)
17. CEMP Project (Community Empowerment through ICTs: Grassroots Evidence from Bangladesh and India), D.Net (Development Research Network), Bangladesh (2009-2010)
18. Pimienta, D.: Linguistic Diversity in Cyberspace – Models for Development and Measurement. In: Measuring Linguistic Diversity on the Internet, UNESCO, Paris (2005)

Appendix 1.A: Status of Community Empowerment

Model	LG(TC)	LG (ICT/TC)	LG(ICT) AND C (ICT)	LG(ICT/TC) AND C (ICT)	LG(ICT) AND C (ICT/TC)
Name of the PRA component	**Shilkhali UP, Cox's Bazar**	**Puba Charbata UP, Noakhali**	**Hathazari UP, Chittagogn**	**Shahapara UP, Gaibandha**	**Fathepur UP, Jhenaidha**
Participatory Democracy Vs ICT	30	35.00	30	28	35
Rights-based Knowledge Vs ICT	25	30.00	45	26	41
Social Violation Vs ICT	30	50.00	30	30	40
Community Involvement Vs ICT	20	50.00	35	24	35
Knowledge of Community Vs ICT	30	30.00	35	30	50
Resource Mobilization Vs ICT	20	45.00	30	26	30
Good Governance Vs ICT	10	25.00	25	20	25
Public and Private Collaboration Vs ICT	80	80.00	0	80	50
Total Score	245	345.00	230	264	306
Average Score	30.625	43.125	28.75	33	38.25
Empowerment Level	Medium	Medium	Low	Medium	Medium

Source: D.Net [17].

Appendix 1.B: Status of Community Empowerment

Model	None	None	C(ICT)	C(TC)	C(ICT/TC)	LG(ICT)
Name of the PRA component	**Kohalong UP, Bandarban**	**Balukhali UP, Rangamati**	**Nila UP, Cox Bazar**	**PurbaBirgaon UP, Daskhin Sunamgonj**	**Joyga UP, Noakhali**	**CharAmanullah UP, Noakhali**
Participatory Democracy Vs ICT	20	15	30	25	32	25.00
Rights-based Knowledge Vs ICT	30	20	25	30	30	30.00
Social Violation Vs ICT	15	10	20	30	35	25.00
Community Involvement Vs ICT	15	10	25	25	32	20.00
Knowledge of Community Vs ICT	35	25	50	20	35	25.00
Resource Mobilization Vs ICT	15	15	25	25	25	20.00
Good Governance Vs ICT	15	15	25	20	34	25.00
Public and Private Collaboration Vs ICT	0	0	0	50	50	0.00
Total Score	145	110	200	225	273	170.00
Average Score	18.125	13.75	25	28.125	34.125	21.25
Empowerment Level	Low	Low	Low	Low	Medium	Low

Source: D.Net [17].

Appendix 2: ICT Penetration and Empowerment Status

Type of ICT penetration	Model of ICT	Location of PRA	Private %	Public %	Average %	Status	Empower-ment %	Status
None	None	Balukhali UP, Rangamati	14	0	5	Low	14	Low
		Kohalong UP, Bandarban	6	3	4	Low	18	Low
Community	C(ICT)	Nila UP, Cox Bazar	13	40	30	Low	25	Low
	C(TC)	PurbaBirgaon UP, Daskhin Sunamgonj	12	24	20	Low	28	Low
	C(ICT/TC)	Joyga UP, Noakhali	24	15	18	Low	34	Medium
LG	LG(ICT)	CharAmanullah UP, Noakhali	10	34	26	Low	21	Low
	LG (ICT/TC)	7 no Puba Charbata UP, Noakhali	21	39	33	Medium	43	Medium
	LG(TC)	Shilkhali UP, Cox's Bazar	30	39	36	Medium	31	Medium
LG and Community	LG(ICT) AND C (ICT)	Hathazari UP, Chittagogn	40	57	51	Medium	29	Low
	LG(ICT/TC) AND C (ICT)	Shahapara UP, Gaibandha	25	25	25	Low	33	Medium
	LG(ICT) AND C (ICT/TC)	Fathepur UP, Jhenaidha	29	43	38	Medium	38	Medium

Source: D.Net [17].

Exploring Digital Divide in the Maldives

Mohamed Shareef, Adegboyega Ojo, and Tomasz Janowski

Center for Electronic Governance, United Nations University IIST, P.O. Box 3058, Macao
mohamed@iist.unu.edu, ao@iist.unu.edu, tj@iist.unu.edu

Abstract. The central role of ICT in development and its ethical implications have kept the longstanding discussions of the Digital Divide active in the international development and research communities, with new perspectives on how to measure and interpret this inequality. In this paper, we examine the nature of the Digital Divide in the Maldives – between the nation's capital and the Atolls, between the Atolls and across the nation, and the evolution of these divides over time. In order to inform more effective policy interventions, we also attempt at identifying clusters within the country that share similar Digital Divide concerns. The results show significant disparities in the penetration of digital technologies. While we can observe the narrowing of the Digital Divide over time, the divide remains significant between the capital and the rest of the nation. Finally, we discuss the implications of these results to ICT development of Small Island Developing States.

Keywords: Electronic Government, Digital Divide, Maldives, Small Island Developing States.

1 Introduction

The advent of the Information Age and rapid developments in Information and Communications Technologies (ICT), particularly the Internet, have created new opportunities for the development of societies and nations. However, the dawn of the Information Society, with its ever-increasing interweaving of ICT into daily lives, has also raised the possibility of exaggerating existing social divides, with ethical implications on key human rights (Universal Declaration of Human Rights - UDHR).

The capacity of the Internet to both empower and discriminate was widely recognised in the mid-1990s [9], giving rise and prominence to the issue of Digital Divide [11]. In particular, with the emergence of Electronic Government, with nations and economies around the world embracing ICT as a strategic tool in public sector modernisation, access to information and service delivery, the phenomenon of Digital Divide brings into focus Article 21 of the UDHR which guarantees individuals the right to take part in the governance of their countries and the right of equal access to public services, among others. With the increasing maturity of Electronic Government, the possible consequences of the Digital Divide in exacerbating existing social, political and economic divides between citizens [24, 25] have serious ethical implications for the delivery of basic human rights [22] across the globe and are a constant

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 51–63, 2010.

concern to the international development community, government leaders and ICT policy-makers.

In a recent report on Citizens' Digital Participation [20], the regulator and competition authority for the United Kingdom communications industries, Ofcom, emphasised that while "digital communications have provided new channels for people to interact with democratic institutions and to become engaged in a range of activities associated with citizen participation, they also pose a challenge: a significant section of the population, lacking access to these technologies or the confidence to use them, may become increasingly disengaged". This highlights the relevance and significance of the Digital Divide even in a highly developed country like the United Kingdom.

This paper presents an exploratory study of Digital Divide within the Maldives. It explores the Digital Divide landscape, identifies clusters of ICT penetration in the Maldives, and examines two key development challenges: the country's numerous small island communities and the geographical distribution of these communities across a comparatively vast sea area. The results show large disparities in the penetration of digital technologies, the narrowing of the Digital Divide over time, and a remaining significant divide between the capital and the rest of the nation.

The rest of the paper is structured as follows. Sections 2 and 3 introduce the small island context of the Maldives and the notion of Digital Divide. Section 4 examines the Digital Divide in the Maldives - research questions (Section 4.1), analysis (Section 4.2) and findings (Section 4.3). Section 5 presents some conclusions.

2 Maldives

The Republic of Maldives is a Small Island Developing State composed of 26 natural coral Atolls composed of 1,192 small low-lying islands, less than 200 of which are permanently inhabited. These 29 Atolls are divided for administrative and governance purposes into 20 administrative regions, also called Atolls. The furthest Atoll capital is located over 500 kilometres from Male' – the nation's capital.

A large proportion of these inhabited islands have an area of less than half a square kilometre and only a few are bigger than two square kilometres. These islands are spread over 115,300 square kilometres of the Indian Ocean, some 823 kilometres from the northernmost point to the south and some 130 kilometres east to west. Of the 115,300 square kilometres, only 298 square kilometres (0.26%) is dry land.

The population of the country is distributed unevenly across 194 islands. According to the 2006 Housing and Population Census, of the 194 permanently inhabited islands, only 4 islands have a population of over 5,000, 131 have a population below 1,000, and 72 have a population below 500. Over one-third of the population of Maldives lives on the capital island of 1.93 square kilometres - one of the most densely populated cities in the world. See Figure 1.

The smallness of the islands, the distances between them and the large number of island communities are the key obstacles for the development of the country. Leading to severe diseconomies of scale, they greatly challenge the delivery of basic services. Concerning the penetration of ICT, Figure 2 shows the fast rise in mobile telephony and stagnant penetration by fixed phone lines. Figure 2 also shows that the use of the Internet, while increasing, is still relatively limited.

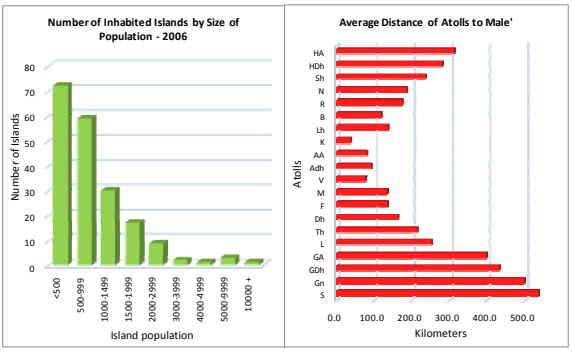


Fig. 1. Geographical and Demographic Distribution of the Maldives [8]

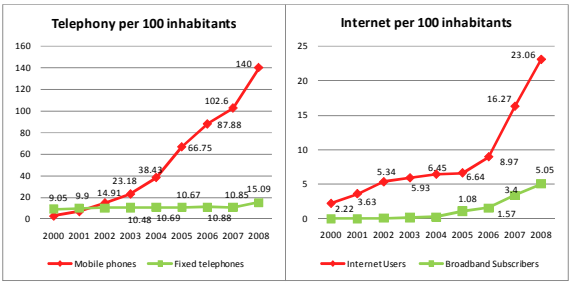


Fig. 2. Growth of Fixed and Mobile Phone Lines [14]

3 Digital Divide

3.1 Defining Digital Divide

A variety of ways have been used to define and characterise the divisions or disparities among people, societies and nations in terms of their associations with ICT, the so-called Digital Divide. In its simplest form, the Digital Divide refers to the gap existing between those with access to ICT and those without, "a new label for a similar concept of the previous generation: information haves and have-nots" [4]. This dichotomous portrayal of information haves and have-nots often refers to the access to and use of ICT [1], for example in terms of the number of phone lines per inhabitant, or the number of Internet users or mobile telephones in the population.

On the other hand, a broader characterisation of Digital Divide is achieved through a multi-dimensional or multi-perspective approach – identifying and using different types of access and measuring different types of divides. Different types of access include [26]: (1) mental access e.g. digital experience, lack of interest or computer anxiety; (2) material access e.g. possession of computers; (3) skills access e.g. user friendliness, education or literacy; and (4) usage access – usage opportunities.

Alternatively, Digital Divide can be characterised in relation to or as a mirror of different types of social disparity. According to [19], Digital Divide encompasses: (1) global divide – divergence of Internet access between industrialised and developing countries; (2) social divide – the gap between information rich and information poor within each country; and (3) democratic divide – differences between those who do and those who do not engage, mobilise and participate in public life through ICT.

Across various definitions and portrayals, Digital Divide has been examined and studied using a variety of factors: technological infrastructure [6, 10], socio-economic development [9, 10, 21], socio-political development [9, 21], legal and regulatory frameworks [3, 9, 10], demography [3, 5], income [3] and culture [18]. The influence of these factors on Digital Divide depends on their evolution over time [9] and the stage of ICT adoption in a country [5].

For the current paper, we adopt the definition of the Digital Divide from [12] – the gap between those who benefit from digital technologies and those who do not.

3.2 Measuring Digital Divide

Given the multifaceted nature of Digital Divide and the fact that it is closely related to and interwoven with various social and human conditions, measuring and quantifying the divide can be also multifaceted.

In its simplest form, Digital Divide can be illustrated by measuring the distribution of ICT across different groups [15], defined based on the factors like age or income. This is a simple way of illustrating the unequal distribution of ICT, and providing a visual representation of the existence of Digital Divide. Another approach is to calculate the ratio of the penetration rates of ICT between groups [13] to identify the gap between groups under analysis, and to track how this gap evolves over time. The gap between groups, expressed as the ratio of ICT penetrations, is a simple quantitative figure representing Digital Divide, showing convergence or divergence of the divide between groups over time. While these approaches capture Digital Divide across groups, they cannot account for many underlying dimensions within the concept [23].

A more rigorous approach to quantifying the disparity or distribution of inequality is to use the Lorenz curve and the Gini coefficient. The Lorenz curve is used to illustrate the distribution or cumulative share of count data across the population, whilst the Gini coefficient summarises the Lorenz curve to a single number representing the degree of inequality within the population. The coefficient varies between 0 and 1, where 0 represents perfect equality and 1 perfect inequality. The Lorenz curve and Gini coefficient provide a good measure of Digital Divide, applied by both research [2, 16] and international development communities [13, 15]. A well-established measure of disparity among groups, it is useful for quantifying Digital Divide across large numbers of entities, and for showing the evolution of the divide over time in terms of changing disparities between groups.

In this paper, we construct the Lorenz curve as a line between consecutive points (Xk, Yk) for the intervals k (k is between 1 and n), and estimate the Gini coefficient by approximating the area under the curve with trapezoids, using the formula:

$$G = \left| 1 - \sum_{k=1}^{n} (X_k - X_{k-1})(Y_k + Y_{k-1}) \right|$$

All methods described above for measuring Digital Divide require defining groups of communities within and between which the measurement of disparity or inequality is carried out. These are often based on the groupings recommended by international organisations like the United Nations or the World Bank, or they are based on existing national or local boundaries, or on factors like demography or race.

This paper applies a different approach. The grouping of people or communities is based on their ICT profiles, using the techniques like the Lorenz curve, Gini coefficient or gap analysis to measure the disparities within and between groups, and ultimately to determine the key determinants of the Digital Divide. This approach not only illustrates and quantifies Digital Divide, but provides a level of support for strategic planning aimed at addressing the divide, based on the clusters of communities which share similar ICT characteristics.

While there are several clustering techniques, we use the Neural Network-Based Clustering method due to its visualisation property. In particular, we use Kohonen's Self Organizing Maps (SOM) [17], a type of artificial neural network that can produce two-dimensional representations of multi-dimensional input spaces, often called maps. Being able to represent groups of communities defined by multiple Digital Divide indicators on a two-dimensional grid helps to identify clusters of entities with similar ICT profiles, and possibly to utilise these clusters to form social infrastructures (e.g. communities of interest) for addressing the Digital Divide.

4 Digital Divide in the Maldives

The Maldives is a country of hundreds of small island communities dispersed over a large space of the Indian Ocean. Its unique geography and demography has had a major effect on the development of individual island communities with respect to each other and especially with respect to the nation's capital Male'.

In this section, we identify these divides with respect to the pervasiveness of personal computers and the use of the Internet and fixed and mobile phones, using the household statistics from the 2000 and 2006 Censuses. The section is structured into research questions (Section 4.1), analysis (Section 4.2) and findings (Section 4.3).

4.1 Research Questions

The primary goal of this work is to understand the nature of the Digital Divide in the Maldives in order to better inform ICT policy formulation and strategic Electronic Governance planning at the national level. Given the Maldives' peculiar geographic and population features, and their influence on the national-level and Atoll-level development, we focus on how such features impact Digital Divide in the country.

Our investigation proceeds in three steps: (1) establish and quantify Digital Divide in the Maldives, (2) measure the significance of the geographic and demographic features of the Maldives to Digital Divide, and (3) examine the dynamics of Digital Divide in the Maldives. These objectives are framed as two research questions below:

How are the Atolls divided with respect to ICT access?

In order to understand the pervasiveness of ICT in the Maldives, establishing the existence and magnitude of Digital Divide is important. Earlier studies of various

disparities in the Maldives tend to compare the haves and have-nots between the capital and the rest of the country, or between individual atolls.

How significant is the geographic and demographic distribution of the Atolls to the Digital Divide?

Establishing the significance of the distance between the Atolls and Male' and between the islands of an Atoll and its capital, to the disparities in access to ICT may inform national-level development strategies particularly to ensure the narrowing of Digital Divide and increasing benefits from information access. At the same time, as large numbers of small island communities give rise to diseconomies of scale, determining the significance of this feature on ICT diffusion can support better planning for community development and population consolidation. In particular, we investigate Digital Divide with respect to: (1) the average distance of the Atolls to Male' and (2) the number of islands with less than 500 people in an Atoll. These variables capture two key geographic and demographic dispersion characteristics of the nation.

In this work we use access to ICT as primary indicator of Digital Divide, with data on ICT penetration from the 2000 and 2006 Household and Population Census of the Maldives [6, 7] which form the primary data used in this analysis.

4.2 Analysis

Led by these two research questions, this section documents the analysis of Digital Divide in the Maldives. Section 4.2.1 examines the divide between the capital and the Atolls, Section 4.2.2 examines the divide across the Maldives, and Section 4.2.3 examines the divide between Atolls. Finally, Section 4.2.4 examines the significance of the country's geographic and demographic features on the divide.

4.2.1 Digital Divide between Male' and the Atolls

Digital Divide has many facets and can be assessed in many ways. This section illustrates the Digital Divide between the nation's capital and the Atolls, using the distribution of ICT between these two groups. It also examines the evolution of the divide by using penetration ratios.

The distribution of ICT based on the number of households in Male' and the number of households in the rest of the country is shown in Figure 3. As is evident from this illustration, mobile phones and televisions (TVs) are the most evenly distributed: 31% of the households in the country (in Male') have 33% of the mobile phones and 31% of TVs, and 69% of the households (in the Atolls) have 67% of the mobile phones and 69% of the TVs. In contrast, the distribution of fixed lines, personal computers and particularly residential Internet connections clearly distinguishes the capital Male' from the rest of the country (i.e. Atolls): 31% of the households (in Male') have 59% of the fixed line phones, 61% of the computers and 78% of residential Internet connections. Clearly, Digital Divide is severe with respect to Internet access, with 31% of the households (in Male') having 78% of the household Internet connections.

Given a clear divide between Male' and the Atolls, we now investigate the evolution of this divide using census data from 2000 and 2006. While the divide is most prominent with respect to Internet pervasiveness, the data on household Internet was

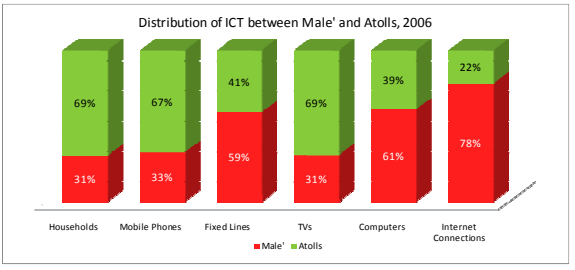


Fig. 3. Distribution of ICT based on the numbers of households in Male' and the Atolls, 2006

not collected during the 2000 Census, so we can only analyse penetration of computers and fixed phone lines. To this end, we use the ratio of penetration as a measure of the divide (or gap) between Male' and the Atolls.

Figure 4 shows the progression of the divide between Male' and the Atolls with respect to the percentages of households with computers (left) and fixed phone lines (right) for 2000 and 2006. The divide, measured as the ratio of the penetration rates, shows that while the absolute difference between percentages of the households with personal computers has increased from 2000 to 2006, the divide between Male' and the rest of the Atolls has actually decreased from 16.8 to 3.6. With respect to fixed phone lines, not only has the gap decreased but the absolute difference did so as well, clearly indicating the narrowing of the divide between Male' and the Atolls between 2000 to 2006.

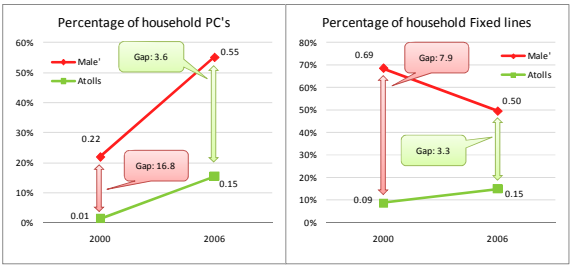


Fig. 4. Evolution of the Digital Divide between Male' and Atolls with respect to Personal Computer and Fixed Line penetration

4.2.2 The Digital Divide across the Maldives

We now investigate Digital Divide across the Maldives. We employ Lorenz curves and Gini coefficients to quantify the disparity across the twenty Atolls plus the capital based on their household ICT penetration, i.e. treating the country as 21 groups defined by numbers of households and household ICT penetrations.

The Lorenz curves for Internet connections, personal computers, and fixed and mobile phones are shown in Figure 5, with Gini coefficients corresponding to these curves summarised in Table 1. From Figure 5 and Table 1 it is evident that the

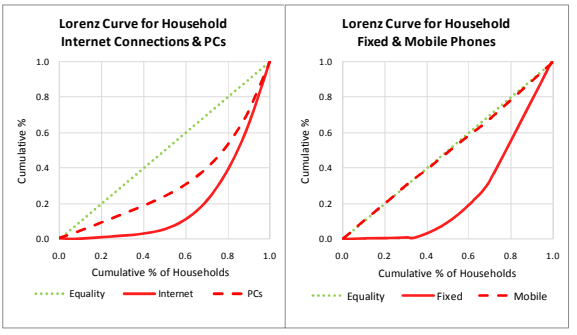


Fig. 5. Lorenz Curves for Household ICT Penetration in the Maldives, 2006

Table 1. Gini Coefficients for Household ICT Penetration in the Maldives, 2006

ICT	GINI Coefficient
Internet Connections	0.57
Fixed Line Phones	0.48
Personal Computers	0.34
Mobile Phones	0.02

penetration of the Internet is the most divisive factor across the country, followed by household fixed line telephones and personal computers. It is also clear that there is no Digital Divide with respect to mobile phones. From the Lorenz curves, 60% of the households with the least household ICT access have about 10% of the household Internet connections, 30% of the personal computers and 20% of the fixed phone lines. This demonstrates that large parts of the country have little access to ICT at home, while at the same time the country has equal access to mobile technology.

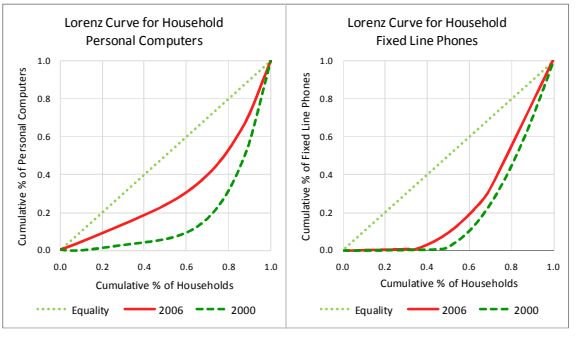


Fig. 6. Evolution of the Digital Divide across the Maldives with respect to PC and Fixed Line penetration

Table 2. Gini Coefficients for Household ICT Penetration in the Maldives, 2000 and 2006

ICT	2000	2006
Personal Computers	0.58	0.34
Fixed Line Phones	0.56	0.48

We now examine the evolution of the divide within the Maldives. In particular, we construct the Lorenz curves and estimate the Gini coefficients for household personal computers and fixed line phones across the country, as shown in Figure 6 and Table 2.

From Figure 6 and Table 2 we can observe that the disparity in the distribution of household personal computers and fixed phone lines across the Maldives has decreased, pointing to a narrowing of the divide across the country. It is interesting to note that the disparity in household fixed phone lines has only decreased by a small factor, in comparison to the household personal computers' penetration. This is consistent with the rapid uptake of mobile technologies in the Maldives and across the world, and the corresponding slowing-down of the fixed phone line penetration in many parts of the world, as highlighted in the World Information Society Report 2007 [15].

4.2.3 Atoll Clusters

In Sections 4.2.1 and 4.2.2 we examined and quantified Digital Divide across the Maldives as well as between the capital Male' and the rest of the country. From this analysis, it is clear that there is a substantial divide between Male' and the Atolls, and substantial disparity in ICT penetration across the country as a whole. This suggests that the Male'-Atolls divide may not be the only substantial Digital Divide in the country, and that there are possible other divides within the group of 20 Atolls.

In this section, we examine Digital Divide using the clustering technique explained in Section 3.2. We employed self-organising, map-based clustering using the household penetration of personal computers and fixed phone lines for 2000 and 2006 as well as Internet connections and mobile phones for 2006, to produce possible clusters of Atolls.

From this analysis, we identified six clusters of Atolls with varying ICT profiles, thus pointing to the possibility of further splits within 20 Atolls. The numbers of Atolls in each of these clusters are given in Table 3, while the 2006 ICT profiles of these clusters are shown in Figure 7. From Figure 7 we can observe the differences in the ICT profiles of these clusters and consequently, their different divide challenges. Clusters A and B have the most developed and similar profiles, but are distinguished by their relative Internet penetration rates. The least developed clusters, E and F, while similar in many aspects, are distinguished by their fixed phone line penetration.

Table 3. Atolls Clusters

Cluster	A	B	C	D	E	F
No of Atolls	1	1	2	5	3	7

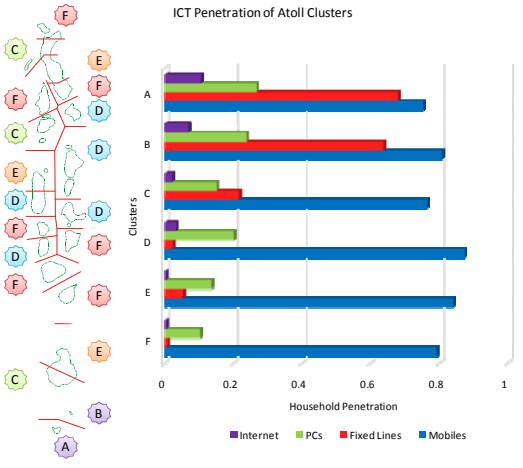


Fig. 7. Clusters and their ICT Profiles

Digital Divide between these clusters in terms of the penetration gap is shown in Figure 8; the cluster with the best penetration is taken as the reference for each ICT measure. The figure makes the divide between Atoll clusters evident. The divide is severe with respect to fixed phone lines and Internet connections while negligible with respect to mobile phones: this is consistent with overall Digital Divide characteristics which were presented in previous sections. This suggests that this clustering retains the main characteristic of the country's Digital Divide.

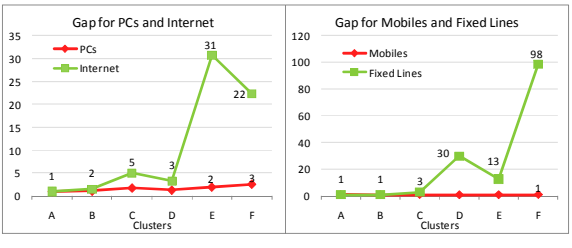


Fig. 8. Digital Divide between the Clusters

4.2.4 Determinants of the Digital Divide

Having explored and quantified Digital Divide across the Maldives, we now examine the possible impact of the country's geographic and demographic features on the divide, particularly on Internet and personal computer penetration. To this end, we investigate the presence of significant relationships between Internet and personal computer penetration, distance of the Atolls from Male', and the numbers of islands in each Atoll with a population below 500.

Table 4 presents the coefficients for the 20 Atolls. From this table, we observe that there is a significant positive correlation between the distance of Atolls from Male'

and their Internet penetration, and a significant negative correlation between the number of small islands in an Atoll and the Internet penetration in the Atoll. While the negative correlation between the number of small islands in an Atoll and their Internet penetration is in line with popular understanding, the positive correlation between the distance of the Atolls from Male' and their Internet penetration is interesting. This could be explained by disproportionate development of the two southernmost Atolls, as identified in our clustering analysis in Section 4.2.3.

Table 4. Relationships between geographic and demographic dispersion and Digital Divide

Feature	Internet	PC	Mobile
Distance from Atolls to Male'	0.5421	0.1868	-0.6060
No. of islands with <500 population in the Atoll	-0.5810	-0.4873	0.02315

Therefore, we examine the correlations between the 18 Atolls, excluding the two southernmost Atolls (clusters A and B). This is presented in Table 5. The table shows that all correlations are negative, in line with popular understanding. However, apart from the correlation between the distance of the Atolls from Male' and the mobile phone penetration, other correlations are not significant. While simple correlation does not establish causality between variables, the apparent lack of significant correlation between Internet and personal computer penetration, and geographic and demographic dispersion, requires further investigation.

Table 5. Relationships between geographic and demographic dispersion and Digital Divide (excluding Clusters A and B)

Feature	Internet	PC	Mobile
Distance from Atolls to Male'	-0.1665	-0.3775	-0.6360
No. of islands with <500 population in the Atoll	-0.3160	-0.2590	-0.1234

4.3 Findings

We illustrated in previous sections the nature of Digital Divide across Maldivian Atolls. We now summarise these findings with respect to our research questions:

How are the Atolls of the Maldives divided with respect to ICT access?

The nation shows wide dispersion in the penetration of household Internet and personal computers. A significant divide exists between the nation's capital Male' and the rest of the Atolls. In addition, significant differences exist among the Atolls as seen from the clustering analysis; six clusters of Atolls with distinctive Digital Divide challenges were identified in our analysis. On the other hand, we found no significant divide with respect to the penetration of mobile telephony across the nation.

How significant is the geographic and demographic distribution of the Atolls to Digital Divide?

While the challenges of geographic and demographic dispersion to national development are fairly well accepted, our analysis found that the relationship between these features and Digital Divide may be less significant. This warrants further investigation of the impact of these factors on Digital Divide, not just from the physical access or possession point of view, but also from the point of view of the usage of and benefit from ICT.

5 Conclusions

The primary aim of the work reported in this paper is to understand the nature of Digital Divide in the small island developing state of the Maldives in order to better inform ICT policy and strategy development at the national level.

In line with this aim, we illustrated and quantified the divide across the country and between the capital and the rest of the country (Atolls). We also applied clustering analysis to obtain a better insight into possible divides between the Atolls. Finally, we investigated the impact on Digital Divide of two of the most significant challenges to national development – the geographic and demographic nature of the island nation.

Our findings indicate the presence of a significant Digital Divide across the country. They also suggest that geographic and demographic features – the distance of the Atolls from Male' and the numbers of small island communities within Atolls, may not be significant with respect to Digital Divide. However, a more thorough analysis is warranted, possibly along the identified Atoll clusters.

Based on the findings, we propose that in addition to more detailed studies of the main determinants of Digital Divide, efficient and purposeful strategies to overcome Digital Divide could be formulated based on Atoll clusters with similar Digital Divide profiles. These strategies could complement national and regional strategies, and rely on knowledge-sharing and collaborative action through communities of interests or other collective measures. In addition we propose that, given the varied nature of Digital Divide across the country, special consideration be given to infoethics to ensure that ICT development impacts positively the development of human rights.

References

1. Campbell, D.: Can the Digital Divide be Contained? International Labour Review 140(2), 119–141 (2001)
2. Chakraborty, J., Bosman, M.M.: Measuring the Digital Divide in the United States: Race, Income, and Personal Computer Ownership. The Professional Geographer 57(3), 395–410 (2005)
3. Chinn, M.D., Fairlie, R.: The Determinants of the Global Digital Divide: Across-Count Analysis of Computer and Internet Penetration. Yale University, Working Papers 881 (2004)
4. Compaine, B.M.: Re-Examining the Digital Divide. Center for eBusiness @ MIT. MIT Sloan School of Management (2001), http://ebusiness.mit.edu/research/papers/130%20Compaine,%20Digital%20Divide.pdf

5. Dewan, S., Ganley, D., Kraemer, K.L.: Across the Digital Divide: A Cross-Country Multi-Technology Analysis of the Determinants of IT Penetration. Journal of the Association for Information Systems 6(12), 409–443 (2005)
6. DNP. Population and Housing Census of Maldives 2000. Department of National Planning, Government of Maldives (2000)
7. DNP. Population and Housing Census of Maldives 2006. Department of National Planning, Government of Maldives (2006).
8. DNP. Statistical Year Book 2007. Department of National Planning, Government of Maldives (2007)
9. Guillén, M.F., Suárez, S.L.: Explaining the Global Digital Divide: Economic, Political, and Sociological Drivers of Cross-National Internet Use. Social Forces 8(2), 681–708 (2005)
10. Hargittai, E.: Weaving the Western Web: Explaining Differences in Internet Connectivity Among OECD Countries. Telecommunications Policy 23(10/11), 701–718 (1999)
11. Hawkins, S.: Beyond the Digital Divide: Issues of Access and Economics. The Canadian Journal of Information and Library Sciences 29(2), 171–189 (2005)
12. IGADD. DigitalDivide.org. Invester Group against Digital Divide, IGADD (2009), http://www.digitaldivide.org/
13. ITU. Bridging the Digital Divide. International Telecommunication Union, Geneva (2004)
14. ITU. ICT EYE. International Telecommunication Union (2009)
15. ITU. World Information Society Report 2007. International Telecommunication Union, Geneva (2007)
16. Jin, J., Cheong, A.W.H.: Measuring Digital Divide: The Exploration in Macao. Observatorio (OBS*) 2(3), 259–272 (2008)
17. Kohonen, T.: Self-Organizing Maps. Springer, Heidelberg (2001)
18. Maitland, C.F., Bauer, J.M.: National Level Culture and Global Diffusion: The Case of the Internet. In: Ess, C. (ed.) Culture, Technology, Communication: Towards an Intercultural Global Village. State University of New York Press, Albany (2001)
19. Norris, P.: Digital Divide: Civic Engagement. In: Information Poverty, and the Internet Worldwide. Cambridge University Press, Cambridge (2001)
20. Ofcom. Citizens' Digital Participation. OfCom - Office of Communications, United Kingdom (2009)
21. Robinson, K.K., Crenshaw, E.M.: Cyber-Space and Post-Industrial Transformations: A Cross-National Analysis of Internet Development (1999)
22. Rundle, M., Comley, C.: Ethical Implications of Emerging Technologies: A Survey. UNDESCO, Paris (2007)
23. UNCTAD. The Digital Divide: ICT Development Indices 2004. United Nations Conference on Trade and Development, United Nations, New York and Geneva (2005)
24. UNDESA. UN Global E-government Survey 2003. United Nations Department of Economic and Social Affairs, United Nations, New York (2003)
25. UNESCO. Internet Governance Forum (IGF) - The First Two Years. A UNESCO Publications for the World Summit of the Information Society - Special issue co-produced with the ITU and UNDESA (2008)
26. Van Dijk, J., Hacker, K.: The Digital Divide as a Complex and Dynamic Phenomenon. The Information Society 19, 315–326 (2003)

Balancing Public and Private Interests in ICT Standardisation: The Case of AVS in China

Junbin Su[1] and Vladislav V. Fomin[2]

[1] School of Journalism and Communication, Xiamen University, Fujian 361005, China
[2] Faculty of Informatics, Vytautas Magnus University, Lithuania
sujunbin@gmail.com, vvfomin@gmail.com

Abstract. This research inquires into how the public interest and private interests can be balanced by a new approach beyond the "Fair, Reasonable and Non Discriminatory" (FRAND) term and Royalty Free in the standardisation process. Using the case of Audio Video coding Standard (AVS) in China, we analyse the mechanisms for treating the Intellectual Property Rights associated with technical contributions of stakeholders and establishing a patent pool with low royalty. The lesson from the AVS case is that, in the Public Dominated Model of standardisation (PDM), public units can successfully contribute intellectual property but cannot easily match the role of private corporations in the standard's implementation. The public-private dilemma in standards development is more complex than that in terms of intellectual property rights.

Keywords: Standardisation, Public Interest, Private Interest, Audio Video Coding Standard (AVS), Public Dominated Model of Standardisation (PDM).

1 Introduction

A standard is usually thought of as a consensus on optimal solution for a specific technical problem [1, 2]. The standardisation process, which involves evaluations of technical solutions and negotiations among stakeholders to achieve consensus on a technically optimal solution, is "by no means the execution of a linear techno-logic." "It is, rather, contingent on institutional factors, actor constellations, actors' interests and perceptions, technical knowledge, and what one might call the artifactual reference of specific coordination problem"[3]. There are bidirectional "translations" underlying the "top-down" management and "bottom-up" coordination processes [4, 5]. On the one hand, the interests of stakeholders are "translated" into a technological contribution, which is expressed in technological language, then evaluated, negotiated and finally adopted into a technical solution. On the other hand, controversies and consensus on technical solutions are "translated" into interests (including the political and economic interests) of stakeholders [6, 7, 8]. At the end of this coordination process, a set of technical rules and sub-rules emerge as an outcome of interest negotiation among relevant actors, and are formulated as a technical standard [3]. When a standard which is adopted for use by society at large, has intellectual property rights

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 64–72, 2010.

associated with part of its technical specification, the complexity of the standardisation process acquires an additional dimension. Here, the status of the standard as a public good is juxtaposed by the temporary monopoly and associated monetary rewards on specific knowledge protected by intellectual property rights.

How can public interest be served under the existing techno-regulatory framework, especially in Information and Communication Technology (ICT) area? Egyedi has argued that there is "a regulatory asymmetry existing between Intellectual Property Right (IPR) interests and compatibility interests" and that "the primacy of IPR ownership and market competition" is anchored by current regulations while the societal significance of compatibility interests, that is public interest, is often neglected [9]. Such "asymmetry" of interests calls for novel theoretical and practical insights on whether the existing *status quo* can be redefined to better serve public interests. While "technical optimality" has traditionally been an expected prerequisite of standards, satisfying this condition in practice requires balanced representation of stakeholders' interests in the process, which in turn requires support by a proper institutional setup [5, 10].

This paper analyses the deficiency of the existing regulatory setup for handling the private and public interests in standardisation. Specifically, we show the limitations of the Fair, Reasonable and non-Discriminatory (FRAND) terms for handling intellectual property rights, and describe what may become a new approach to balance the private and public interests based on the case of the Chinese Audio Video coding Standard (AVS). Given the sheer volume and significance of ICT in today's information society, re-thinking the problem of better protecting public interest in ICT standardisation is timely and important.

2 The Weak Position of Public Interest under the FRAND Terms

Under the current institutional setup of the formal (committee-based) standardisation process, the holders of "essential" patents are expected to obey the FRAND licensing principle, while their actual interpretation of what FRAND means and how it can be implemented on a case-to-case basis is out of the control of a standard development organization (SDO). Such an organisational setup often contributes to a situation in which the patentee and the standard adopters would have different ideas on what FRAND means [11, 12].

The MPEG-family of standards presents an example, where the administration of the patent pool is carried out externally to the formal SDO body. MPEG LA is an agency which lies outside the formal SDOs, and is in charge of the MPEG-family standards and manages patent pools for patentees of MPEG2, H.264/AVC[1], MPEG4 Visual and MPEG4 System. It seems that, by reducing the cost for patentees to license their patents together, MPEG LA could facilitate a broader adoption of the standards under the FRAND framework. *Ex post*, MPEG LA largely succeeded in doing that in the case of MPEG2 standard, and met users' reluctance to adopt MPEG4 standards because the royalty burden was perceived to be excessive by some. For

[1] H.264/AVC (Advanced Video Coding) is a CODEC standard developed by the ITU-T Video Coding Experts Group (VCEG) together with the ISO/IEC Moving Picture Experts Group (MPEG), which is technically identical to MPEG Part 10.

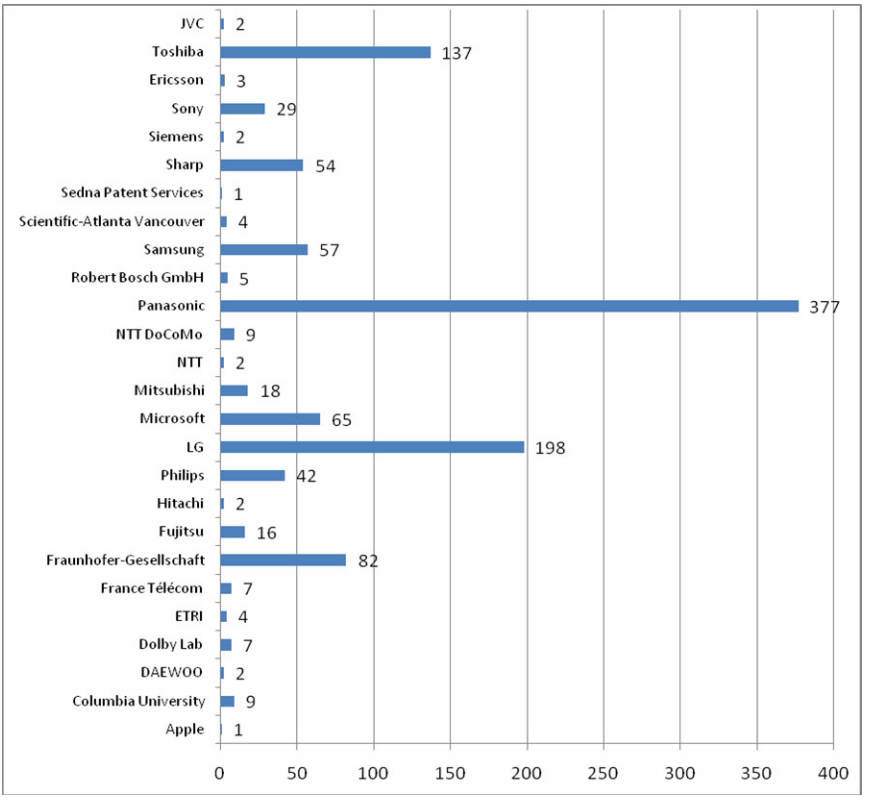


Fig. 1. Composition of Patent Pool of H.264/AVC[2]

example, the European Broadcast Union (EBU) claimed that it was disappointed by the MPEG LA's terms and conditions for the use of AVC [13]. The essential challenge underlying the MPEG LA case is that a "reasonable" requirement of FRAND is too vague and powerless to regulate the patent holders especially when patent licensing is dealt with outside the SDOs after standard-setting.

It is becoming more a rule than an exception that development of a public standard[3], such as H.264/AVC/MPEG4, is likely to involve contributions by private stakeholders which hold "essential" patents (as outlined in Fig.1). The patent pool of H.264/AVC/MPEG4 consists of 1135 patents, only 95 of which (less than 8.4%) come from non-profit institutes that include, for example, Columbia University, the

[2] The data in Fig.1 is sourced from the MPEG LA website, http://www.mpegla.com/, retrieved on May 6, 2010.

[3] We use the term "public" to denote the global and cross-industry significance of an ICT standard, and the fact that it is developed and maintained by international formal standard setting organisations whose mission are to develop standards, which can "facilitate universal access so that people everywhere can participate in, and benefit from, the emerging information society and global economy". See e.g. http://www.itu.int/net/about/mission.aspx/

Electronics and Telecommunications Research Institute, and the Fraunhofer Society for the advancement of applied research (*Fraunhofer-Gesellschaft zur Foerderung der angewandten Forschung e.V.*). The composition of H.264 /AVC patent pool indicates that technical contributions from private corporations dominate the technical coordination process which we refer to as the Private (interest) Dominated Model of standardisation. When most of essential patents or most of patentees in a public standard come from commercial corporations and could be licensed outside SDO under the FRAND, the public interest is under risk of being "kidnapped" through high royalty fees by the private interests of a few corporations. In the patent pool of H.264/AVC, 23 of all the 26 patentees are private corporations, by which AVC could be used as a tool either to pursue a monopoly high royalty fee or to limit the actions of possible new competitors.

The ambiguity of the FRAND principles have come to be a serious problem in ICT standardisation, as exemplified by MPEG standard licensing case, when private interests have diminished its success to be established as a standard that serves public interests. Especially when the standard is a multi-purpose and cross-industry "base" standard, such as MPEG standards, the obstacles caused by intellectual property right policies may have acted as true "reverse salients" that imposed a broad and deep retarding effect on technological innovation [14]. However, without assurance for the protection of, and rewards for, their intellectual property, there may be a lack of positive incentives to motivate private stakeholders to contribute to standards development. Such a juxtaposition of interests poses a question: how to deal with intellectual property rights more appropriately? How to protect the private interests of technical contributors while not sacrificing the public interests of users?

3 Public Interest in AVS Standard Setting Process

The Audio Video coding Standard (AVS) is an alternative standard set by the AVS Workgroup. It aims at solving the problem of an excessively high royalty fee caused by the domination of private interests in the H.264 or MPEG-family standards. To analyse the efforts of the AVS case is to shed light on a possible new approach to balancing public and private interests in ICT standardisation.

3.1 The Mission of AVS

The mission of AVS workgroup is to develop technical standards which serve public interests. Technically, the standard setting mechanisms of AVS (i.e., rules, procedures, and organisation of the standard setting process) are essentially the same as that of the ISO/IEC and the ITU which jointly developed H.264/AVC/MPEG 4: there, top-down management structure is combined with bottom-up decision making and technical contribution processes. What is different is the policy on intellectual property rights.

To avoid the vagueness of FRAND principle, AVS adopted a different approach to the two commonly used FRAND and "Royalty Free" approaches. In the case of AVS, there is a so-called "public technical standard with pre-defined competitive- price licensing of patent pool" [15]. The committee's decision on whether a stakeholder's

technical contribution is acceptable is based on two factors. First, the technical contribution should be technically advanced and available. Second, essential patents should be licensed free or licensed in an AVS patent pool, which is formulated under the management of AVS workgroup during the standardisation process. The innovation of this AVS standardisation process is that licensing of essential patents is regulated *ex ante*, and not *ex post*, as in the case of FRAND policy based standard setting.

Another innovative aspect of AVS standard setting is that more than 20% of its members are public units which include universities and research institutes. These public units contribute most of the essential patents to the AVS standard. For example, six of the nine contributors to the AVS video part are public units. They include the Institute of Computing Technology of the China Academy of Science (CAS), Zhejiang University, Tsinghua University, Huazhong University of Science and Technology, Beijing University of Technology, and the Sun Yat-sen University. Public units contribute 37 of the total 42 technical contributions in AVS1-P2 and 35 of 52 contributions in AVS1-P7 (video for mobile application). The patent pool is managed by the AVS Patent Pool Administration Center which is a non-profit organisation [16].

3.2 Public Interest Dominates AVS Standard Setting Process

Standardisation has received considerable attention since the 1980s, when Farrell and Saloner compared the market, committee, and hybrid standardisation mechanisms. Formal negotiation through a committee can avoid some problems of market mechanism. Farrell and Saloner argued that a hybrid mechanism, and a market bandwagon plus committee negotiation could be more effective in coordinating the social benefits [17].

Schmidt and Werle criticised the economic models for concentrating on choices of actors on the basis of a presumed "payoff matrix" while completely ignoring the technical content of standards [3]. They argued that, besides economic interests, political and professional interests play crucial roles in standardisation: they formulated an alternative set of three modes of standardisation, namely governments, markets and committees, which produce respectively three categories of standards: mandatory, *de facto* or industry standards, and voluntary consensus standards [18, 19]. Because of technical "infrastructural characteristics", few standards are set by a pure market mechanism [20]. To balance the private interests and public interests, most standards are the outcomes of committee negotiation. But whether and how the committee mode differs within the different contexts is still unclear. How to set standards through a proper committee mode is an important problem to be solved.

The techno-political context established by China's National Plan - the Tenth Five-Year Plan, and the development of the hi-tech industry in particular, enables a better understanding of China's motivation to pledge to adopt 2,000 international standards a year for the first five years of the 21st Century so as to reach the target of 80 per cent of key industrial standards that conform to international standards [21]. While key industrial standards are important in the context of export strategies, the strong emphasis on the development of endogenous hi-tech industries also needs the development of home-grown standards. The creation of a large number of endogenous standards requires a well-functioning standardisation infrastructure to support, maintain, and protect the intellectual property rights of the national standards, well-trained

staff to undertake the research and development, and the integration of the national and international operation of the standards development.

With regard to standardisation infrastructure, the Standardization Administration of China (SAC) was set up at the top of the standards infrastructure hierarchy. The SAC has vice-ministerial status and is part of the Chinese General Administration of Quality Supervision Inspection and Quarantine (AQSIQ). The SAC was established to develop the Chinese standards agenda and to help bring domestic standards into alignment with international standards [22]. The AQSIQ emerged out of the reorganisation of China's standards system in 2001 which followed accession to the World Trade Organisation. The SAC now serves as China's "national body" to most international standards organisations including the International Standards Organization and the International Electrotechnical Commission which jointly develop MPEG-series standards. It oversees the administration of the national standards system [23].

With regard to handling intellectual property rights, the AVS Workgroup was established to operate an open, international development process, with an independent intellectual property rights policy. The goal of reducing licensing costs involves the AVS in developing a patent pool that tries to balance Chinese law and cultural values with global practices. The goal of a 1RMB (a Chinese yuan) license fee per unit of consumer-level encoders/decoders in China may not have been achieved, but the existence of AVS as a competitor to the H.264/MPEG4 standard, with lower license fees, may have encouraged the MPEGLA to lower royalty fees for its controlled standards: in the end, this meets the initial goals of the AVS project to re-define the balance between public and private interests in the audio-video codec standards domain.

Based on the case study of AVS standardisation, in our earlier work we formulated a model of committee standardisation, called the Public (interest) Dominated Model (PDM) [24]. The PDM has several distinctive characteristics as compared to the existing international regulatory standards development regime.

First, public institutions play a more visible role in the PDM. To avoid the heavy burden caused by adoption of foreign standards bearing intellectual property right royalties, government agencies in developing countries will encourage public research institutes and universities to play a dominant role in setting endogenous standards, thus complementing the weaknesses of domestic firms at least in an initial stage. As representatives of public interests, the purpose of public research institutes and universities involved in standard-setting is to enhance research capability and to train talent, not to pursuit economic interests. Therefore, it becomes possible under the PDM to form a patent pool with a low-fee license.

Second, under the PDM, intellectual property rights policies are made unambiguous *ex ante*. In the case of the AVS, participants must follow a strict intellectual property rights policy: according to it private patent holders could not claim patent royalty individually but have a binary choice of licensing it royalty-free or licensing it in the AVS patent pool. Standards set under the PDM are likely to have lower licensing costs, and thus contribute to wider adoption: the latter is especially important for innovation diffusion in developing countries.

Third, implementations of standards set under the PDM are likely to require more support from industries in an early stage. Because of the weaknesses of firms'

participation in PDM standard-setting, most of the firms may ride the fence and wait for a bandwagon effect to emerge. Even though the intellectual property rights policies under the PDM may be helpful for the implementation of standards, the licensing cost is not the only factor that determines the behaviour of a firm in making an adoption decision. In the case of the AVS, there is an AVS Industry Alliance which is formed by 18 influential domestic firms to promote the application of AVS standards. The AVS Industry Alliance is expected to lead the creation of a bandwagon effect in the market.

The PDM can motivate public non-profit bodies effectively to contribute technical efforts to standard-setting. This is extremely important when the incentives of other participants are insufficient, as is often the case with formal standard-setting [5]. The PDM can also moderate, or even minimise, the risk of public standards being manipulated by private interests. By encouraging public bodies to play active roles in standardisation, the PDM can set up a patent pool which is timely and which protects *both* the public interests of a standard as a public good *and* the private interests of patent holders.

4 Conclusion and Discussion

Compared to developed countries, domestic firms and industries in countries that are catching-up possess less market and financial power and weaker research and development capabilities. Hence, their technical capability and willingness to contribute to international standardisation is considerably lower. The case of AVS shows that government agencies in developing countries can encourage public research institutes and universities to play an active and a visible role in setting standards and in supplying public expertise where there is a lack of private expertise. Such an approach can effectively diminish intellectual property rights' claims associated with the particular standard, as well as help to build the institutional and research and technical development expertise necessary to leverage a standards development infrastructure. As the representatives of public interests, the purpose of the public research institutes and universities that are involved in standard-setting is to enhance research capability and to train talents, not to pursuit economic interests.

The AVS case is far from being a success in terms of its implementation. While it is worthwhile to explore the Public Dominated Model of standardisation further, we learned from the AVS case that public units can successfully contribute intellectual property but they cannot easily match private corporations' roles in the standard's implementation. Usually, private corporations which could lead the standard's adoption would rather follow the bandwagon than actively lead it. On the other hand, public units were charged with the creation and contribution of intellectual property to the standard, and yet thus have no actual duty to implement standards in the market.

While a new patent pool approach proved a new promising solution to balancing public and private interest in standards, which carry the status of public good, it did not foster the implementation of AVS to the expected level. This makes us conclude that the public-private dilemma in standards development is more complex than that of intellectual property rights terms. Future research should take into account that a standard's users, setters, and society at large all have a different understanding of

what represents an "optimal" balance of public and private interests in the standardisation process. The May 2010 announcement of Google's promoting of WebM[4] – a royalty-free and open source based video/audio CODEC format [26] – presents a good example of such a complex set-up, where the balancing of public-private interests spans across corporate and open source technology development and across royalty-free and intellectual property right-royalty based product offering. Thus, further research is needed to understand what the promising frameworks are for combining private and public interests in technology standards development to foster wider market implementation of standard-based technologies, products and services.

Acknowledgment. The authors thank the anonymous reviewers for their comments and advice on an early version of this paper. The research has received funding from the European Community's Seventh Framework Programme (FP7), under the grant agreement number SSH7-CT-2008-217457. The authors are also thankful to their Chinese and European colleagues from FP7's "China EU Information Technology Standard Research Partnership" project for their helpful suggestions on the AVS case study.

References

1. Sanders, T.R.B.: The Aims and Principles of Standardization. International Organization for Standardization, Geneva (1972)
2. Verman, L.C.: Standardization: A New Discipline. Ardon Books, Hamden, Conn. (1973)
3. Schmidt, S.K., Werle, R.: Coordinating Technology: Studies in the International Standardization of Telecommunications. MIT Press, Cambridge (1998)
4. Schmidt, S.K., Werle, R.: Technical Controversy in International Standardization, MPIFG Discussion Paper (935). Max Planck-Institut für Gesellschafsforschung, Köln (1993)
5. Fomin, V.V., Vries, H.J.D.: How balance is balanced enough? Case studies of stakeholders' (under-) representation in standardization process. In: Proceedings of the 6th Biennial Standardization and Innovation in Information Technology (SIIT) Conference, Tokyo, pp. 99–112 (2009)
6. Callon, M.: Some Elements of a Sociology of Translation: Domestication of the Scallops and Fishermen of St. Brieuc Bay. In: Law, J. (ed.) Power, Action and Belief, pp. 196–233. Routledge and Kegan Paul, London (1986)
7. Latour, B.: Science in Action: How to Follow Scientists and Engineers through Society. Harvard University Press, Cambridge (1987)
8. Su, J.: An Inquiry into the Coordination Mechanism of Technological Standardization in a STS Perspective. Ph.D. Dissertation. Tsinghua University, Beijing (2008)
9. Egyedi, T.M.: IPR Paralysis in Standardization: Is Regulatory Symmetry Desirable. IEEE Communications Magazine 4, 2–8 (2001)
10. International Telecommunication Union: ITU's history (December 12, 2009), http://www.itu.int/net/about/history.aspx
11. Stern, R.: Antitrust Division gives IEEE standard setters the okay to ask patentees how RAND they are. IEEE Micro, 106–109 (May-June 2007)
12. Cooke, W.: FRAND or Foe. Managing Intellectual Property 160, 31–33 (2006)

[4] WebM consists of the VP8 video codec and audio streams. It is an open, royalty-free standard and could be thought of as an alternative to H.264 in web-based application [25].

13. European Broadcasting Union: EBU Technical Statement-D 96-2003: Joint H.264/MPEG-4 AVC Patent License, http://www.subtel.cl/prontus_tvd/site/artic/.../ebu_mpeg4_avc.pdf.
14. Hughes, T.P.: The evolution of large technological systems. In: Bijker, W.E., Hughes, T.P., Pinch, T.J. (eds.) The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology, pp. 51–82. MIT Press, Cambridge (1993)
15. Huang, T., Gao, W., Reader, C.: A new approach for developing open standard with a more reasonable patent licensing policy (2006), http://www.avs.org.cn/reference/HuangLSSB-confirmed-final.pdf
16. Gao, W.: AVS: From an Idea to Practice (2008), http://register.wise.astri.org/events/avsdb/presentations/AVS_Talking_at_HK_forum_2008.pps
17. Farrell, J., Saloner, G.: Coordination through Committees and Markets. RAND Journal of Economics 19(2), 235–252 (1988)
18. David, P.A., Greenstein, S.: The Economics of Compatibility Standards: An Introduction to Recent Research. Economics of Innovation and New Technology 1, 3–41 (1990)
19. Blankart, C.B., Knieps, G.: State and Standards. Public Choice 77, 39–52 (1993)
20. Tassey, G.: Standardization in Technology-based Markets. Research Policy 29, 587–602 (2000)
21. Ure, J.: China Standards and IPR Chapter. Telecommunications Research Project, University of Honk Kong, http://www.trp.trpc.com.hk/papers/2006/china_ipr_stds_2006.pdf/
22. Suttmeier, R., Yao, X.: China's Post-WTO Technology Policy: Standards, Software and the Changing Nature of Techno-Nationalism. The National Bureau of Asian Research: Special Report, No. 7 (2004)
23. Suttmeier, R.P., Yao, X., Tan, A.Z.: Standards of Power? Technology, Institutions, and Politics in the Development of China's National Standards Strategy: The National Bureau of Asian Research, p.13 (2006)
24. Su, J., Fomin, V.V.: Public Dominated Standardization. Paper presented at the International Conference on Internet Technology and Applications, Wuhan, China, August 21-23 (2010)
25. WebM Project: What Is WebM? (May 25, 2010), http://www.webmproject.org/about/
26. Slivka, E.: Google Announces 'WebM' Open-Source Video Format, Plans for Android Television Integration (May 19, 2010), http://www.macrumors.com/2010/05/19/google-announces-webm-open-source-video-format-plans-for-android-television-integration/

The European VCD System: Facilitating Public Procurement through Criteria-to-Evidence Mapping

Ansgar Mondorf and Maria A. Wimmer

University of Koblenz-Landau, Institute for IS Research, Research Group E-Government,
Universitätsstraße 1, 56070 Koblenz, Germany
mondorf@uni-koblenz.de, wimmer@uni-koblenz.de

Abstract. To facilitate European Union (EU)-wide interoperability in public eProcurement, the European Commission co-funds the PEPPOL project. PEPPOL aims at setting up pan-European pilot solutions that conjointly exist with national infrastructures. One of the key building blocks is the Virtual Company Dossier (VCD), an electronic cross-border document container that carries attestations and candidate statements required to evidence the fulfilment of non-exclusion and selection criteria in public tendering procedures. The attestations and candidate statements available in the various Member States often differ in their quality, relevance to certain criteria and format. In this contribution we present a concept to facilitate the correct mapping of national evidences to selection and exclusion criteria of a contracting authority from a different EU Member State. We present a solution that supports mutual recognition of diplomas, certificates or other evidence with a decision-support system called the European VCD System.

Keywords: Public Online Procurement, PEPPOL, Virtual Company Dossier, Interoperability.

1 Introduction

Since 2003, interoperability in eGovernment has been largely investigated in research (see e.g. [1, 2, 7, 10, 14]). Interoperability refers to the capability of information and communication technologies (ICT) systems (and their underlying business processes) to exchange information or services directly to operate effectively in collaboration contexts (cf. [8, 9]). The European Commission (EC) has established an institution that takes care of interoperability in the public sector. The Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens (IDABC) has developed the European Interoperability Framework of which a second version is currently under revision [8, 9].

Existing research and practice (see e.g. [1, 2, 7, 8, 9, 10, 11, 12, 14]) distinguishes among different levels of interoperability. The following interoperability levels are put forward in the European Interoperability Framework [9]:

- **Political context** describes that cooperating partners need to have compatible visions, and need to focus on the same things.

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 73–85, 2010.

- **Legal interoperability** refers to the synchronisation of the legislation in the cooperating Member State so that electronic data originating in any given Member State is accorded to proper legal weight and recognition wherever it needs to be used in other Member State.
- **Organisational interoperability** refers to enabling processes to cooperate.
- **Semantic interoperability** refers to the exchange of information in an understandable way within and across organisational borders.
- **Technical interoperability** refers to the ability to connect systems by defining standard protocols and data formats.

A major objective of the EC is to enable European-wide eProcurement across borders by creating common principles and technical solutions that are applied within all Member States (cf. the eGovernment Action Plan [4]). According to a study by the EC, governments are the largest buyers in the European Union that purchase goods and services at a level of 1.5 billion euros (which corresponds to around 6 % of the gross domestic product). However, governments are lagging behind major industries in exchanging relevant information with key actors such as economic operators. Therefore, the definition of common models for electronic data exchange is perceived as extremely relevant for companies to participate in public eProcurement. The study also reveals that by using eProcurement governments could save up to 5% on expenditure and the transaction costs for both buyers and suppliers could be reduced by 50-80% [5].

As a response to these challenges, the EC co-funds the Pan-European Public Procurement On-Line (PEPPOL) project[1] within the Competitiveness and Innovation Framework Programme (CIP)[2]. PEPPOL aims to set up pan-European pilot solutions for public procurement and contributes thereby to interoperable solutions for public procurement across Member State countries as well as simplifies eProcurement procedures.

One of the key building blocks of PEPPOL is the Virtual Company Dossier (VCD), an electronic cross-border document container that carries the attestations and candidate statements required in public tendering procedures. The contribution at hand will first introduce the process of a tendering procedure and the role that the European VCD System will play in it. In section 3, we present the overall concept of the European VCD System. We conclude with some lessons learned from current specification activities as well as an outlook on the next steps need for the implementation of the European VCD System.

2 Tendering Processes and the Role of a European VCD System

A tendering process is typically initiated by a contracting authority which prepares a call for tender based on a set of documents, usually consisting of a) the publication of a contract notice, b) the tender contract documentation, c) the technical specifications, and d) additional documents. The contract notice is produced and transmitted to an appropriate notification system such as the official gazette of the European Union, Tenders Electronic Daily (TED)[3] – see step (1) in Fig. 1.

[1] http://www.peppol.eu/
[2] http://ec.europa.eu/cip/
[3] http://ted.europa.eu/

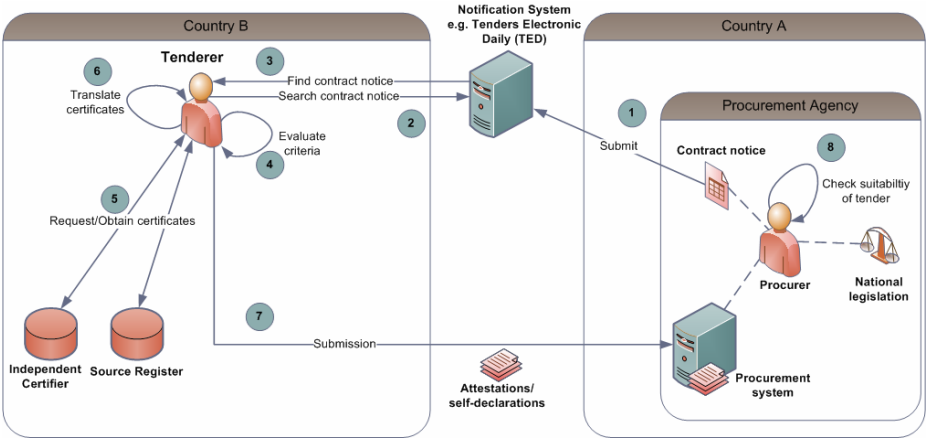


Fig. 1. Status quo procedure for participating in cross-border public procurement

An economic operator can use means such as the TED system to retrieve the relevant information about active tenders – see steps (2) or (3) in Fig. 1. TED publications of contract notices usually contain the tender and contract documentation including detailed criteria, specifications and conditions. Sometimes, the information in a contract notice provided in TED is not complete. Hence, the economic operator has to get in contact with the contracting authority in order to obtain the exact conditions pertaining to the tender and to avoid any potential failure in interpreting the requirements for participation.

If an economic operator decides to participate in a public cross-border tender, selection and exclusion criteria have to be evaluated – see step (4) in Fig. 1. This means that the economic operator has to interpret the criteria set out in the contract notice of another country and find appropriate evidence (attestations, statements, and certificates) within his/her own country to indicate compliance. These forms of evidence can either be retrieved from competent issuing bodies (e.g. certifiers, source registers, banks, public authorities) – see step (5) in Fig. 1 – or they can be issued by the economic operator himself/herself for example to indicate technical qualifications and competencies. Especially in cross-border public procurement, contracting authorities may also require the translation of specific evidence – see step (6) in Fig. 1.

Having collected all the relevant evidence and attestations, the economic operator can finally submit the dossier with all evidences to the contracting authority (together with the bid). Such documents may be distinguished by such criteria as:

a) who issues an evidence (e.g. trusted issuing bodies),

b) what quality of trust does the evidence have (e.g. self declaration, solemn statement or original evidence),

c) what replacements may exist for a given piece of evidence (self declaration, declaration on oath or solemn statement),

d) for which legal form is the evidence to be issued.

Fig. 2 visualises the taxonomy of evidences developed throughout the PEPPOL project.

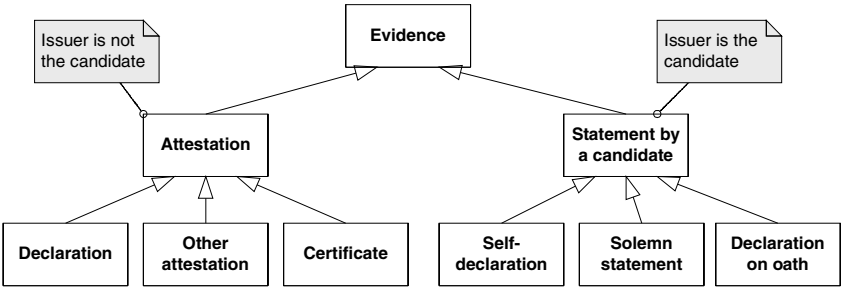


Fig. 2. Taxonomy of evidences

Another complication relates to the constellation of an economic operator. If the economic operator has one or more sub contractor(s), different evidences may be needed for the different types of tenderers. Likewise, the economic operator may be a bidding consortium with a lead tenderer and one or more further members. Each of these tenderers may also have subcontractors. The taxonomy for tenderer structures is shown in Fig. 3. In this case, the collection of evidences is affected by yet another complexity driver.

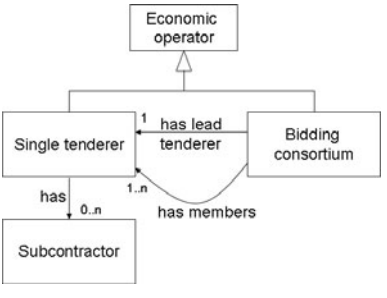


Fig. 3. Concept for the tenderer structure of economic operators

Finally, single tenderers and subcontractors may have a broad range of legal forms. Evidences do exist for specific legal forms. In some cases, evidences are to be issued only for natural persons, i.e. for persons with specific roles in the legal and organisational setup of an organisation.

As can be recognised, the step of selecting, collecting, and evaluating appropriate evidences to prove suitability becomes a major task and burden for economic operators and contracting authorities. Two different contexts drive the mode of action of both stakeholders:

- The decision about whether certificates, documents and other evidences are in conformity with the criteria of the tender is taken by the contracting authority. Contracting authorities are bodies governed by public law. They are also bound by their national provisions of public law and therefore apply their national law (lex fori). The European procurement directives are

implemented into the various national Member States' laws; part of this law is the principle of the mutual recognition of diplomas, certificates and other evidence of formal qualification [3, 6].
- Economic operators are private entities. They operate under the national conditions of their home country and are not governed by public law. They can only provide evidence which is available in their home country and may produce candidate statements according to the foreign law of a contracting authority.

The interplay of the two different modes of action leads to difficulties, when there is a need to prove or evaluate suitability. The following two examples indicate some of the difficulties identified in the context of the PEPPOL project's VCD analysis:

- A contracting authority in Austria issues a Call for Tender and a German economic operator wishes to participate in this tendering procedure. According to Austrian law, criminal records have to be provided for all representatives of the economic operator. In Germany it is sufficient to present the criminal record of one representative. The key questions for both stakeholders are: What legislation is now applicable? How many criminal records have to be provided?
- A contracting authority in Italy requests an anti-mafia declaration. In Italy anti-mafia declarations are typically issued by competent public authorities. In most other countries, no equivalent document exists. Again, the key questions are: What legislation is now applicable? How can economic operators from other countries provide evidence that relates to this specific criterion? How will the contracting authority measure that a foreign economic operator has proved this criterion sufficiently?

These two examples demonstrate the difficulties that may occur and hinder the actors involved to operate the processes of evidence provision and evidence evaluation effectively.

The context described in this section is the starting point for conceptualising a European VCD System. The next section introduces parts of the legal and technical specifications of a European VCD System, which will provide effective and legally compliant decision-support for economic operators and contracting authorities in European cross-border public procurement.

3 Specification of the European VCD System

3.1 Semantic Interoperability Model

The European VCD System is focusing on the legal interoperability of evidences on the basis of European and national legislation. It is therefore necessary to gather national contexts and to define a basic European semantic interoperability model that supports the mutual recognition of certificates and qualification documents.

The national procurement domains are linked to a single European common domain. For every national domain a representation of the national context is developed

which provides an overview of national criteria demanded in public procurement, and how these are evidenced. The national contexts are connected with a single European semantic interoperability model which acts as a pivotal element. Thereby, the selection and non-exclusion criteria defined within Articles 45-51 of the European Directive 2004/18/EC represent the common reference criteria, while the national criteria for individual public tenders in respective countries are considered to be the local criteria [3, 6].

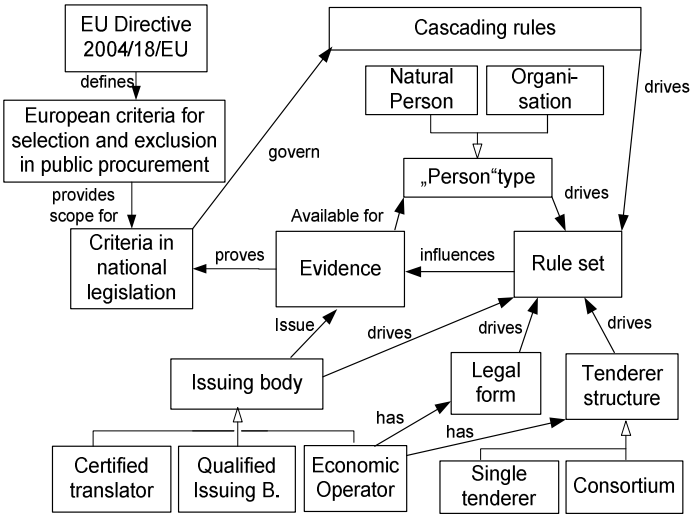


Fig. 4. Semantic interoperability model of the European VCD System

The semantic interoperability model supports basic guidance in applying the relevant community rules on mutual recognition of evidences in cross-border procurement procedures. The semantic model especially requires and provides:

- A mapping between available national evidences of economic operators and the selection and exclusion criteria set by the contracting authority in another country through European criteria. These European criteria of selection and exclusion are directly derived from Articles 45-51 of Directive 2004/18/EC [3, 6];
- A provision of a rule set supporting alternative means for evidencing criteria, when foreign economic operators are considered.

As the criteria according to the EU Directive are the same for all Member States, these criteria act as the pivotal element for the cross-border mapping in the European VCD concept. The semantic model is thereby able to clarify the relationship between national attestations of similar type and the kind of criteria to which those documents refer. In consequence, an economic operator participating in a tender published by a foreign country can quite easily understand the requirements (what criteria have to be

fulfilled) and decide which are the best national attestations (self declarations included) to prove the criteria requested by the contracting authority when applying a specific rule set. Likewise, the contracting authority can check through the same mapping mechanism to ascertain whether the attestations submitted express fulfilment with the relevant criteria or requirements. The following subsections detail the legal rule-set and the technical specification for the European VCD System.

3.2 Legal Specification

As shown in Fig. 4, the legal specification of the European VCD System is driven by cascading rules, the tenderer structure, the legal form of economic operators, and the availability of evidences for specific types of persons (either legal persons or natural persons). With regard to trustworthiness and mutual recognition, the quality of the issuing body (trusted issuing body, economic operator, or statement before a notary) also plays an important role.

The cascading rules play a key role and provide a general approach for finding equivalent evidences if no comparable evidence exists in another country. It is assumed that rules with regard to mutual recognition do exist within the different countries – cross-border public procurement as such happens, even though in most Member State countries to a marginal extent. Many countries therefore have implemented with cascading rules which rank different evidence categories according to their quality and format.

In the VCD context, a cascade is understood as a series of alternative evidences that occur in successive stages or descending order, each of which is dependent on the preceding one. The cascade indicates in a ranking order which evidences should, and which alternatives could, provide a legally accepted proof of a certain criterion when no comparable evidence exists in another country. Within a national tendering procedure the contracting authority will apply its national law and, in particular, will apply the cascading rules to find out which evidence type to accept. The rules of the contracting authority will be used to justify whether the evidence will be accepted or not. If the economic operator provides evidences in the highest evidence category that is available in his/her home country (according to the descending order of the cascading rules) these evidences have to be accepted as substitute evidences by the tenderer.

In order to differentiate evidences on the European level, a concept for classifying evidences along four levels is defined (in a descending order of quality and trust) as a framework for cascading rules:

1. **Evidences created by competent issuing body:** Such documents are issued by an authority or trusted third party (public and private) that has the competence to provide statements in this particular domain.
2. **Declaration on oath:** A declaration on oath has to be declared in the presence of a competent authority. A false declaration made on oath is itself a criminal offence.
3. **Solemn statement:** Solemn statements are declarations where a competent body (e.g. a notary) confirms as a witness the identity of the person who is making the self declaration. This raises credibility but does not have other legal implications than the self declaration itself. Through the

witness, trust in the person making the self declaration is intended to be increased.

4. **Self-declaration:** A self-declaration is an informal statement which has in principle no further legal consequence apart from offences like fraud.

The categorisation for the cascading rules is used within the different national contexts so as to define the standard evidence and the possible substitute documents or evidences that an economic operator may provide as valid proof of a particular criterion. Categories 2-4 are created by the economic operator and act as general substitute categories while category 1 is always considered to be a valid standard proof (it can be for example a tax certificate, an evidence of professional risk indemnity insurance, or a quality assurance certificate). Issuing bodies for category 1 documents receive the highest level of trust on the side of the contracting authority. They also form the highest quality of evidence.

The descending order introduced by the different categories is the basis for finding the best possible match to complement the non-existence of an evidence in a country. The economic operator's final decision with regard to substitute evidence is driven by the cascading rules[4] in the country of the contracting authority. The available options in the country of the economic operator are either evidence created by a competent issuing body (category 1) or by a candidate statement produced by the economic operator (categories 2-4).

The cascading rules determine the options. If a cascading rule outlines levels 1-3 as an accepted proof of evidence then this has to be checked against the options which the economic operator has. If (1) is an available option in the country of the economic operator it has to be taken. If (1) is not available, the economic operator has to provide a candidate statement. In this case the candidate statement should be either a declaration on oath or a solemn statement (in cases where a declaration on oath cannot be produced).

This approach also applies for cases where no match to European criteria exists. For example in the case of an anti-mafia declaration, Italy has to define a virtual criterion for its national "anti-mafia" criterion and the correlating cascading rules for it. A virtual criterion is needed because the Directive does not explicitly mention this specific Italian criterion. In this case, most of the European countries do not have a matching national criterion; thus, they have to state that this criterion and rule is not applicable. Hence, the economic operator can only produce a candidate statement. The Italian cascade then defines which categories of candidate statements will be accepted.

Besides the cascading rules, the implementation of the European VCD System is influenced by other factors that are shown in Fig. 4. These rules are only briefly outlined below:

– Natural Person: Some evidences can only be issued for natural persons but they are not available for organisations. Many countries only issue criminal records for natural persons. Countries may apply different rules that

[4] Note: Unfortunately, cascading rules differ across EC Member States.

describe which of the natural persons within an economic operator have to prove a given criterion.
- Tenderer structure: Within a tendering procedure, tenderers may participate in different roles. The major roles defined within the European VCD System are single tenderers, subcontractors and bidding consortia (with a lead contractor and further members of a consortium). Some evidences have only to be presented for a particular role (e.g. the lead contractor or the members of the consortium, but not the subcontractors).
- Legal Form: Depending on the legal basis of an economic operator, different evidences may exist to prove a given criterion. For example, evidences to prove the official enrolment in a professional register or in a trade register may depend on the legal basis of the operator.
- Field of profession: There are some evidences that depend on the field of profession. Some evidences can for example only be provided if an economic operator is member of a particular organisation which is dependent on the specific profession.

The legal rules drive the technical concept of the European VCD service. Its technical specification is outlined in the following subsection.

3.3 Technical Specification of the European VCD Service

In terms of technical specification of the European VCD service, Fig. 5 provides an overview of the main components and their interrelations.

The Tenders Electronic Daily (TED) interface denotes an interface to the electronic publication office of the European Union. Contract notices stored on this system could be evaluated by the European VCD System by automatic processing of the criteria defined in a particular Call for Tender.

The European VCD System must provide a functionality to calculate the evidences in the economic operator's country on the basis of national criteria published in the country of the contracting authority. For the electronic representation of the criteria and evidences, the concept of an ontology is used (for details on the ontology concept see e.g. [13]). The VCD ontology serves as data and rule set storage. It consists of different parts: the top-level ontology defines the general concepts that are applicable in all Member States and thereby set a common European (legal) framework. National ontologies are defined for each Member State in order to describe the national legislation and the mappings of national criteria to evidences. Hence, the ontology can be considered as VCD mapping tree that interconnects the legislation and evidences within the different countries through common pivotal elements, the European criteria.

The functionality for the management of the ontology and the data contained in it is provided by the component called the VCD ontology manager. The ontology manager thereby defines different rules for accessing and maintaining the various parts of the ontology.

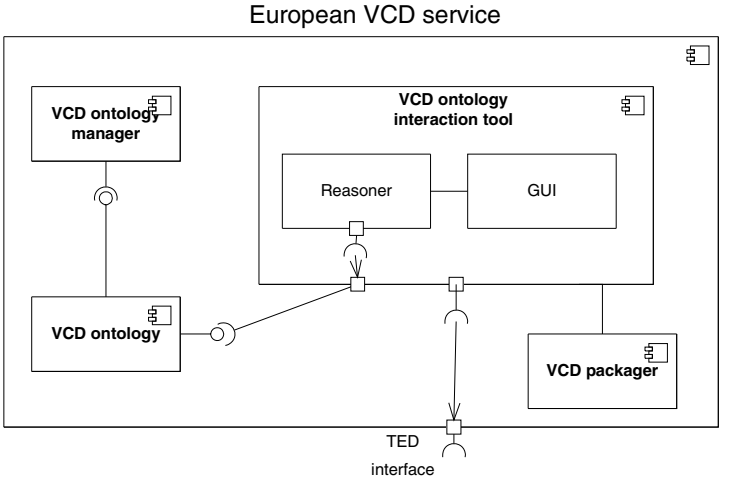


Fig. 5. Components of the European VCD service

The core functionality of the European VCD System is the VCD ontology interaction tool. It provides the graphical user interface and enables the generation of a list of evidences that are in accordance with the rule set mentioned in the previous section. The ontology is queried through two reasoner components, one which manages the rule set related to tenderer structures and one which manages the rule set in relation to the criteria-to-evidence mapping and the cascading rules. The procedure to map a list of criteria from one country to a set of evidences from another country can be described through the following five steps (the first step is optional and depends on the publication procedure that is chosen by the contracting authority):

1. Some contracting authority may refer to particular evidences in the contract notice/call for tender instead of using national criteria. In this case at first the correlating national criteria in the contracting authority's country have to be identified (optional).
2. In a second step the national qualification criteria are mapped to common European criteria serving as a pivotal element. The European criteria may be extended through virtual criteria that describe requirements which are unique to specific countries.
3. In a third step the mapping between the European criteria and the national criteria of the economic operator's country is performed.
4. The national criteria of the economic operator's country are used in the next step to identify the correlating evidences.
5. Finally the rule set (e.g. cascading rules) of the contracting authority is applied to the evidences identified in the country of the economic operator. This ensures that the evidences are correctly prepared under the conditions of the contracting authority.

The calculation of the mapping is performed by using the mapping tree defined within the ontology.

When the ontology interaction tool has calculated the relevant evidences, the user, i.e., the economic operator, retrieves a VCD package skeleton (which is an XML document) which refers to an XML schema defined for the VCD document container. The XML document generated by the European VCD System is called a skeleton, as it does not yet include the individual evidences. The component which compiles this VCD package skeleton is called the VCD packager. The user retrieves this VCD package skeleton and, in a next step, contacts his/her national VCD service provider, who can collect all evidences from the issuing bodies and who can compile a full VCD package for the economic operator.

With the compilation and provision of a VCD package skeleton, the service of the European VCD System is completed. The European VCD System is planned to be publicly available and maintained centrally at European level.

4 Concluding Remarks and Outlook

One of the major objectives of the PEPPOL project is to facilitate EU-wide interoperability in public eProcurement. Therefore common principles and technical solutions have to be developed that are applied within all the Member States. eProcurement requires efforts to be made by public administrations, in particular to exploit new technologies for interoperability that enable easy information accessibility and improve the availability of pan-European services and interaction among citizens and businesses [8].

The VCD, as one of the key building blocks of the PEPPOL project, should support economic operators in any European country to draw on company information which is already registered somewhere in its home country and to submit these evidences electronically to any public sector awarding entity in Europe. The evidences and the underlying legislation currently differ from Member State to Member State: this makes it difficult for economic operators to participate easily in foreign public procurements procedures.

In this paper, we have presented a concept for a European VCD System. We described the concept according to the legal and technical specifications that provide an opportunity to harmonise the different national systems in Europe without changing them.

The next steps in the PEPPOL project are to start with the implementation of pilots. The project will thus undertake an incremental prototyping procedure with a proof of concept pilot, a test pilot, and a production pilot. It is planned that, in November 2010, the European VCD System will run in its first production version.

Even though the concept for the European VCD System provides an innovative, intelligent and advanced service to facilitate cross-border public eProcurement, there are a number of challenges that the project team will have to face to achieve the substantial objectives of the initiative. Some of these challenges are a) to define the overall governance process, b) to settle procedures for the maintenance of the ontology and rule set for criteria-to-evidence mappings and c) to find an appropriate host for the European VCD System, which will ensure that the ontology always stays up-to-date and legally compliant with European and national public procurement

laws while the ownership of the ontology remains with the individual Member States.

The VCD and the European VCD System will lower the transaction costs of economic operators by supporting them in creating a qualified VCD package in their home country. With the VCD it will be easier for business entities to make cross-border submissions of evidences and, thereby, to increase the ratio of meeting the legal and formal company qualification criteria and selection criteria for the awarding phase of a tender.

Acknowledgements. PEPPOL is co-funded by the European Commission under the Competitive and Innovation Programme, Information and Communication Technologies Policy Support Programme (ICT PSP). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained in it.

References

1. Charalabidis, Y. (ed.): Interoperability in Digital Public Services and Administration: Bridging E-Government and E-Business. IGI Global, Hershey (2010)
2. European Commission, Linking up Europe: The importance of Interoperability for eGovernment Services Commission Staff Working paper, Commission of the European Communities, Brussels (2003)
3. European Commission, Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts. Official Journal of the European Union, 30.04.2004 (2004)
4. European Commission. i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All. European Commission: Brussels, COM, 173 (2006)
5. European Commission, Action plan for the implementation of the legal framework for electronic public procurement. European Commission, Brussels (2004)
6. European Commission, Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors. Official Journal of the European Union, 30.04.2004 (2004)
7. Guijarro, L.: Analysis of the Interoperability Frameworks in eGovernment Initiatives. In: Traunmüller, R. (ed.) EGOV 2004. LNCS, vol. 3183, pp. 36–39. Springer, Heidelberg (2004)
8. IDABC, EIF: European Interoperability Framework for Pan-European E-Government Services. European Communities (2004)
9. IDABC, EIF: Draft for public comments – as basis for the European Interoperability Framework for Pan-European E-Government Services 2.0. European Communities (2008), `http://ec.europa.eu/idabc/servlets/Doc?id=31597` (accessed on October 15, 2010)
10. Kubicek, H., Cimander, R.: Interoperability in eGovernment - A Survey on Information Needs of Different EU Stakeholders. European Review of Political Technologies 3, 59–74 (2005)

11. Peristeras, V., Tarabanis, K.: The Connection, Communication, Consolidation, Collaboration Interoperability Framework (C4IF) For Information Systems Interoperability. IBIS - International Journal of Interoperability in Business Information Systems 1(1), 61–72 (2006)
12. Scholl, H.J., Klischewski, R.: E-Government Integration and Interoperability: Framing the Research Agenda. International Journal of Public Administration 30(8), 889–920 (2007)
13. Staab, S., Studer, R. (eds.): Handbook on Ontologies. Springer, Berlin (2004)
14. Wimmer, M.A.: Integrated service modeling for online one-stop Government. EM – Electronic Markets, Special Issue on e-Government 12(3), 1–8 (2002)

Money Laundering and FATF Compliance by the International Community

Ali Alkaabi, George Mohay, Adrian McCullagh, and Nicholas Chantler

Information Security Institute, Queensland University of Technology, GPO Box 2434, 126 Margaret Street, Brisbane, QLD 4001, Australia
a.alkaabi@isi.qut.edu.au, g.mohay@qut.edu.au, a.mccullagh@qut.edu.au, a.chantler@qut.edu.au

Abstract. This paper examines the anti-money laundering systems of Australia, the United Arab Emirates (UAE), the United Kingdom (UK) and the United States of America (USA), the extent to which they have implemented the Financial Action Task Force (FATF) recommendations, and how compliance with these recommendations is affected by local cultural and economic factors. The paper makes use of FATF evaluation reports to compare the countries' compliance; it examines some of the underlying cultural considerations and culture-specific ethical issues that affect the extent of compliance, and how cultural and ethical considerations may affect good governance. The findings indicate that the UK and the USA are the most advanced with regards to their compliance with the FATF recommendations and Australia and the UAE less so. The UAE is in particular found to be least compliant. We relate this finding to previous work on how a country's legal and financial systems develop in line with its religion, culture and socio-economic situation, and examine how such local factors have affected the UAE's financial and anti-money laundering and combating the financing of terrorism (AML/CFT) systems. This research will be of interest to policy-makers and government agencies involved in addressing money laundering and its successful detection and prosecution.

Keywords: Money Laundering, FATF, Compliance, Australia, UAE, UK, USA.

1 Introduction

There are, generally speaking, two reasons why organisations and individuals may wish to launder money. First, to hide illegitimately acquired income or to avoid divulging activities which if closely scrutinised might reveal related illegal activities. Second, to hide legitimate income in order to avoid income tax in countries in which it is levied. If the extent of money laundering is extreme, then this represents a substantial threat to the revenue and economy of a country and possibly an untenable level of (probably organised) criminal activity. Therefore, it is in society's interests to detect money laundering. Prevention of money laundering will arguably prevent loss of government revenue and will likely prevent or at least reduce criminal activity.

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 86–97, 2010.

Consequently, countries worldwide have legislated against money laundering. At the international level, the Financial Action Task Force (FATF) developed the 40+9 recommendations on anti-money laundering and combating the financing of terrorism (AML/CFT) [1] in an attempt to provide a good governance framework. These 40+9 recommendations are generally recognised as an international standard for implementing any AML/CFT system. Countries such as Australia, the UAE, the UK and the USA have reformulated their legislation and regulations to bring them into line with the FATF recommendations. Interestingly, these four countries among others have been identified by the United States' (US) Department of State as major money laundering countries in 2008 [2]. To the authors knowledge this paper will be the first paper that compares a modern Islamic country such as the UAE with three modern western jurisdictions such as Australia, the UK and the USA.

The work described in this paper focuses on these four countries for a number of reasons. The UAE has been selected as the funding for this research has been provided by the UAE[1] and because the UAE, while a modern and rapidly developing economy, is an Islamic jurisdiction and thus to that extent distinctly different from the other three countries. Australia is included as the research has been undertaken in Australia while the UK has been selected because it is a jurisdiction representative of the European Community. Finally, the USA has been selected for a number of reasons, the principal being that as the world's largest economy it needs to be included in any study of this sort.

This paper analyses the differences in the AML/CFT systems of Australia, the UAE, the UK and the USA, and the extent to which they have interpreted and remained faithful to the FATF recommendations. The paper makes use of the FATF evaluation reports for Australia in 2005 [3], the UAE in 2007 [4], the UK in 2006 [5] and 2009 [6] and the USA in 2006 [7] to compare their compliance and discusses the local factors, such as cultural and economic factors, that have arguably affected the UAE's compliance with the FATF recommendations.

Section 2 analyses and compares the extent of compliance of these countries with the FATF recommendations. It also discusses the implications for non-compliant countries. Section 3 analyses how local factors have arguably affected the UAE's compliance with the FATF recommendations. Section 4 presents our conclusions.

2 Compliance with the FATF 40+9 Recommendations

In the recent FATF evaluation of their AML/CFT systems, countries were required to submit follow-up reports indicating their progress with achieving compliance. Australia, the UK and the USA have reported back to the FATF. The only published follow-up report arising from these evaluations is one for the UK AML/CFT system which shows that the UK system has made substantial progress and has reached a satisfactory level of compliance with all the core and key recommendations[2] including recommendation 5, which concerns "customer due diligence and record-keeping". Follow-up reports for Australia and the USA are not available in the public domain at

[1] This research is funded by the Abu Dhabi Police, UAE.

[2] According to the FATF, the core recommendations are 1, 5, 10, 13, SR II, and SR IV, and the key recommendations are 3, 4, 23, 26, 35, 36, 40, SR I, SR III and SR V.

the time of writing. The UAE was to report to the FATF in March, 2010. Compliance with FATF recommendations is rated as follows: fully compliant (C), largely compliant (LC), partially compliant (PC) and non-compliant (NC). Compliance with each recommendation is measured against essential assessment criteria. This section compares how Australia, the UAE, the UK and the USA comply with the FATF 40 recommendations (see Table 1). The section then proceeds to compare how these four countries comply with the FATF 9 special recommendations (see Table 2).

2.1 Compliance with the FATF 40 Recommendations

The FATF 40 recommendations on AML are categorised into four groups: (a) legal systems; (b) preventive measures; (c) institutional and other measures; and (d) international co-operation.

Legal systems. The UK and the USA are fully or largely compliant with 'Legal systems' recommendations 1, 2 and 3. The UAE is largely compliant with two recommendations; however, it is only partially compliant with recommendation 1 concerning money laundering offences. The FATF [4] indicated that the UAE has criminalised money laundering but the predicate offences in the law do not cover all types of serious offences such as drug trafficking and corruption, which is not completely in accordance with the FATF recommendations.

Preventive measures. Australia is non-compliant with nine of the 22 recommendations, and is only partially compliant with 8 other recommendations and in particular is non-compliant with the core recommendation 5 regarding customer due diligence. The FATF [3] noted that its customer due diligence is limited in its extent by not covering all varieties of financial institutions. Australia is only partially compliant with core recommendation 10 (record keeping) and key recommendation 23 (financial sector supervision). The FATF noted that the AML/CFT (referred to as AML/CTF in Australia) supervisory system is not in accordance with its recommendations in relation to ensuring that financial institutions have an effective AML/CFT programme in place.

The UAE is non-compliant with core recommendations 5 (customer due diligence) and 13 (suspicious transaction reporting), and it is only partially compliant with key recommendation 23. The FATF noted that there is no core customer due diligence obligations in any law or regulation of the UAE. It also found that there is no requirement in UAE law or regulation to report suspicious transactions related to financing of terrorism. The FATF found that there is a lack of a defined basis to recognise a transaction as suspicious. These deficiencies may in part be the result of the fact that UAE law does not impose customer due diligence obligations and does not clarify the UAE's Financial Intelligence Unit (FIU) responsibilities.

The UK is largely or fully compliant with all core and key recommendations that address 'Preventive measures'. However, it is non-compliant with recommendations 6, 7 and 22 from this group. The FATF [5] indicated that there are no requirements within the UK AML/CFT system concerning the identification of politically exposed persons and noted that there are no requirements specified for financial institutions to collect information with regards to correspondent banking.

In addition to being non-compliant with recommendations 12 and 16, the USA is only partially compliant with recommendation 5 concerning the establishment of

customer due diligence. The FATF [7] found that there are no requirements for some cash dealers such as life insurance agents to establish customer due diligence, and generally there are no clear requirements to perform ongoing customer due diligence.

Institutional and other measures. With regards to 'Institutional and other measures' recommendations 26-34, Australia is partially compliant with recommendations 29 and 34. The FATF noted that Australian Transaction Reports and Analysis Centre (AUSTRAC) powers of enforcement are limited to criminal sanctions and appear to be rarely applied. While the AML/CFT system of Australia has some problems in compliance with the previous recommendations, it is fully compliant with key recommendation 26. In contrast, the UAE system is partially compliant with recommendation 26 concerning the FIU. The FATF found that the UAE's FIU has some problems in relation to collecting, analysing and disseminating suspicious activity reports. The FATF also noted that the UAE's FIU does not publish annual reports with statistics concerning its activities. It is difficult to find information in relation to the number of suspicious transactions reported each year in the UAE, as we found in a separate work [8]. The UK AML/CFT system is partially compliant with recommendations 33 and 34. The FATF noted that the UK system does not have sufficient measures to identify accurate information concerning beneficial ownership[3]. The USA AML/CFT system has some problems in compliance with recommendations 33 and 34. The FATF indicated that the US system does not have adequate measures in place to make sure that there is accurate information available in relation to the beneficial ownership.

International co-operation. With regards to recommendations 35-40, Australia, the UK and the USA are fully or largely compliant with these recommendations. In contrast, the UAE is less compliant than the other countries. It is partially compliant with recommendations 38 and key recommendation 40. It is expected that the UAE will address these areas of deficiencies. The main deficiency is that there are no legal provisions that define how confidential information will be shared with other foreign counterparts.

In summary, and as shown in Table 1, the USA followed by the UK appear to be most advanced in terms of compliance with the FATF 40 recommendations, with the UAE being least compliant.

Table 1. Summary of compliance with the FATF 40 recommendations on AML

Country	Fully compliant (C)	Largely compliant (LC)	Total (C+LC)	Partially compliant (PC)	Non compliant (NC)	Total (PC+NC)
Australia	12	9	21	10	9	19
UAE	5	12	17	16	7	23
UK	19	10	29	8	3	11
USA	12	22	34	2	4	6

[3] By beneficial ownership it is meant the enjoyment by anyone who has the benefits of ownership of a security or a property and yet nominally does not own the actual asset.

2.2 Compliance with the FATF 9 Special Recommendations

This section compares compliance with the FATF 9 special recommendations on Combating Financing of Terrorism (CFT). The FATF simultaneously evaluated the CFT and Anti-Money Laundering (AML) systems in Australia, the UAE, the UK and the USA. Table 2 illustrates a summary by country of compliance with the FATF 9 special recommendations on CFT. Once again, the USA followed by the UK appear to be most advanced in terms of compliance, with the UAE being least compliant.

Table 2. Summary of compliance with the FATF 9 special recommendations on CFT

Country	Fully compliant (C)	Largely compliant (LC)	Total (C+LC)	Partially compliant (PC)	Non compliant (NC)	Total (PC+NC)
Australia	-	5	5	3	1	4
UAE	-	3	3	2	4	6
UK	5	3	8	1	-	1
USA	3	6	9	-	-	-

Australia, the UK and the USA are either compliant or largely compliant with the core and key special recommendations. In contrast, the UAE is non-compliant with core special recommendation IV concerning suspicious transaction reporting. The UAE is only partially compliant with the key special recommendation I regarding implementing the 1999 UN International Convention for the Suppression of the Financing of Terrorism, and the key special recommendation III regarding imposing effective laws for freezing and confiscation of funds used for financing of terrorism.

2.3 Implications of Non-compliance with FATF

Overall, Australia is non-compliant or partially compliant with three core and key recommendations (5, 10 and 23). The UAE is non-compliant or partially compliant with nine core and key recommendations (1, 5, 13, 23, 26, 40, SR I, SR III and SR IV). The USA is only partially compliant with core recommendation 5. This finding suggests that there are additional steps that need to be taken by Australia, the UAE and the USA to address the identified deficiencies. The UAE, in particular, needs to do more work to ensure that its AML/CFT system is effectively implemented in accordance with the FATF recommendations.

Non-compliance with the FATF recommendations has negative implications for a country and its relations with other countries. The implications of non-compliance include the increased risk of exploiting a country's financial system for criminal purposes by organised criminals and terrorists, with consequent implications for a country's economy, society and victims of crime [52]. There are also specific implications of non-compliance with respect to dealing with countries which are compliant. To protect its interests and minimise risk, a compliant country may impose tough regulations in dealing with non-compliant countries. A non-compliant country can face obstacles from international organisations and other compliant countries, obstacles such as discouraging foreign investment, trade and relationships, and damaging reputations with international organisations such as the World Bank and the International

Monetary Fund (IMF). The IMF (2009) [9] noted that "money laundering and terrorist financing activities can undermine the integrity and stability of financial institutions and systems, discourage foreign investment, and distort international capital flows".

There are other implications. A non-compliant country may not be able to provide international law enforcement with useful information such as customer identification and transactions records to assist in tracing the origins of transaction monies. In 2009, the G20 Working Group on Reinforcing International Cooperation and Promoting Integrity in Financial Markets [10] indicated that countries should implement measures that protect the global financial system from uncooperative or non-compliant countries with FATF recommendations that create risks of illicit financial system. In conclusion, non-compliance with the FATF recommendation means a heightened risk for a country's financial systems, reputation, and its interests in dealing with other countries in an extremely globalised world.

3 Factors Affecting Compliance

The previous section analysed and compared the extent of compliance of the USA, the UK, Australia and the UAE with the FATF AML/CFT recommendations. The UAE is the least compliant with the AML/CFT recommendations which is perhaps not surprising. The FATF requirements presuppose the existence of a sophisticated good governance environment and an advanced information technology (IT) infrastructure being established. Good corporate governance is a western creation that relies in the modern environment on the availability of appropriate human resources and developed policies and procedures, and ethical standards, together with audit capability and capacity. This may not be readily available in a developing economy at a stage in advancing its specific economy in a global environment. The compliance obligation to FATF may require some compromise when it comes to a non-western economy but such compromise must not open the door to criminal elements to launder money at the expense of other jurisdictions. This section examines some of the underlying cultural considerations and culture-specific ethical issues that affect the extent of the UAE compliance, and how cultural and ethical considerations may affect good governance and the establishment of shared codes of practice. This examination covers religious, cultural, socio-economic and financial factors that appear to be important in the case of the UAE.

3.1 Ethical Behaviour, Good Governance and Culture

The Internet has brought to the fore and highlighted many new situations fraught with ethical considerations. These considerations arise because the Internet provides so many options for communication and options to access global information resources from a single point of access. It is exactly this power and its potential for misuse that has attracted the attention of national and international organisations interested in the use of the Internet for the common good. Of specific note in this regard is SIG9.2.2 [11], the IFIP Special Interest Group on a Framework for Ethics of Computing, which has been working in this domain for 20 years and which in 1999 published an influential monograph that has direct relevance to the work described in this paper, "Ethics

and the Governance of the Internet" [12]. It is likewise the opportunities provided by the Internet that are exploited by money launderers, giving rise to the evocative phrase "the big cyber-laundering machine" [13].

One of the most pervasive ethical considerations highlighted by global information access concerns the tension between the need for privacy and anonymity on the one hand and the need for accountability on the other [14, 15]. This particular conflict of course transcends national and cultural boundaries, but balancing privacy and anonymity against accountability is pivotal in attempts to combat money laundering globally [14]. As discussed below and in sections 3.2 and 3.3, it presents an especially acute challenge for emerging and developing economies. The UAE at least is progressively addressing the issue.

AML presents a prime example of this conflict between privacy (and anonymity) and accountability, at both the international level where AML efforts rely on identifying the nature of trans-national financial transactions, and also at the local level where identifying suspicious transactions is reliant on reports to the relevant national FIU. There are of course other IT-related ethical issues which are just as relevant but here the focus will be culture-specific. For example, the role of women in society differs markedly across cultures and this relates at a practical level to issues such as the 'digital divide' – not between developing and developed states in this case, but within communities – and open access to the Internet. Open access to the Internet is a point of focus [12].

In Section 3.3 we examine the role played by the Hawala system in the UAE which differentiates it from the other three jurisdictions analysed. Hawala is an honour-based system which is pervasive in many Islamic economies throughout the world. It is used to transfer money or value between people in a local community without any interaction with financial institutions. It has virtually no parallel in western culture and presents a direct challenge to AML efforts. In the case of the UAE, this challenge is addressed through a Hawala broker registration scheme which is, however, still voluntary.

There is another, more complex, example of cross-cultural difference with significant underlying ethical considerations which is examined in Section 3.2. It relates directly to the fight against terrorism on the one hand and society's obligation to provide for the needy on the other. Crimm [16] indicates that implementing the FATF strict standards on AML/CFT can affect the effectiveness and the remit of Islamic charities, and consequently 'cut off' financial support to the needy. This issue does not arise in western culture where company legislation and income tax legislation have historically resulted in careful regulation of charitable institutions.

These two examples illustrate some of the difficulties that face the international community in establishing internationally shared and accepted codes of practice. While establishing principles of good governance is paramount, whether with respect to AML or with regard to international financial markets or whatever, the difficulty is in the detail. In other words, establishing principles of good governance will most likely involve the reconciliation of local cultural and ethical differences if there is to be internationally shared and accepted codes of practice. This could involve compromise so as to accommodate cultural differences and ethical standards. The case of the UAE's progressive alignment with FATF is a salutary example of such reconciliation.

These dilemmas lead naturally to questions regarding the advantages and disadvantages, and the feasibility in general, of constructing a single international framework based on a consensus of divergent views. There is evidently no easy way to do so. Experience shows that building such a consensus is a slow process, and it is important to accept this at the outset of such attempts, in order to avoid premature acceptance of failure. Success requires a willingness of all parties to cooperate and to reconcile differences. Experience also shows that the path to global consensus requires the participation not only of champion international agencies but also of local and regional bodies as well as other stakeholders. The latter is paradoxically made possible by the nature of the Internet – its global nature, the very issue that prompts attempts to achieve the consensus – and the vested interests of non-regulatory, commercial stakeholders. Two recent examples of achieving some degree of such a consensus through regional bodies are the reconciliation of the European Union (EU) and USA approaches to the protection of privacy [12] and cooperation between FATF and regional FATF-style bodies (APG, CFATF, MONEYVAL, GAFISUD, MENAFATF, EAG, ESAAMLG, GIABA[4]) [17]. The work undertaken by the FATF and the FATF-style regional bodies facilitates similar or comparable approaches for implementing AML/CFT systems. While the FATF recommendations are in many cases not fully implemented by the member countries, these recommendations are still considered as an important framework for countries to use in order to counter money laundering and terrorist financing. The focus here is to observe the advantages that the FATF experience creates for proceeding towards a harmonised AML/CFT system and how it has succeeded in bringing these different countries and organisations to agree in principle on international standards for AML/CFT systems.

3.2 Religious and Cultural Factors

The UAE's culture has developed from a strong belief in Islam which governs people's way of life, behaviour and decisions [18]. This has had a significant impact on UAE culture. The UAE culture is accordingly in many ways significantly different from the culture in Australia, the UK and the USA.

The founding members of the FATF – which did not include the UAE – such as Australia, the UK and the USA, have unavoidably left their cultural imprint on the organisation and its operations. This has some natural consequences when it comes to FATF evaluations. Johnston and Carrington (2006) [19] indicate that there is a problem when the FATF do a mutual assessment evaluation of the AML/CFT systems in member countries. This problem is how to implement FATF standards that have been structured in the context of developed economies and apply them to the financial markets of emerging and developing economies. These developing economies [19] typically comprise a substantially different culture and history to that of developed economies. Johnston and Carrington note that trying to impose measures which are unsuitable for developing countries may lead to non-compliance with the FATF standards [19]. Kanatas and Stefanadis (2005) [20] note that culture and legal systems support each other and that economic development and financial structures are affected not only by a country's legal system but also by its culture. They show that

[4] The full titles of all these organisations are given on the Members and Observers page of the FATF website.

the development of a country's legal and financial systems is related to its religious beliefs. They note that culture is "the engine of economic prosperity and growth and a critical factor in the development of financial markets". When people talk about culture, they talk about a way of life, what people believe, and how they apply that to develop their regulations, organisations and institutions. Kwok and Tadesse (2005) [21] argue that countries differ in the configuration of their financial systems because they are different in terms of their national cultures.

According to the US Department of State (2007), Islam is practiced by 96% of the population in the UAE [22], making it a dominant influence on the country. Islam prohibits any activity funded by money derived from unlawful trade or ill-gotten property and prohibits using illegal money for charities [23]. Money gained from gambling and bank interest is prohibited in Islam [23]. This is in marked contrast to normal practice in Australia, the UK and the USA.

While there is no income tax in the UAE, Muslims are required as a part of their religion to "[fulfill] the God right through paying money 'Zakat' to charities or to the needy people" [23]. Charities play an important role in Muslim practices. Crimm (2008) [16] noted that "as Islam places a high value on compassion, wealth redistributions, social justice, and supporting and enhancing fellow humans, both philanthropy and charity play crucial roles for Muslims and their civil societies". The FATF special recommendation VIII indicates that countries should have effective laws and regulations concerning non-profit organisations that can be misused for the financing of terrorism including taking a risk-based approach that identifies the aims of the organisation, its size and the amount of money it handles [1, 24]. The challenge is in identifying what kind of activities constitutes terrorism and whether financing some such activities would be considered as the financing of terrorism. The World Bank (2006) [25] noted that while countries have agreed on combating the financing of terrorism, the "meaning of terrorism is not universally accepted due to significant political, religious and national implications that differ from country to country". Crimm [16] indicated that implementing the FATF strict standards on AML/CFT could affect the extent of Muslim charities and consequently effectively 'cut off' financial support to the needy. Many countries such as the UAE have imposed some obligations on charitable organisations to protect them from misuse. All charitable organisations in the UAE are regulated and monitored by the Ministry of Social Affairs [2]. The UAE also specifies legitimate channels for charities to transfer money outside the country in order to minimise possible use of these funds for illegal purposes. In 2002, the UAE government regulated that all licensed charitable organisations wishing to transfer money overseas, must do so through either: the Red Crescent Authority, the Zayed Charitable Foundation, or the Muhammad Bin Rashid Charitable Trust [2]. This allows people to make charitable donations whose destination can be monitored.

Islam's prohibition of bank interest means that an important service provided by Islamic banking is the buying and selling of goods without interest. For example, if a person wants to buy a car, they do not give the money directly to the seller. Instead, the bank buys the car and resells it to the buyer/ bank customer. This practice is called Murabaha [26] and is pervasive throughout the UAE banking sector. It is noted that while some non-Islamic banks in Australia for instance have started to recognise the need for such services, this is again in marked contrast to normal practice in Australia, the UK and the USA.

The UAE is a cash-based economy in which carrying large cash amounts is a normal practice and this makes it more difficult to impose requirements concerning

reporting large cash transactions. Imposing regulations (for instance, requiring all large transactions to be reported) in such circumstances is very difficult if not impossible. While many consider this to be a good cultural trait, it is problematic for the purpose of analysing the money cycle. Finally, the UAE is a society based on strong homogeneity [27] which is characterised by strong extended family relationships and close family ties [28]. There is a concern here especially when applying the FATF standards that relate to customer due diligence. For instance, if a person goes to a bank to conduct a transaction and finds that he/she knows the bank's employee, it is quite likely that the employee will not undertake due diligence procedures. (In fact, this practice is not limited to only the UAE culture although it is considerably more prevalent in the UAE than some other countries. Bedi and Acharya (2005) [29] note that personal relationships "can lead to poor compliance [with AML] standards as many US Private Banks have found out".) In the UAE, carrying large sums of cash and purchasing properties and expensive products by cash is normal [4]. The US Department of State [2] noted that according to the UAE, "[c]ustoms officials, police, and judicial authorities tend to not regard large cash imports as potentially suspicious or criminal type activities, arguing that the UAE is a cash-based economy, and it is not unusual for people to carry significant sums of cash".

3.3 Socio-economic and Financial Factors

The US Department of State (2007) indicates that oil makes up most of the UAE export earnings and it dominates the economy [22]. Oil provides wealth to the country and its people.

One of the socio-economic factors that affects the UAE financial system and differentiates it from the three other countries in this study is the use of the Hawala system. The Hawala system is used to transfer money or value between people in a local community without any interaction with financial institutions. Viles (2008) [30] defines Hawala as "a system by which people in geographically remote areas can give things of value to each other, without the physical (and, now, without the electronic) conveyance of money". The UAE has established regulations in relation to Hawala which require that Hawaladars should register themselves and then they are recognized as Hawala Brokers [31]. The UAE intends to ensure that the Hawala brokers provide details of money transfers and report any suspicious transfers. The registration is still voluntary and UAE authorities have no legal power to examine Hawaladars for non-compliance.

Australia, the UK and the USA are all recognised as developed economies, while the UAE is an emerging economy. In the UAE, in contrast to Australia, the UK and the USA, there is no tax on income and this has at least two interesting implications. The first is that the motivation for money laundering in order to achieve tax avoidance is absent. The second is that the cycle of money is harder to trace as a result of not having to report income. The obligatory reporting of income in other countries enables the flow of money to be more easily followed. While the UAE requires financial institutions to report any transactions that are unusually large for a given account with no legal purpose or reasonable or economic grounds [32], there is no general requirement to report income by companies or by individuals.

The financial systems in Australia, the UK and the USA are very similar and are dominated by their stock markets [21] and although UAE financial systems have

some similarities with these countries, there are important differences. These differences play an important role in how the country implements its AML/CFT system.

3.4 Summary

It is inevitable that achieving the good governance requirements implicit in the FATF recommendations is difficult; this is due at least in part to different ethical and cultural values internationally. It is nonetheless of paramount importance in combating money laundering, terrorism and organised criminal activity to address this challenge; doing so requires a careful, country by country, consideration of local factors and values. Overall, in the context of the four countries examined in this study, it is submitted that further steps are needed by both the UAE and the FATF in order to achieve a higher degree of compliance with the FATF recommendations.

4 Conclusion

This paper has investigated the implementation of the FATF recommendations by Australia, the UAE, the UK and the USA. Gaps in compliance were identified for the core and key recommendations for three of the four countries studied and the analysis indicates that there are additional steps that need to be taken by Australia, the UAE and the USA to address the identified deficiencies. The AML/CFT system of the UAE in particular is least compliant with the recommendations. The paper has examined some of the underlying cultural considerations, and culture-specific and ethical issues that affect the extent of the UAE compliance, and how cultural and ethical considerations may affect good governance in general and the establishment of shared codes of practice. The paper has examined religious, cultural, socio-economic and financial factors that appear to be important in the case of the UAE. These factors represent a real challenge to any country such as the UAE when implementing its regulations and financial institutions. Given the global and widespread nature of money laundering, it is vital that local and international communities cooperate to meet these challenges.

Acknowledgement. We gratefully acknowledge the comments of our anonymous reviewers who have assisted considerably in focusing our analysis on how ethical and cultural considerations relate to the development of an internationally shared approach and a consensual international framework.

References

1. FATF, http://www.fatf-gafi.org/dataoecd/7/42/38896285.pdf
2. US Department of State, http://www.state.gov/documents/organization/120055.pdf
3. FATF, http://www.fatf-gafi.org/dataoecd/22/38/35509034.pdf
4. FATF, http://www.fatf-gafi.org/dataoecd/47/55/41721938.pdf
5. FATF, http://www.fatf-gafi.org/dataoecd/44/9/37101772.pdf
6. FATF, http://www.fatf-gafi.org/dataoecd/44/8/44048060.pdf
7. FATF, http://www.fatf-gafi.org/dataoecd/44/12/37101706.pdf
8. Alkaabi, A., Mohay, G., McCullagh, A., Chantler, N.: A Comparative Analysis of the Extent of Money Laundering in Australia, UAE, UK and the USA. In: Finance and Corporate Governance Conference, Melbourne (2010), http://ssrn.com/abstract=1539843

9. International Monetary Fund, http://www.imf.org/external/np/exr/facts/aml.htm
10. G20, http://www.g20.org/Documents/g20_wg2_010409.pdf
11. IFIP-SIG9.2.2, http://www.info.fundp.ac.be/~jbl/IFIP/cadresIFIP.html
12. Berleur, J., Duquenoy, P., Whitehouse, D. (eds.): Ethics and the Governance of the Internet, IFIP SIG9.2.2 IFIP Framework for Ethics and Computing (1999), http://www.info.fundp.ac.be/~bl/IFIP/Ethics_and_Internet_Governance.pdf
13. Lovet, G.: Fighting Cybercrime: Technical, juridical and ethical challenges. In: Virus Bulletin Conference, Geneva, pp. 63–76 (2009)
14. Bynum, T.: http://plato.stanford.edu/archives/win2008/entries/ethics-computer/
15. Nissenbaum, H.: The Meaning of Anonymity in an Information Age. The Information Society 15, 141–144 (1999)
16. Crimm, N.J.: The Moral Hazard of Anti-Terrorism Financing Measures: A Potential to Compromise Civil Societies and National Interests: Islamic Law and Law of the Muslim World Paper No. 08-32. Wake Forest Law Review (2008)
17. FATF, http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236869_1_1_1_1_1,00.html
18. ArticlesBase, http://www.articlesbase.com/travel-tips-articles/culture-tips-for-dubai-travel-208239.html
19. Johnston, R.B., Carrington, I.: Protecting the financial system from abuse: Challenges to banks in implementing AML/CFT standards. Journal of Money Laundering Control 9, 48–61 (2006)
20. Kanatas, G., Stefanadis, C.: Culture, Financial Development, and Economic Growth. Preliminary Version (2005), http://finance.eller.arizona.edu/documents/seminars/2004-5/CStefanadis.Culture04-05.pdf
21. Kwok, C.C.Y., Tadesse, S.: National Culture and Financial Systems. William Davidson Institute Working Paper No. 884 (2005), SSRN http://ssrn.com/abstract=1017605, http://ssrn.com/abstract=1017605
22. US Department of State, http://www.state.gov/r/pa/ei/bgn/5444.htm
23. Alagha, S.: Money Laundering from Islamic perspective. Journal of Money Laundering Control 10, 406–411 (2007)
24. FATF, http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf
25. World Bank: Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism. The International Bank for Reconstruction and Development/The World Bank/The International Monetary Fund, Washington DC (2006)
26. HSBC, http://www.hsbcamanah.com/
27. Sindelar, H.R., Peterson, J.E. (eds.): Crosscurrents in the Gulf. Routledge, Washington (1988)
28. Swadi, H.: Child Mental Health Services in the United Arab Emirates. Child Psychology and Psychiatry Review 4(1), 27–29 (1999)
29. Bedi, R., Acharya, A.: AML/CFT - New Policy Initiatives. PriceWaterhouseCoopers and Institute of Defence and Strategic Studies. PWC-IDSS Thought Leadership Series (July 2005), http://www.c-cft.org/publication/pdf/PwC-IDSS_200507.pdf
30. Viles, T.: Hawala, hysteria and hegemony. Journal of Money Laundering Control 11, 25–33 (2008)
31. Central Bank of the UAE, http://www.centralbank.ae/AMLSU.php
32. UAE Government, http://www.centralbank.ae/pdf/AMLSU/RegulationSummary-2005.pdf

Ethical Governance for Emerging ICT: Opening Cognitive Framing and Achieving Reflexivity

Philippe Goujon and Catherine Flick

Faculté d'Informatique, Facultés Universitaires Notre-Dame de la Paix,
Rue Grandgagnage 21, 5000 Namur, Belgium
pgo@info.fundp.ac.be, catherine.flick@fundp.ac.be

Abstract. The impact of techno-scientific developments on societal evolution and lifestyles no longer needs to be demonstrated. The last half of the twentieth century has witnessed a considerable acceleration of the integration of technological elements, Information and Communication Technologies (ICT) into the means of economic production in particular, and social life in general. This article aims to address the methods and practices by which we can effectively open the currently closed cognitive framing of those involved in making ethical governance decisions. This can be done by introducing a second-order reflexivity to allow for accountability and participation in a governance strategy that enables real effectiveness of ethical norm expression in technological projects. This paper draws on the Louvain school of theory of Lenoble and Maesschalk (cf. especially 2006) [10]. The paper's two authors are both involved in the EGAIS[1] and ETICA[2] EU FP7 projects where they are further developing and testing out the approach outlined in order to establish an effective ethical governance approach for future European co-financed technology projects.

Keywords: Emerging Technologies, Ethics, Governance, Reflexive Governance, Technology.

1 Introduction

The rapid change and evolution of ICT presents opportunities for social interaction and the management of life activities in new and often unfamiliar ways. The diversity of use and application areas brought about by the convergence of different media offers great potential for enhancing many aspects of living. At the same time, the main characteristics of these technologies (such as Ambient Intelligence) that lend themselves to inspiring visions of the future also hold the potential for negative ethical impacts. Some ethical difficulties are now familiar to many people, such as challenges to privacy.

Even so it might be hard to identify potential risks in new applications and contexts, especially if we take into account the extent to which new technologies are now

[1] http://www.egais-project.eu/
[2] http://www.etica-project.eu/

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 98–111, 2010.

embedded in everyday human activities. Other risks are less obvious and are likely to become harder to identify since nowadays ICT is becoming "seamless, unobtrusive and invisible" [14]. In other words, the growing process of incorporating ICT into human activities conditions behaviours with processes that are often unconscious or not clearly perceived by the users. This paper uses as its focus, and point of criticism, the many European Commission co-financed projects that concentrate on technological development. The authors are involved in the EGAIS and ETICA projects, which are also co-financed by the European Commission. The aim of the two projects is to explore how to include ethical considerations most effectively in technology-related projects.

2 Background

Unfortunately not all projects that are related to technical developments sufficiently integrate the ethical issues that can arise. In particular, the governance[3] of ethics is often missing, with no guidelines for dealing with ethical issues provided either by the European Union or on a broader international level. Within the European Union, however, the lack of attention paid to ethics has now been recognised: the Seventh Framework Programme (FP7) and to some extent the Sixth Framework Programme (FP6)[4] have incorporated some ethical guidelines and ethical support for co-funded projects. These approaches to address ethical challenges vary, but they are often presented as different ways to identify potential ethical issues at some stage in the research project. Further examples of the attention being paid to the importance of ethics in technological projects include the ETHICBOTS[5], MIAUCE[6], and SWAMI[7] projects.

It is insufficient, however, to determine and address the ethical problems raised by ICT from a theoretical perspective if such approaches have no practical impact and remain external to the development of the technical project itself. It is, of course, always possible to analyse a specific technology or area – such as quantum computing, ambient intelligence, or intelligent robots – and determine the ethical issues related to

[3] The concept of governance is defined by Jessop as "the reflexive self-organization of independent actors involved in complex relations of reciprocal interdependence" [8, p.1]. The most recent developments of the concept, in the context of the European Union, for example, qualify this mode of coordination as democratic, participative and pragmatic, with a focus on supporting collective action (Maesschalck, unpublished, pp. 3-4). According to Jessop, governance is now seen as an "important means to overcome the division between rulers and ruled in representative regimes and to secure the input and commitment of an increasingly wide range of stakeholders in policy formulation and implementation" [8, p.3]. This new governance model requires both groups (rulers and ruled) to engage in a social learning process [12]. Indeed, joined participation in collaborative problem-solving can lead to critical scrutinising of governing variables: goals, values, plans and rules [1].

[4] The Framework Programmes are the initiative of the European Union for funding research and technological development. For more information on the current FP (called FP7), see http://cordis.europa.eu/fp7/home_en.html/

[5] ETHICBOTS, http://ethicbots.na.infn.it/

[6] MIAUCE, http://www.miauce.org/

[7] SWAMI, http://is.jrc.ec.europa.eu/pages/TFS/SWAMI.html/

it: however, doing this ignores the foundation of the ethical issues: how, and in what context they were identified and raised, and what conditions are required to address them efficiently. That is to say, we are interested in determining what the conditions for efficient expression of the determined norm (that is, the effectiveness of implementation of a norm in the development of a particular technology) are, in relation to the ethical issues that are raised. If we are looking at the ethical issues of ambient intelligence, for example, different contexts will raise different issues, due to different personal, cultural, social, economic, political, and scientific influences. It also ignores the conditions required to resolve these issues. Instead, it assumes that the mere act of raising the issues provides the solution to them as well.

These presuppositions are common in European Union technical research projects, particularly those which incorporate specific ethical experts, such as MIAUCE and ACTIBIO[8]. Ethical considerations are, by themselves, insufficient to settle the problem of the relationship between ethics, technologies, and society, above all in the field of ICT and emerging technologies. As a result, the alignment between project development and ethics is far from being achieved. Additionally, the positivist approaches of the social sciences, for example, in their applied "sociology of morals", can reinforce the efficiency of instrumental methods (which are typically those of "social engineering" even if they do not specifically encourage cognitive and normative reflexivity).

The risk is that, by not addressing the institutional, cognitive, and rule conditions for effective integration of those considerations in the context of a technical project, the ethical considerations will be excluded from the technical rationale and treated as a totally separate domain. Ethics is separated from technology in the development process and is ultimately imposed rather than jointly developed. The consequence of this separation is a loss of impact and an undermining of the integral role of ethics in the application of technology.

In this paper, we address the conditions required to identify ethical issues in ICT: particularly concentrating on ethical issue resolution through considering the effectiveness of ethical reflexivity in the technological development process. In this way, the paper does not use a sectoral approach which reduces the debate to the application of a priori accepted principles. Thus, it avoids the problem of the approach becoming a reduced deduction of consequences from the application of such principles to a perceived context. To do this we favour an approach developed by Lenoble and Maesschalck [10] which allows for "opening of the cognitive framing" and "achieving reflexive governance"; hence, the title of our paper. This approach will be discussed later. Many of our examples are of European Union research projects, but the problems and their potential solutions are more generalisable to all technology development.

3 The Challenges for Ethics in ICT

In looking at how we can define a new reflective, deliberative, and ethical governance, we will specify a theoretical framework for improved governance mechanisms that identify and address potential ethical issues arising from new and emerging ICT.

[8] ACTIBIO, http://www.actibio.eu/

At the same time we remove the separation between ethics and technology, and between the theoretical justificatory approach to determining ethical issues and the application of ethical reflexivity in resolving those issues.

Practically, the main challenge that is investigated in this paper is of a profound lack of background: a strong push for technology development too often obscures the need for any deep ethical consideration that would take place even before a technical project is funded, developed and deployed. Some efforts have, however, begun to consider ethics and ICT in the Ambient Intelligence (AmI) domain that adopt different approaches: analysis from scenarios (e.g. in PEACH[9]), or "ethical review" panels (set up after the project has started, e.g. in MINAmi[10]) that consist of "ethical experts" who may come from a completely separate community.

The reflexive articulation of ethical norms and cultural contexts raises many problems, the first of which is the condition of an ethical reflexivity[11]. This challenge is natural, since the researchers and technical developers of ICT systems focus mostly on the technical and economics challenges before them. They not usually aware of potential ethical issues because they see ethical considerations and analysis as an obstacle to either technical or economic development or both.

In short we must first analyse not so much the problem of determining solutions to ethical issues. Rather, we must settle the conditions for raising ethical questions. We must develop a new approach that authorises a real reflexivity which allows for a questioning of the integration of ethics into complex technical systems. The obligations set out by economic constraints, interests concerned with the influence of experts, the general impression of the inevitability of technical projections, social requests, and consumers' needs make it increasingly difficult to define the conditions needed to ensure a critical perspective that can respect the moral autonomy requirements for thought.

We do not mean that existing criticisms do not allow for a certain reflexivity. We argue nevertheless that these criticisms generally show a tendency to restrict ethics to a categorical field. They sacrifice the existence of tension in the name of flattering pragmatism, they are satisfied with ad hoc answers to artificially isolated specific contexts, and they are conditioned or influenced by the reigning instrumental rationality.

The danger is to limit the debate to the scientific perspective alone[12] and to shun an approach based on technology assessment that debates both the meaning and the ethical, cultural and social challenges. Instead of initiating an inclusive debate on the nature of the different forms of knowledge and vision of world, discussions limit the debate by adopting a positivist and, more often than not, reductionist approach that leads to cognitive closure. Hence how to elicit the cognitive opening-up required for a

---

[9] http://www.peachbit.org/

[10] MINami (MIcro-Nano integrated platform for transverse Ambient Intelligence applications, an FP6 project).

[11] Reflexivity may be defined as the capacity of actors and institutions to revise basic normative orientations in response to the evolution of economic, techno-scientific or political systems and to shortcomings in current modes of regulation. This reflexivity is not given, however, as is clearly shown by the growth of science and technology.

[12] Hence the importance of expertise, and the tendency among politicians to favour traditional, "top down" governance of activities in which risks are involved.

genuine reflexivity that would allow us, as Ladrière [9] puts it, to extract the existential and the political meaning from the objective meaning?

The economists' answer appeals to the industrialists, for it confirms their practices and habits. Positivism has become so potent these days that the Enlightenment project of emancipation through reason is, for the most part, either rejected or ignored. In its place appear instructions on how to increase people's power over social processes that have been reduced to the status of objects. Hence again there is a difficulty in controlling the rampant growth of technological innovations politically. Often as not, political institutions make do with a regulatory and financial framework inside a dynamic system that is accompanied by positive feedback that leads to overheating.

In this context, expertise, whether it is philosophical or scientific, becomes the indisputable new source of normativity[13]. The problems revealed are confined to a scientific perspective alone; this means that the challenges taken into account are confined to the realm of strict scientific rationality. Democracy is confiscated. One must be wary of any theory which tries to objectify the world we experience in order to predetermine the form of the world we share. There is a big risk that the possibility of genuine reflexivity will be stifled by a technological and scientific rationality that imposes its value system with, as a result, a dismissal of the prestige of moral reason.

What is at stake is of importance. Various forms of "sectoral ethics"[14] tend increasingly to reinforce the characteristics of social differentiation in modernity by proposing an internal, and specific, framing of moral problems. This risks the exclusion of other external and alternative framings. As a consequence ethics is disconnected from the design of the technological device. The lack of a concrete assessment grid that would outline the embedding of ethics into technological development makes this issue important.

Briefly, the European situation is currently as follows[15]: some European Commission co-financed ICT projects investigate ethical aspects, but ethical considerations are not included as a "matter of course" in the development cycle. In some cases, ethical experts are brought in at some stage in the project to assess the ethical implications. As a result ethics is often an "add-on", a sort of accessory and instrumentalised guarantee. It is neither properly integrated nor understood in its methods and objectives which are clearly very different from the method and objectives of science and technology.

Consequently, there is a strong need for the inclusion of ethical considerations before, during and at the end of technical and scientific projects, so that the technology "incorporates" and tackles the ethical side (within its whole concept and implementation). The risk is that, by not analysing the conditions (institutional, rules, or cognitive aspects) for the effective integration of those considerations in the context

[13] Normative is contrasted with its antonym, positive, when describing types of theories, beliefs, or statements. A positive statement is a falsifiable statement that attempts to describe ontology. A normative statement, on the other hand, is a statement regarding how things should or ought to be. Such statements are impossible to prove or disprove, thus forever banishing them from the world of the scientific.

[14] By "sectoral ethics" we imply that some forms of ethics are applied to very specific fields or disciplines. Examples could include nanoethics, bioethics, or computer ethics.

[15] These observations are intended to relate to European Commission co-funded projects that the ETICA and EGAIS projects is intended to review.

of a technical project, the ethical considerations will be excluded from the technical rationale and treated as a totally separate domain. The consequence of this separation is a loss of impact, and an undermining of the integral role of ethics in the application of technology. This is quite understandable since the technology can only be limited to the set of its rules (that is, objectivity, and the technical rationality which frames its vision and conception).

Ethics is never the answer (since ethics is always conditional). Rather, ethics is established in this dynamic movement of questioning, before the action and on a border, which separates our subjective existence (with its presuppositions, its preferences, its convictions, its hidden motivations) from the constraining externality (among them, economic, political, hierarchical, technical, and ideological constraints). A moral freedom of positioning is fundamental, since it is open to questioning its possibilities and conditions.

These issues are at the basis of this problem if we desire to take the fundamental changes that affect our world into account. Unfortunately too many projects see ethics as the answer, and thus incorporate technology assessment, value-sensitive design, and other expert-based ethical assessment of technical projects. In reality ethics is *the problem*.

4 Limitations of Technology Assessment and Ethical Expertise

The image of ethics as an answer leads to many "ethics of…" fields in which it is possible to talk about ethics in relation to a particular field. But where do we ultimately arrive? The result is always the same: the analysis of a context from a reconstruction that is limited by the expert's framing and expertise as well as *bounded rationality* [13], so that a full reconstruction of the context is impossible. Each issue identified and each approach for resolution decided on is characterised by fundamental problems.

All forms of technology assessment processes involve some sort of expert committee designed to give input on the potential impacts of the technology. Many of the more modern forms of technology assessment involve some sort of stakeholder input. They one or more of many tools available to gauge the concern of users, shareholders, or other interest groups. The inclusion of participants from outside the expert community and from the groups that are likely to be affected by the technology is very important not only for the identification of norms, but also the construction of the contexts within the technology. However, the norms constructed by both the experts and the stakeholder participants are in no way required to be ethical norms. In fact they are most likely to be societal norms and expectations of the target groups. Of course some of these may correspond to ethical norms, but there is no definite requirement within technology assessment for the explicit establishment of normative ethical horizons.

The ethical approaches that are used in technology assessment depend greatly on the context. However, it is safe to say that ethical approaches are not usually appealed to as such, even if some provide the underlying motives for carrying out the technology assessment. Consequentialism features highly in traditional technology assessment, such as those identified in 1977: "[Technology assessment] emphasises those consequences that are unintended, indirect, or delayed" [3] or in 1972: "Technology

assessment is an attempt to establish an early warning system to detect, control, and direct technological changes and developments so as to maximise the public good while minimising the public risks" [2].

Later on, however, more deontological approaches underpinned the ideas for incorporation of the public and other interest groups in the discussions regarding technology and the potential impacts of it on society. Normative technology assessment processes involve a particular focus on assessing technology against moral principles such as beneficence, respect for autonomy, justice, and harm prevention [15]. A virtue ethics-based approach[16] is rarely found in technology assessment (however implicit), because it relies on assessment of the processes and practices involved in directing technology rather than the technology itself.

In terms of reflexivity, technology assessment processes rarely involve any such process in their own procedures. With each type of technology assessment comes a structured approach that is followed. It often includes the selection of stakeholders and experts, and methods of conducting focus groups.

However, technology assessment could be used as part of a reflexion process within a project, allowing for a learning operation to take place and then the project to adapt to the findings of the reflexion, and to determine the conditions for effective integration of norms into the technology being developed. Real-time technology assessment does attempt to integrate some sort of reflexivity into its approach, by assessing the technology throughout its lifespan of design and implementation. However, this is limited by the primitive nature of early technology and the problem of choice of stakeholders. It is these limitations that really restrict technology assessment to being a tool to incorporate into an overall reflexive approach on a larger view of the technology and its ethical impact on society rather than for it to be used as the point of reflexivity.

Not only do ethical experts generally promote the closure of the cognitive framing, but they actively bring their own biases to shape any participation of the group. As particularly examined by Goven [6], there are two major challenges. First, expert bias is a problematic part of participatory technology assessment approaches. Second, the management of bias may create a sense of scientific unity.

Information sessions run the risk of establishing knowledge hierarchies without allowing participants the time to reflect adequately on the information being passed on. Even after the informing process is over, much of the discussion time is used for further clarification rather than establishing opinion and responses to the technology. This prevents "a thoughtful lay response" [6]. It inhibits the capacity of the actors to understand the issues and context fully: how can the actors have the cognitive capacity to assess the technology to the degree required purely as a result of the teaching and discussion of experts, without questioning the framing and context of the assessment process itself?

A further problem is that "the strategy of managing bias by ensuring the presence of both proponents and opponents [also] resulted in creating the impression of a unified scientific opinion" [6]. A "for or against" polarity is established in the group. The established experts may be unified and enthusiastic about the technology, and those

[16] Virtue ethics was first put forward by Aristotle, and focuses on the moral character of the agent making decisions rather than on the outcomes, procedures, or rules.

opposed to it may be given much less credibility (they may be accused of rhetoric, or find themselves without an authoritative voice to present their views). Goven concludes [6] that an even-handed approach, with both proponents and opponents present as experts, can still prevent expression of the full range of implications, since these experts could still well be operating within a particular framing (such as occupation, or background from a certain socio-economic status). They may simply serve to give the illusion of diversity while maintaining a closed framing.

Since effective ethical governance requires the opening of the cognitive framing, the problem of expert bias is a tangible one. There may be good will among the experts to properly inform the participants and to engage actively in discussion and democratic deliberation. However, the intrinsic way in which the participatory approaches are set up incite a particular framing for the process which is not subject to adequate reflection. The experts inadvertently end up biasing the forum even if they deliberately try to avoid doing so.

These problems are linked to the conceptions of framing that shape the technology assessment processes. With experts as the source of normativity, and the revealed issues confined to their perspectives, ethics becomes an accessory to the process. There is not proper integration of ethics, and there is an emphasis instead on asserting or justifying the normativity put forward by the experts. This is reflected in some of the analyses of the outcomes of technology assessment processes, which are discussed in the next sections of the paper. There, the agreed resolutions end up having little real effect on the actual trajectory of the project. The differing conceptions of framing also impede the will of those involved in asserting change within the project to actually make changes. Instead they are more likely to minimise the changes the recommendation requires if the framing in which they were made differs from their own.

Thus, technology assessment simply serves the technology: the experts reduce the normative horizon to something of their own construction and use stakeholder input to attempt to justify their decisions, or use stakeholders as guinea pigs to assess the social acceptance of the technology instead of questioning the social acceptability of the technology on the whole. This ultimately renders the form of assessment to a reduction to proceduralism. Although the approach provides a dialogue-based grounding of moral rules and a linking of the individual and community will, it nevertheless relies on a limited context, with a restricted relationship between rational justification of norms and their context of application.

5 A Critical Perspective

Every technological artifact is a construction which rests on some a priori rationale (e.g., social, political, or economic). Even if the construction is partially suggested by preliminary information on the behaviour of the objects, it reinterprets this behaviour starting from its own categories. The political impact of a technological artifact cannot thus be assigned to the artifact alone. The impact must be allocated to the techno-speeches which diffuse the technology, give it a specific meaning, and envisage specific uses for it. Data processing and innovations that are related to ICT, even if they seem to be binding on individuals, actually come to satisfy a need and to fulfil

a function that is largely dependent on the cultural features of the society in which they fit.

It is only from the condition of recognising the non-neutrality of ICT that one can start to change their cognitive framing and can start to consider ethical and societal issues. Without this preparatory step, the world and technology can only be interpreted within the restricted cognitive fields allowed by the framing (in this specific case, the technological framing). The result is to either negate any justification for ethical and societal considerations or to instrumentalise them and consider them as a means to obtain a sort of ethical guarantee and label.

All ethical guidelines share this challenge: they do not take into account the issue of their application, and so, most of the time they have no effect at all. The mechanism which consists of providing an answer expected by a given context (such as an economic or an industrial context) poses ethical questions, since the context itself becomes the justification of the social function of ethics.

This recognition of the non-neutrality of ICT nevertheless returns a realistic ambition of relativising instrumental rationality and aiming at political and societal control, which means also its rehabilitation into the world of social and cultural life. It is certain a priori of intelligibility which guides the technical steps. The immediately urgent issue is to correct the manner of approaching ICT development, particularly the approaches which separate the social approaches from the technological ones, and political approaches from economic and ethical. Too often the accepted responses are only the economic, political and institutional constraints. It is undeniable, for example, that policy-makers are fascinated by technology. Positivism continues to influence our political leaders, who are in a state of utter disarray in relation to the complexity of our world. A symptom of this tendency is the call to use technology in all areas of public policy – such as education, health, environment, administration – to solve the problems which affect our society, and afterwards to use an appeal to ethics to justify the decisions that were already taken (for example, through the use of a European ethical assessment of technical projects).

Thus we need to recognise that the possibility of holding a critical perspective does not mean we can ensure its reality. Indeed, many factors can prevent the effectiveness of its achievement.

6 Theoretical Consequences for an Ethical Governance

Every norm aims to institute a way of life that is judged to be rationally more acceptable. The formal rules that condition the rationality of this choice, such as calculation of optimisation, argumentative rules, or any formal mechanism, do not guarantee the transformation of existing ways of life. The achievement of an ideal way of life that is called for by a norm is conditioned by something other than the simple formal validity of the rule.

In reality, the norm can only be expressed by establishing a reflexivity on the perceptions of the ways of life that are lived by and accepted by those to whom the norm is addressed. To suppose that an adaptation of the dominant perception and the corresponding ways of life will happen automatically or will be linked directly to the simple implementation of a formal mechanism that conditions the acceptability of the norm is to misunderstand this reflexivity.

Proceduralism (i.e., rule-making) is insufficient. It is evident in that the arrangements that are needed in order to organise the reflexive capacity of the actors to identify the various effective possibilities on which the operation of the selection of the norm will be carried out are problematic. Whether a norm is effective in modifying a way of life in a rationally acceptable way presupposes an independence from the discursive procedures that are used to select what is rationally acceptable. All the procedural mechanisms and rational approaches to the determination of a norm cannot by themselves assure the modification of a way of life.

By increasing the capacities for reflexivity with regard to the conditions that relate to the production of the norm, the effectiveness of norm expression could be measured. This measurement could take place according to the incentives needed to enable the reflexive reconstruction undertaken by the actors, and driven by what motivates their attempts to institute a new way of life.

Without the organisation of this common reflexive capacity, and the form of negotiation it involves among the various norms to be constructed, the normative injunction risks remaining insufficient even if the objective is judged relevant and legitimate. The operation of judging the conditions of the choice of the rationally acceptable idealised way of life (that is, the rational determination of the norm that is supposed to enable the achievement of this objective, and the effective transformation of this way of life by the application of the norm) is distinct and asymmetric. Asymmetry is the way in which the social meanings of a norm are conditioned by an operation that cannot be anticipated by formal variables of reasoning (variables that condition the norm's relevance). Therefore every reconstruction of the process that was enacted by the production of a norm itself mobilises two operations which do not respond to the same conditions of production. The intersecting articulation of this asymmetry is the very focus of governance arrangements.

In order to undertake these operations, it is necessary to organise the reflexive capacity of the actors. This has to be done by constructing the capacities of the reflexivity. It should be done in such a way as not to presuppose it as already existing due to a formal method, such as argumentation, deliberation, debate, or discussion. All these formal methods presuppose their own conditions; as such, they do not necessarily involve reflexivity. It is therefore important to make sure that every application of a norm presupposes not only a formal moment of choice about its acceptable normative constraints, but a selection of the possibilities that is made according to the perception of what is an acceptable way of life within the community concerned.

However, without a negotiated construction of the moment of reflexivity that is specific to the conditions for the application of the norm, there will be no control of the process of the expression of the norm. It will be left to the dominant common culture to express it. What is often presented as the only effective choice is always conditioned by an operation of this sort, including the construction of deontological codes (that is, codes of behaviour or codes of practice). Criticism of this reconstruction of the reflexivity used in the construction of the social norm also affects the moral approaches to legitimacy. Economic theories often obliterate the operation of the choice of possibilities that already condition the effects of rational decisions[17]. Yet

[17] This blind point affects the rational choice theory framework.

deliberative or communicative approaches[18] also miss the challenge of providing the appropriate conditions to ensure an effective expression of the ethical objectives they intend to promote.

Institutional cooperative arrangements are necessary for the effectiveness of the expression of norms in concrete situations, as well as for the legitimisation process of the norm. These arrangements are a result of the contextual limitation as an inescapable part of the reflexive operator of modality.

The institutional arrangements for this reflexivity have to be established. This is the very aim of the ETICA project. This will help to overcome the fundamental limitations of existing ethical approaches, which ignore the fundamental issue of the moment of the application of the norm.

Determining these arrangements will allow actors and institutions to experience a learning process whenever they are confronted by an ethical issue. They will reflect on the success of the learning process, and reframe the context of the situation in order to establish a norm more effectively within the context. From a more official perspective, this experience will enable us to assess the effectiveness of the result of that process.

7 Overcoming the Limitations of Current Approaches

Overcoming these challenges is not simple. Bounded rationality imposes serious constraints on those involved in the ethical analysis of projects; it is one of the constraints that "limit public actors' capacity to adequately diagnose and cure […] problems" [11]. There is a necessity not only to require co-operation from inside and outside the technological development process, but to require a much fuller cognitive understanding "by bringing actors together from across sectoral, disciplinary, and other divisions of modern life" [11]. Coupled with procedural rationality, "the setting up of mechanisms to promote self-learning within organisations", this approach opens up "dialogue between all the parties concerned by a problem" [5]. It enables a reflexivity between the justification of a rule and the application of the rule within a practical context [4]. Only through opening up dialogue and co-operation among the currently separated ethical and technological groups will we be able to experience the required learning operation. However, opening up discussion is not the only criterion.

In many technological projects, public participation is unlikely to be adequate due to the problems of expertise and pre-existing power structures that are introduced by the participants [11]. Although rule-making (often called "proceduralism") offers some solutions to encouraging the democratic aspects of this process, it is insufficient to account for the internal power-plays and various external influences on such procedures.

Instead, we need to ensure a second-order reflexivity that allows project participants to test the governance process continually for social legitimacy. This enables "continued discussion and proofing through testing of ideas and comparison of results, including raising questions of distributive fairness and overall efficiency" [11], as well as genuine accountability of governance.

[18] Such as the procedural approaches of Habermas [7].

The other problem with a Habermasian proceduralist approach [7] is that it assumes that the rational justification of ethical norms (that is, the identification of the norms) brings with it the conditions for the implementation of the norms. The rational justification of a norm cannot, first, be arrived at by a process of consensus or compromise, nor, second, can it be decided by a majority vote by a democratic process. This approach presupposes that those who are to implement the norms have a will to be ethical.

Following in Lenoble and Maesschalck's footsteps [10], we cannot simply accept ethical norms as they are identified. Instead, we need to examine the construction of these norms, taking into account their relationship to the context in which they are to be implemented.

At this stage of our argumentation therefore, we wish to summarise: the main challenges that we have encountered thus far in European technology development projects are as follows:

1. There is a separation between ethical and technological communities
2. Expert and participatory approaches are insufficient by themselves to provide effective and efficient ethical governance procedures
3. There is a separation between the context of application of the norm and the context of the legitimisation of the norm
4. There is a problem with the reflexive relationship between the construction of the norm and the context.

Effective governance arrangements must thus address the construction of contexts and norms, the application of these, and the relationship between the construction of the norm and the context.

Progressive reflexive governance requires a threefold approach. The approach proposes that the actors involved organise themselves in a way that enables them to be reflexive about their own construction of the framing, context, and norms. This approach involves the previously discussed learning process. It requires the actors involved to assess their own framework for the selection of governance practices, so that they can decide whether these practices are appropriate to use. "A form of governance would qualify as reflexive if it favoured the success of the learning operation required to satisfy the normative expectations of participants in a collective action" [10].

The learning operation is particularly required after encountering an external "shock" factor, that is, a problem that has arisen which requires a decision to be made. The decision-making process here requires choosing a real-life solution that is supposed to optimise the ideal objective that is illustrated by the anticipation of an idealised way of life. The involvement of this anticipation of a normative horizon is very important in ensuring that the values involved in the decision are ethical values. This requires, however, that the decision-maker ensures that the possibilities of the context within which the idealised way of life is to be achieved are not exhausted. He or she transforms the context in order to incorporate the new ideal norm brought about by the "shock". Two examples follow. One is the identification of minority interests in a project: how would deaf people use the technology that is being developed in the project? Another example could be identification of the dual-use nature of a particular technology. These sorts of decisions require the participating actors to "learn" and

shift their framing by transforming the context, so that the construction of the norms and context take these new developments into account.

Lenoble and Maesschalck [10] advocate a contextual pragmatist approach, which requires a self-capacitation on behalf of the actors, allowing the actors to identify and understand how their own identity impacts on the decisions and tools they make and use. This understanding allows the actors to build a representation of themselves, the context, and the relationship between the two. However it is not this relationship between the actors and their own selves, but the relationship between the actor, other actors, and the institutional mechanisms that form the framework within which they interact that is key. These theorists wish to go beyond requiring the actor to have the will to be ethical. They desire an effective expression of ethical norms to take place (and to result in behavioural change). Finally, they advocate a mechanism for "vigilance" which is "designed to assess the extent to which the institutional mechanisms set up by the actors, in interaction with each other, have made it possible […] to carry out the hoped for adjustments and learning effects" (ibid, [10]). This monitoring process throughout the duration of a technological project would permit a continual assessment of the effectiveness of the governance framework and the capacity of the actors to "commit themselves" to cause ethical change within the project's own trajectory.

This approach satisfies the requirements for ethical governance. It allows for the opening up of cognitive closure, through inclusive participation of actors from across many backgrounds. Yet it also confronts the problem of pre-existing power structures. It continually assesses the capacity for the actors themselves to reflect on their own participation, background, and context so that the effect of these pre-existing structures is minimised. It evaluates the usefulness of the framework and tools within the framework that are being used, and provides an environment in which an external "shock" is efficiently dealt with while preserving the ability to effect ethical change in a technological project.

8 Conclusions

This paper addresses the background behind a need for a new governance approach in technological development projects. It establishes the separation between the ethical and technological communities and the limitations of current approaches, and it proposes an approach that escapes the limits of formalism by allowing for genuine second-order reflexivity. It is necessary to construct the framing of the context in relation to the norm, and to open up the context for a feedback mechanism to enable a reflexivity on the opening of the framing.

In order to do this, we have proposed the use of the Louvain school theory of Lenoble and Maesschalck [10]. This school of thought provides a framework in which we can construct a two-way relationship between the norm and the context. Thus, we can overcome the limitations of current governance approaches and achieve a second-order reflexivity.

This theoretical development is a work-in-progress for the authors in conjunction with the EGAIS and ETICA EU FP7 projects. It is in these projects that we will further develop and test the approach outlined in order to establish an effective ethical governance approach for future technology projects.

References

1. Brabant, C.: For a Reflexive Governance of Education: the Example of Home Education in Quebec. In: Proceedings of the European Conference on Educational Research, September 19-21. University of Ghent (2007)
2. Cetron, M.J., Connor, L.W.: A method for planning and assessing technology against relevant national goals in developing countries. In: Cetron, M.J., Bartocha, B. (eds.) The Methodology of Technology Assessment. Gordon and Breach Science Publishers, New York (1972)
3. Coates, J.F.: Aspects of innovation: Public policy issues in telecommunications development. Telecommunications Policy 1(3), 196–206 (1977)
4. De Munck, J., Lenoble, J.: Transformation in the Art of Governance: A Genealogical and Historical Examination of Changes in the Governance of Democratic Societies. In: De Schutter, O., Lebessis, N., Paterson, J. (eds.) Governance in the European Union, pp. 189–212. Office for Official Publications of the European Communities, Luxembourg (2001)
5. De Schutter, O.: Proceduralising European Law: Institutional Proposals. In: De Schutter, O., Lebessis, N., Paterson, J. (eds.) Governance in the European Union, pp. 189–212. Office for Official Publications of the European Communities, Luxembourg (2001)
6. Goven, J.: Citizens and Deficits: Problematic Paths toward Participatory Technology Assessment. In: Proceedings of the Summer Academy on Technology Studies 2002, Inter-University Research Centre for Technology, Work and Culture, October 29, pp. 1–18. University of Klagenfurt (2002)
7. Habermas, J.: The Theory of Communicative Action. Translation: T. McCarthy. Polity, Cambridge (1981/1984)
8. Jessop, B.: Governance and Metagovernance: On Reflexivity, Requisite Variety, and Requisite Irony. Department of Sociology, Lancaster University, Lancaster, UK (2002), http://www.lancs.ac.uk/fass/sociology/papers/jessop-governance-and-metagovernance.pdf/
9. Ladrière, J.: Philosophie politique et philosophie analytique. In: Ladrière, J., Van Parijs, P. (eds.) Fondements d'une théorie de la justice. Essais critiques sur la philosophie politique de John Rawls, p. 222. Éditions de l'Institut Supérieur de Philosophie, Louvain-la-Neuve (1984)
10. Lenoble, J., Maesschalck, M.: Beyond Neo-Institutionalist and Pragmatist Approaches to Governance. In: REFGOV working paper, UC Louvain (2006)
11. Overdeest, C.: The Open Method of Coordination. In: New Governance and Learning: Towards a Research Agenda. Working Paper, The New Givernance Project. University of Wisconsin-Madison (2002)
12. Schön, D.A.: The Reflective Practitioner: How Professionals Think in Action. Temple Smith. London (1983)
13. Simon, H.A.: Models of Bounded Rationality. MIT Press, Cambridge (1982)
14. Wright, D. (ed.): Safeguards in a World of Ambient Intelligence (SWAMI). Final Report (2006)
15. Verbeek, P.-P.: Persuasive Technology and Moral Responsibility: Toward an Ethical Framework for Persuasive Technologies. Persuasive 6, 1–15 (2006)

Section 2

Virtual Technologies and Social Shaping

Virtual Technologies and Social Shaping

David Kreps

Information Systems, Organisations and Society Research Centre
University of Salford, Salford, Lancashire, UK
d.g.kreps@salford.ac.uk

Virtual Technologies have enabled us all to become publishers and broadcasters. The world of information has become saturated with a multitude of opinions, and opportunities to express them. Track 2 "Virtual Technologies and Social Shaping" of the 9th Conference on Human Choice and Computers (HCC9) explores some of the issues that have arisen in this new information society, how we are shaped by it, and how we shape it, through i) two papers addressing issues of identity on social networks (Pearson and Burmeister), ii) two papers about the glut of information now available on the web and strategies for dealing with it (Lenarcic et al. and Westwood), and finally iii) a paper on the tricky problem of virtual property theft (Patterson et al.).

In the first pair of papers, Erika Pearson's "Making a Good (Virtual) First Impression: The use of visuals in online impression management and creating identity performances" argues that visual elements are becoming an increasingly important component of identity performance on social networking sites. Working from a narrative approach to identity, this paper explores how images on SNS are used both as part of an impression management strategy to present identity, and as signs that others on the site can read and interpret as they develop an understanding of the identity of others. Drawing on interview data conducted with users of the Livejournal SNS, this paper argues for a growing visual literacy among users of social networking sites. Oliver Burmeister, meanwhile, in "Virtuality improves the well being of seniors through increasing social interaction" argues that virtual social interaction amongst seniors is strengthened through face-to-face contact. While confirming previous studies that have shown the strengthening of virtual friendships result from physical meetings, this study also showed that virtual face-to-face meetings have a similar benefit. As more seniors around the world are encouraged to stay at home longer, rather than enter institutional care, virtual sociability is being shown to provide the necessary social inclusion benefits for particularly mental well being, that has been identified in psychological and sociological studies of seniors.

The democratisation of the web brought about by the social networking phenomenon and the associated web 2.0 tools enabling easy web publishing for the masses not only brought about the blogosphere, but additionally the phenomenon of 'dead' blogs, and the primacy of search – and its greatest purveyor, Google – in the day-to-

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 115–117, 2010.

day use of the web. The first of these issues is explored by John Lenarcic and Pradipta Sarkar in their paper, "The Tragedy of the Virtual Commons as manifested in the Death of Blogs." The life span of weblogs is investigated with reference to Lanham's view of the "Economics of Attention" and Hardin's conception of the "Tragedy of the Commons." It is advanced that the unfettered buildup of inactive blogs is leading to a surfeit of information that effectively disables potential readers due to an excess of choice. One factor indicating healthy activity in a blog is postulated as being sufficient feedback from readers that leads to the emergence of an ongoing social network. This is viewed as an example of a virtual technology shaping social groups. Research-in-progress is outlined that refers to observations of various film music blogs derived via the case study method, featuring a focused commentary on one that has subsequently been a victim of death in the blogosphere. In this case, the forced extinction of a blog is taken to be an example of human foibles influencing the download spiral of one instance of a virtual technology. Sean Westwood, explores the second issue, Search, in his "How to measure public opinion in the networked age: working in a Googleocracy or a Googlearchy?" The rise of the internet has transformed information acquisition from a top-down process originating from media elites to a process of self-selection and searching. This raises a fundamental question about the relationship between information acquisition and opinion formation: do the processes occur in parallel or as part of a self-directed feedback loop? That is, do we look for information to make opinions, do we look for information to support our opinions, or do we do both simultaneously? Analysis using Google search and polling information from the 2008 US presidential election suggest that public information queries are reflective of polling data and election outcomes. The sheer quantity of search data on political terms also suggests that public information desires may surpass standard assumptions of public political sophistication.

Finally, in this virtual setting where we are all publishers, the tricky issue of ownership, and intellectual property, is addressed by Nicholas C. Patterson and Michael Hobbs in their paper, "A Multidiscipline Approach to Governing Virtual Property Theft in Virtual Worlds." The crime of virtual property theft has become a serious problem in virtual worlds in recent years. Players of these games are repeatedly falling victim to this crime, with little or no repercussion for the offender. Virtual property often has a substantial real world monetary value and the theft of such items impacts greatly on victims. The problem of virtual property theft is complex, involving many legal, regulatory and technological factors. As such, trying to address this problem in a single dimension is not sufficient, each factor need to be addressed with a multidisciplinary approach. In addressing this problem, this paper provides a model for describing the issue of virtual property trading and the issues associated with virtual property theft. The paper also proposes an approach for handling virtual property theft based on improvements to laws related to virtual property and theft, improvements to the virtual world software components and better regulation from governments.

Acknowledgments. As track programme chair, I would like to thank my co-chairs, and all the programme committee members for their efforts in supporting the organisation of this track. In this respect, I would especially like to acknowledge the following for their intellectual and organisational inputs: Niki Panteli, Martin Warnke, and Claus Pias.

Making a Good (Virtual) First Impression: The Use of Visuals in Online Impression Management and Creating Identity Performances

Erika Pearson

Department of Media, Film and Communication, University of Otago,
P.O. Box 56, Dunedin, New Zealand
erika.pearson@otago.ac.nz

Abstract. This paper argues that visual elements are becoming an increasingly important component of identity performance on social networking sites. Working from a narrative approach to identity, this paper explores how images on SNS are used both as part of an impression management strategy to present identity, and as signs that others on the site can read and interpret as they develop an understanding of the identity of others. Drawing on interview data conducted with users of the Livejournal SNS, this paper argues for a growing visual literacy among users of social networking sites.

Keywords: Goffman, Performance, Identity, Impression Management, Social Networking Sites.

1 Introduction

The rise of social networking sites has been well-documented in both the academic and popular literature. Much has been written about such sites [1], from the earliest BBS through to Facebook as the current SNS-*de-jour*, and how such sites are connecting individuals into communities of interest that may have little resemblance to make-up of their face-to-face, embodied social networks. However, much of the existing literature focuses on the textual nature of these SNS – 'words on a screen,' to paraphrase's Turkle's famous phrase [2]. Whilst text is still arguably the dominant element in facilitating online social interaction, platforms such as Facebook, Livejournal, and even Twitter include technological infrastructure that makes it easy (in many cases, simply point-and-click) and subsequent subtly encourage [3] users to include visual information, such as photos, either into their textual flow or onto the site that surrounds and frames the written exchanges.

This paper argues that such visual components contribute to the overall creation of a virtual identity, an online social self that engages with and is a part of the online virtual community, as part of the visual component's plural function in the online social space. By careful selection and control of these visual elements, individuals engage in a form of virtual impression management of their online persona or personas. Other participants in the online group can then read these visual cues and extract

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 118–130, 2010.

from them information that helps create an impression of the disembodied other with whom they are interacting. These visual cues can be read in isolation or as part of the overall semiotic structure of the online presence, to create their impression of the others' identity. This new semiotic richness is further enabled by the growing ease of use and sophistication of the tools that allow users to easily collect, manipulate, upload and engage with such images.

To support this argument for a growing visual sophistication in identity construction and performance among SNS users, this paper will draw on data collected during a study of Livejournal users regarding their use of images as part of their social activity on the site. This paper argues that in the relationship between users and SNS, users are becoming increasingly skilled not just in reading such visual information within a virtual social context, but also in the creation and deployment of such visual cues to help facilitate the development of particular virtual identities – that in fact these visual cues are being deployed as part of deliberate strategies of online impression management. This paper concludes by discussing some of the implications of visuality and impression management for the future of online identity formation and social group behaviour.

Firstly, however, it is necessary to explore further these notions of identity and impression management as they relate to online environments.

2 Identity and Impression Management

Identity as a concept encompasses a vast range of perspectives and ideas, and the disembodied nature of the internet further complicates issues of definition. In regards to online social networking, it may be useful to consider identity as the development of a biographical narrative that is constructed and reconstructed through relationships with the platform of interaction and with the wider social network within which it is situated [4, 5]. This definition, though not without its problems [6], encompasses the notion that identities, whether embodied or not, pseudonymous or not, have a history and a shared experience within their context [7] and deploy common signs and marker or props that helps enforce a consistent and decodable presentation of self within the wider social context. The construction and reconstruction of an identity narrative then becomes part of what Goffman [8] refers to as an everyday performance.

By taking this approach to notions of identity, the relation to issues of impression management becomes clear. Impression management is a broad term used in a number of fields to refer to the strategies and processes employed by individuals to influence how others perceive them [9, 10]. Impression management may be carried out for instrumental reasons, such as to evoke a particular response from others, or it may be used for more expressive means, such as creating a general presentation of self which would persist beyond a single encounter and which would both facilitate the social contact and create for others an understanding of identity that tallies in some way with the individuals own claimed or desired self-identity [11].

Though these two conceptions of impression management overlap significantly, it is this latter form of self-presentation that this article will primarily engage with. The works of Erving Goffman and his dramaturgical approach to identity and issues of impression management will form the basis of the analytical framework of this study.

Such an approach to examining identity presentation in SNS is not novel [12, 13] [14], but this particular study will look at how users of SNS deploy visual cues as part of a performance of a persistent identity narrative that they construct as part of their online activity.

Impression management relies heavily on the specific context in which the social interaction is taking place. I would argue this to be especially true in online interactions. The 'rules of conduct,' to borrow the phrase from Goffman, are the obligations and constraints that frame the interaction. These may be explicit laws or moral obligations, or more implicit honorifics or acts of etiquette [11]. In an embodied interaction, these rules of conduct are part of the shared cultural and social context of the space. Online, however, the participants may be situated in quite different contexts – for a successful social interaction, and thus successful impression management, the rules of conduct must be clear to all parties in the virtual environment. Thus rules of 'netiquette' can be seen to be part of wider context in which impression management occurs. However, these 'rules' are not universal, but are different between groups and shift over time or with changing context [15]. Therefore, in considering online impression management strategies, it is important to remember the shaping effects of such 'rules of conduct.'

It is also arguable that online impression management strategies are influenced by the channel of communication used to support the social interaction. Different rules of conduct, and indeed different social connotations can be ascribed to similar behaviours on different channels of communication or different social networking sites (think for example the different activities one might expect to find on MySpace as opposed to LinkedIn). Again, to adopt Goffman's terminology, we choose different impression management strategies depending on the stage (or SNS channel) on which we are performing, the props we have available (or are allowed by the site architecture) to deploy, and the audience we are expecting to engage with. For an individual to develop an impression management strategy, they have to have some understanding of the other that they are trying to make an impression on (often by 'reading' the impressions or identity narratives already given out in a particular environment, and then modulating their own impression management strategies accordingly).

Goffman's work was originally based on face-to-face contacts, with all the subconscious cues (such as dress or body language) providing both supplementary identity information and feedback for the performance of a particular identity. But as Browning and Stephens note:

> It was assumed that ICTs would provide less 'social presence' and would filter out essential cues for interpreting what was going on, and there would be less rich media than face-to-face communication. Yet there is a growing collection of studies showing that people can use 'lean' media for effective social interaction… [11, p. 69]

People using ICT, and particularly CMC, adapted their performance and their impression management strategies to the new medium. For example, in purely text-based environments such as BBS and IRC chat, participants used emoticons, a consensual set of symbols (such as :D and /o\) to reintroduce social and expressive information once conveyed by body language. As participants became conversant with the shared

symbolic vernacular of these new virtual environments, they adapted their impression management strategies to take advantage of these new modes of expression [16].

It is the core argument of this paper that this modification of self-performance and impression management strategies to incorporate new visual modes of communication is driving the shifting visual literacy of online participants within the context of specific online social networking sites. With this claim in mind, this paper will now explore one example of the use of images in online identity and impression management.

3 Impression Management and Visuals on Livejournal

Livejournal [17] is a social networking site that has been running since 1999 that allows users varying levels of access to customize their page on the site depending on the type of account they hold (paid, ad-supported, or free). This customization includes the option to use pre-made or to develop their own unique backgrounds (known as layouts), and to have different numbers of small, 100x100 pixel images, referred to as userpics or sometimes as icons. Each user (who often uses the site under a pseudonym) can choose from the list of pictures they have uploaded a specific userpic for each separate post or comment they make on the site. This differs from other popular SNS such as Facebook, which only allow a user to associate one image with their account or username at any one time.

Beyond these varying visual customization options, Livejournal also supports the ability for a user to embed images, video or other visual content into their posts and comments, either through html coding, or through a WYSIWYG client built into the Livejournal user interface. Third-party clients also offer users different point and click tools to help them embed such content into their posts.

These three forms of visual content – layouts, userpics, and embedded content – mean that Livejournal has the capacity to support a visually lush virtual environment. For this paper, the focus will be on how users understand these images (both the ones they create and the ones they see made by others) in terms of identity and impressions management strategies.

The follow data are from open-ended, semi-structured interviews with a subset of Livejournal users who participated in a wider study of the uses of images of Livejournal that was conducted in 2007. A link to a survey had been circulated among English-speaking Livejournal users using a variation of snowball sampling where those who had taken the survey then posted a link to all their friends on the site, and so on. These users then elected to click the link and complete the survey. Interview subjects were then selected at random from the survey respondents who had completed an opt-in section of the survey indicating their willingness to participate in follow-up interviews. All subjects were English-language speakers over 18 years of age who used Livejournal. Due to the sampling method (particularly self-selection during the snowball phase), and the relatively small number of interviews (survey: N=610, interviews: N=21), it must noted that these results may not be indicative of the Livejournal community as a whole[1], but instead may reflect the subset of the user group who

[1] Particularly the large Russian/Cyrillic language community who were excluded by the English-language nature of the study.

actively use or consider their own image strategies and were motivated to complete the survey. That said, their responses still give a tantalizing insight into the image use strategies of those who can manipulate and work with Livejournal's capacity to support visuals.

The aim of the initial survey was to attempt to gauge the extent to which images are being used, in terms of both creation and consumption, but it is in the interviews where motivations and reading strategies are described by the users themselves. Because of this, and because only a relatively tiny number of survey respondents participated in the subsequent interviewers, this paper will concern itself solely with the interview data. The interviews were conducted via email, and the textual transcripts of the interviews were then coded around a small number of core themes.

All interviewees had been using Livejournal for between three and seven years, with the majority of them having been using Livejournal for approximately four years at the time of the interviews[2]. The interviewees reported a reasonably diverse range of self-described visual skills in both reading and creating images.

Whilst the interviews covered a wide range of issues regarding visuals and Livejournal, it is the discussions regarding identity and impressions management that have been excerpted for closer analysis. In particular, two key themes are relevant to the question of impression management, visuality, and online social networking – how users manage their own visual performance, and how they read the visuals put forth as part of other's online performances. Interview data was coded under these two themes is excerpted below and discussed in terms of identity, performance, and impression management.

The first theme taken from the interviews relates to how the users select and control their visual performance in Livejournal to promote or maintain a certain desired facet of their online identity. It must be noted that throughout the interviews, it was clear that users found it hard to articulate and reflect upon their own identity construction practices as they pertain to images. This may be in part due to the 'backstage' nature of such identity construction practices, as opposed to the 'frontstage' nature of the interviews with an interviewer that was personally unknown to them.

Even so, the interviewees did betray some of their strategies for impression management, often as they compared the perceived strategies of others with their own. In this regard, the interviewees often began by noting the expressive impact of images in their Livejournaling activity. For example, one respondent noted:

> "….I tend to associate different userpics with certain kinds of moods or to the same extent, to the kind of content of a specific post...and rightly or wrongly, assume that any readers of my LJ [Livejournal] will do the same!" Respondent #11

Later in the interview, the same respondent elaborated further on this emotive connection in regards to their wider reading habits:

> "…over time, I've come to associate specific userpics with certain members of my F-list [friendslist]…. Quite often, I scan my list to see who has updated, and will whiz by icons that I don't recognise (those

[2] Interview excerpts have been included 'as is' including typographical and grammatical errors. Editorial clarification is provided as needed in [square brackets].

> used by LJ users posting in a community, for example), and will stop at ones that are familiar to me - those of my friends. Occasionally this backfires as another user may have the same icon as one of my LJ friends and for a second I'm confused as to why I don't immediately recognise the writing style or contents of the post." Respondent #11

Similar comments were made by a majority of the interview subjects, and it was one of the dominant themes of the interview overall. In terms of images as semiotically rich means of communicating identity and helping to manage their impression, two ideas are suggested. Firstly, that images, particularly images appended to accounts such as userpics/icons, can be read in multiple ways simultaneously – as both identity marker for the account overall (associating particular userpics with particular otherwise disembodied users), and as additional information relevant to the *specific* post (association with moods or content). This may be specific to Livejournal, where the architecture of the site enables the user to select userpics off a pre-loaded list for each post or comment, but also has implications for readership on sites that force a more static visual code onto their users.

Userpics, and to a lesser extent, layouts, are also seen to be part of a larger strategy of online identity and impressions management that transcends the boundaries of a specific SNS, and even the distinction between the virtual identity and community and the embodied identity and community of the user. For example, these three quotes are from three different interviewees, but all play on the common theme of consistency in the visual construction of an identity narrative in a social space.

> "I mainly use a very recent photo of myself as my default icon! I feel, personally, that it's important that I BE who I am - to the extent that I can be - online. Of course, I want it to be the most flattering photographic representation, yet I feel it needs to be authentic." Respondent #15

> "I stick to one icon, which I tend to use on lots of different services (i.e.; My LJ icon is also my Facebook image, or at least they're both from the same photo)….I want my different accounts in different places to be seen as parts of a whole. I only use different services because of what they provide, not to present different versions of myself." Respondent #20

> "I had my own icon with my LJ name on it and yellow daffodils. When I deleted it [old LJ account], I really missed the icon too. A friend of mine made a new one with my new LJ name and yellow daffodils. The funny thing is that when I commented on other people's journals some of my old 'friends' recognized me, even if my LJ name is very different now. I guess I am the one with the daffodil icon. "Respondent #6

For these respondents, the visual information conveyed in their userpics is part of a wider strategy of identity association that persists across time and even SNS platforms, and which continues despite changes in username or account name, which would be assumed to be a primary source of persistent identity in cyberspace. The user image can, in very limited ways, be thought of as analogous to a face, a

consistent and instant visual identity cue (however, care must be taken not to over-extend this metaphor). Users select and maintain certain image associations over time, even cultivating otherwise generic visual cues (such as with the daffodils) to indicate personal identity within specific social groupings. These images become 'owned' in the sense that they are invested with the shared history developed along with the image's usage – they in effect become a marker of a persistent, recognized identity.

Of course, for persistent identity management strategies to function, they need to be read by others. This leads into the second theme that arose in the interviews, how others engaged with these identity cues and management strategies.

The interviewees were able to far more easily articulate their strategies for reading and understanding the use of visuals and images by other users (perhaps, again, because reading is also a frontstage act). They highlighted two key elements that recurred in how they see others using visual in Livejournal – for identification, and to decode personality traits.

As noted earlier, it was at first thought that social interactions conducted online using services such as SNS would have a thinness, a reduced 'social presence' as the mediated and virtual nature of the connection stripped out the non-verbal cues such as expression and body language, dress and deportment. Yet these interviews, and similar studies on other online cohorts [18] suggest that these users are beginning to put these cues back into their online interactions by using specific visuals elements as markers of a particular identity performance. This tallies with the dual encoding of information interviewees seemed to suggest as noted above – that alongside context-specific markers of mood or relationship, images also functioned in a more general sense as a quick way of saying within the shared social space that 'this is me.'

For example, the interviewees often made comments such as:

> "I have difficulty matching images to names, so if people are frequently changing their icons, I can't use them for identification. I have to go find the username written somewhere on the screen instead. "Respondent #20

> "I also most identify people on LJ with one or more userpics – I think people in general so visually orientated that it's tough to NOT associate the user with some kind of visual at some point." [original emphasis] Respondent #14

This last comment is particularly interesting, in that it suggests a substitution behaviour between online and offline identity strategies – this notion of substituting the face/body and associated non-verbal cues with a small set of static images was implied by a number of the interviewees. One interviewee went further:

> "[visuals like userpics are]…little non-verbal clues that are so sorely missing in pure text; to me, they are online equivalents of body language and other secondary visual cues." Respondent #13

This user made a direct and explicit correlation between visuals and substitute non-verbal cues – however, they also ranked such cues secondary to the textual communication, the words of a screen, which were also emphasized by many respondents to be the key information on the page.

The identifying use of images went beyond mere association over time. An even more prevalent theme was the assumptions these users made about other users based on the visual content of their journals. It is here that issues of impression management, particularly in terms of those knowing who are the intended recipients of the impression management strategy, come to the fore.

Users infer a lot about other users through their use (and perceived 'misuse') of visuals, especially layout designs and embedded visuals. Many of their readings of such visuals seemed based on ingrouping and outgrouping judgments – members of 'my' group have this aesthetic and use these visual elements in these ways, and members of that group use other elements. For example:

> "A highly personalised layout conveys the information that the user is highly computer literate (unless there is a credit to someone else) Sophisticated or low key, understated layouts convey that the user is older and perhaps more educated (if reflected by content) Bright pink layouts with Hello Kitty pictures convey that the user is likely to be younger/not sophisticated. Often choice of layout gives an idea of whether the user may be quite extroverted or introverted. Nondescript layouts are less informative but could convey that the user is either not very engaged with lj at all, or not very visually orientated." Respondent #7

> "If their icons all blink, move, or are animated, i am inclined to think they are selfish and pushy--they are forcing their annoying "look-at-me, look-at-me" icon into others' space. If their icons are all anime, or television-derived, i'm inclined to think they are disinterested in real sharing, fundamentally uninteresting, and probably shallow. if they post a lot of memes that have graphics, i'll come to the same conclusion--they're uninteresting. On the other hand, if they post updates of their lives with photos for illustration, i feel i'll understand them better because i can *see* a little glimpse of what's going on--what their space is like, what they look like (a face behind the words), what they're up to." Respondent #12

> "I tend to immediately like people who reference cultural artifacts (books, movies, etc) I like in their icons." Respondent #16

In this sense, these visual might be better considered not in terms of an isolated individual identity, but as part of a social identity that the individual user cultivates and manages using such images and design strategies as appropriate to that social group to declare 'this is where I belong.' One interviewee was able to articulate more fully these multiple purposes of images in regards to an individual's plural identities:

> "Some icons are used to indentify [sic: identify] with a particular community, others are more generic. Some posters use one self-identifying icon all of the time, allowing them to move between communities with ease. Photos and artwork often open dialog in communities, which can be fun and interesting, or divisive and

> controversial. It depends on the content. Overall, I believe that visuals in any form are part of who we are on LJ as people and as individuals in larger groups." Respondent #17

Userpics in particular often appear to function as a marker of affiliation by drawing on source materials and visual tropes and cues specific to particular subgroups. Tarkowski, in his analysis of userpics and peer production, also highlights the intersection of cultural and individual identity and notes the influence of popular culture in these images [19]. As noted earlier, these users seem to make these image do the work for multiple roles: identity marker, a claim to social belonging, a reference to a shared interest or popular culture icon, a sign of a mood or even a denotative part of the text (i.e.: "this is the kind of dress I'm talking about).

The strategic deployment of images within a specific social group and through a channel with particular technological capabilities involves a multi-leveled understanding of the role such images play in context. A single image can be simultaneously a marker of identity, a signal of in-grouping, and an expression of emotion or context. Rebaza noted a similar multiplicity of meanings in Livejournal userpics [20]. Other users then decode (or fail to decode) one or more of these layers in ways that make sense to them, and from repeated interactions and continuous cycles of coding and decoding of visuals alongside text and other content, slowly develop an understanding of each other in the virtual environment.

4 Discussion

Though these interviews dealt mainly with the interviewees own perceptions of their visual reading and writing strategies in their own online social contexts, their comments suggest some interesting implications for the future of user-generated multimedia and social networking and strategies of online identity and impression management.

Firstly, as in other forms of impression management, understanding the rules of conduct as pertains to a particular social network or community is vital to creating an impression strategy that will be read positively or as intended. As many interviewees emphasized, certain aesthetic preferences, colour palettes, or subject choices led them to read the sender of such images in certain ways, some more desirable than others — young, immature, of like mind, etc. A recurring theme across the interviews was how quickly a new contact could be disregarded if their presentation included undesirable images or aesthetic in layouts or userpics. By knowing the rules, and more importantly, in having the visual skills to engage with and conform to those rules in ways that were still unique, a user could present an identity that would garner a positive reaction and thus further engagement from others in the network. In other words, they had successfully used images to communicate their understanding of the 'rules of conduct' for that social group.

Secondly, it must be reiterated that the technological platform and channel of communication (in this case, Livejournal) also has significant impact on the strategies chosen by virtue of the kinds of visual control it allows — from differing numbers of userpics depending on account type, through to varying levels of sophistication in layout design depending on whether a user can (either themselves or through the

agency of others [21]) code a new CSS layer, or whether they have to use an existing skin or default layout. Image creation and manipulation (using tools such as Photoshop™ or Gimp) also limit the level of visual information a user might code into their displays. Different levels of social currency are ascribed to different skill sets by different groups, based upon the priorities of those groups. Alongside this, cross-platform and cross-channel consistency in visuality is also increasing in importance as some users seek to build a consistent visual identity strategy across multiple SNS, such as Facebook and Livejournal. That said, different platforms with different visual capabilities may enable different strategies of visual self-expression. For example, Facebook, which is now arguably the biggest single repository of photos on the web [22], only allows a single user image which is appended to all text, yet visual expression is still enabled through referring to user photo albums and even the visuals associated with quizzes and other elements which appear on the livefeed of all users. This architectural framework then forces different visual strategies than those that might have been used on other SNS such as Livejournal.

Thirdly, and perhaps most importantly, for visual to have such value in online impression management as these informants seem to imply it does, then there must be some level of online shared symbology for these more complex images, just as there is for the emoticons that evolved in text based exchanges. The multi-layered nature and richness of the visual elements in userpics, layouts and in-text visuals does leave them open to more diverse interpretations but I would argue that, within a specific context (an in-group using a particular platform) there is a consistency of image reading that is part of in-group membership. Thus visuals that employ these in-group visual cues not only convey emotional and identity information about the discrete individual, they also contribute social information about the place of that individual in the network. This, I argue, is partly why users can immediately discard certain user sites as 'immature,' 'unsophisticated' or 'shallow' – they are not conforming to the implicit in-group rules of reading and writing imagery, and thus indicate a lack of shared history or trust. Through this, skills of visual creation, manipulation and deployment become an increasingly important part of an overall individual and social impression management strategy in web 2.0 environments.

These strategies of reading visuals, and of writing visuals to be read in desired ways, is becoming an important part of overall strategies of impression management for users of social networking sites that allow such visual expressions of self. By manipulating visuals alongside text, users can help 'flesh out' their online self-presentation with personal, social, emotive and indicative information that other users can read (with varying levels of sophistication) to develop their own understanding or impression of that identity, and how it relates to their own in the online social context.

To conclude this paper, I would like to outline some implications of the above research and suggest possible future research directions in this area.

Firstly, though limited by its sample and scope, this research suggests that, at least among these users using this platform, there is a growing level of sophistication in the reading and deconstruction of images as they pertain to online identity. I would suggest that this may be due in part to both the increased capacity for easier inclusion of visuals on this platform, and to a growing expectation from users to have a visual component to the online self-presentation (whether it be a unique userpic, a personalized layout, or something more creative). This then raises questions as to whether this

behaviour is unique to sites like Livejournal (which foster such a diverse range of visual customization) or whether equivalent behaviours can be found on more visually consistent sites such as Facebook.

Secondly, and perhaps more contentiously, I would argue that the desire to create a positive impression in online social networks using visuals is in part helping to drive an overall increase in visual literacy amongst those users. This research indicated that these users had developed their own skills (in what might be considered an 'amateur' rather than 'amateurish' [23] way) in terms of being able to manipulate and use images as part of their online social interactions. I would argue that this growing sophistication is being driven by a desire to present the best virtual 'face' in online engagements. Because there is such a personal need to use visuals effectively, I argue that users feel motivated to develop visual skills, whether that be in terms of aesthetics, manipulation, or deployment (such as with CSS code). Furthermore, the nature of Web2 social networks creates an environment where users feel empowered to learn from each other techniques for visuals, thus driving an ever-widening recursive loop between images presented and the meanings associated by the social group to such images. As one respondent notes regarding how they believe their skill in creating visuals has changed over time:

> "I can 'see' how other artists do something new in a piece and it spurs me on to try the technique in my own way. Sometimes their advances create a jumping off point for my own and I'm able to develop something new from their inspiration." Respondent #17

Such sharing of techniques and visual approaches can also be seen on Livejournal where those interested in creating layouts, userspics or other site-specific visuals often forms communities such as userpic-sharing communities, or LIMS ('Last Icon Maker Standing") communities where creators share ideas and even have 'competitions' to create images along certain themes. Such competitions, and the more informal evaluation of images that appears to be part of the overall experience of social activity on the site, suggest a kind of 'appreciation' is going on where, if images are used, they have to be 'good' images within the overall calculus of identity evaluation that occurs in this virtual space. This then returns to an earlier point about the multiple layers of information – social, informational, personal – that can be contained within the image that is deployed within a social context. However, this research only scratched this surface of this layering function of identity images, and it is an area that would benefit from further research.

5 Future Implications

Though this research looked at image use in one particular web 2.0 platform, it does open up questions for the use of images across the social web. Firstly, with different platforms enabling different forms of visual expression (multiple versus single userpics, embedding images, customizing layouts), will skills in creating and understanding such visuals change as different platforms obtain dominance in the social networking cyberscape? If visuals are to become a part of the everyday function of social networking sites, will people develop sophistication in creating images as well

as reading them, or is the experience of these Livejournalists and their 'amateur' visual creation an aberration?

Beyond this, and given the growing plurality of sites and services offering social networking for various groups, is it feasible to expect a 'universal' visual lexicon (such as evolved with the core group of emoticons), or are visuals too layered and too open to multiple interpretations to expect widespread commonality in creating and interpreting identity-related visuals? Or is it, as these respondents seemed to indicate, related more to the *context* in which the image is created, produced, disseminated and finally read.

References

1. boyd, d.m., Ellison, N.B.: Social Network Sites: Definition, history and scholarship. J. Computer Mediated Communication 13(1) (2007), http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html
2. Turkle, S.: Life on the Screen: Identity in the Age of the Internet. Simon & Schuster, New York (1995)
3. Skog, D.: Social Interaction in Virtual Communities: The significance of technology. International Journal of Web Based Communities 1(4), 464–474 (2005)
4. Liu, H.: Social Network Profiles as Taste Performance. J. of Computer-Mediated Communication 13(1) (2007), http://jcmc.indiana.edu/vol13/issue1/liu.html
5. Hardey, M.: Life Beyond the Screen: Embodiment and identity through the internet. The Sociological Review 50(4), 570–585 (2002)
6. Ladd, K.: Textuality, Performativity and Archive: Examining the virtual body in socially networked space. MA Thesis, University of Toronto (2009), http://hdl.handle.net/1807/18093
7. Donath, J., boyd, d.m.: Public Displays of Connection. BT Technology Journal 22(4), 71–82 (2004)
8. Goffman, E.: The Presentation of Self in Everyday Life. Anchor, New York (1959)
9. Leary, M.R., Nezlek, J.B., Downs, D., Radford-Davenport, J., Martin, J., McMullen, A.: Self-Presentation in Everyday Interactions: Effects of target familiarity and gender composition. J. of Personality and Social Psychology 67(4), 664–673 (1994)
10. Panteli, N., Duncan, E.: Trust and Temporary Virtual Teams: Alternative Explanations and Dramaturgical Relationships. Information Technology and People 17(4), 423–441 (2004)
11. Browning, L., Stephens, K.K.: Impression Management and ICTs. In: Browning, L.D., Steinar Saetre, A., Stephens, K.K. (eds.) Information and Communication Technologies in Action, pp. 65–72. Routledge, New York (2008)
12. Marwick, A.: I'm a Lot More Interesting than a Friendster Profile: Identity presentation, authenticity and power in social networking services. Paper Presented at AoIR IR6.0: Internet Generations, Chicago, IL (2005), http://www.tiara.org/papers/marwick_friendster_authenticity_power.doc
13. Kendall, L.: Shout Into the Wind, and It Shouts Back: Identity and interactional tensions on Livejournal. First Monday 9(3) (2007), http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2004/1879
14. Pearson, E.: All The World Wide Web's A Stage: The performance of identity in online social networks. First Monday 3(2) (2009), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2162/2127

15. Fono, D., Raynes-Goldie, K.: Hyperfriends and Beyond: Friendship and social norms on Livejournal. In: Consalvo, M., Haythornwaite, C. (eds.) Internet Research Annual, vol. 4, pp. 91–118. Peter Lang, New York (2007)
16. Marwick, A.: Selling your self: Online identity in the age of commodified Internet. University of Washington, Washington (2005) (Unpublished MA Thesis), http://www.tiara.org/papers/amarwick_sellingyourself_mathesis.doc
17. Livejournal, http://www.livejournal.com
18. Siibak, A.: Constructing the Self through the Photo selection - Visual Impression Management on Social Networking Websites. Cyberpsychology: Journal of Psychosocial Research on Cyberspace 3(1) (2009), http://cyberpsychology.eu/view.php?cisloclanku=2009061501&article=1
19. Tarkowski, A.: Peer production of popular culture at the Live Journal blogging site. Banal blogging or cultural struggle? Presented at RE: Activism: Re-Drawing the Boundaries of Activism in New Media Environments. Budapest (2005), http://mokk.bme.hu/centre/conferences/reactivism/submissions/tarkowski
20. Rebaza, C.: Online Gestures: Icon Use by Fan Communities on Live Journal. Paper Presented at 41st Hawaii International Conference on System Sciences. Hilton Waikoloa Village Resort, Waikoloa (2008)
21. Pearson, E.: Digital gifts: participation and exchange in Live Journal communities. First Monday 12(5) (2007), http://firstmonday.org/issues/issue12_5/pearson/index.html
22. Wong, P.: Conversations About the Internet #5: Anonymous Facebook Employee. The Rumpus (2010), http://therumpus.net/2010/01/conversations-about-the-internet-5-anonymous-facebook-employee/?full=yes
23. Lessig, L.: TEDTalks: Laws That Choke Creativity [online video file] (2007), http://www.ted.com/talks/larry_lessig_says_the_law_is_strangling_creativity.html

Virtuality Improves the Well Being of Seniors through Increasing Social Interaction

Oliver K. Burmeister

Centre for Research in Complex Systems, School of Computing and Mathematics, Charles Sturt University, Boorooma Street, Wagga Wagga, NSW 2678, Australia
oburmesiter@csu.edu.au

Abstract. Virtual social interaction amongst seniors is strengthened through face to face contact. While confirming previous studies that have shown the strengthening of virtual friendships result from physical meetings, this study also showed that virtual face to face meetings have a similar benefit. As more seniors around the world are encouraged to stay at home longer, rather than enter institutional care, virtual sociability is being shown to provide the necessary social inclusion benefits for particularly mental well being, that has been identified in psychological and sociological studies of seniors.

Keywords: Ethnography, Human Computer Interaction, Online Community, User Centred Design, Value Sensitive Design.

1 Introduction

Social inclusion is increasingly being seen as critical to the health and general well being of seniors. Psychosocial research has shown that the mental and overall well being of seniors is significantly enhanced through society resourcing the social engagement of seniors; the more socially active seniors are, the better it is for their long term well being [1, 2, 3]. Governments around the world are concerned that the ageing population is putting financial and other resourcing pressures on the services provided to their senior citizens. They are looking for ways to keep seniors at home and out of institutional care longer and technology is a major potential contributor to such aims. Yet a challenge is that of social isolation at home, which raises particularly mental health concerns [2, 4]. It is in this area that this paper shows the benefits of virtual social interaction for seniors.

Studies of what is effective for social inclusion inform that design process, enabling the design of better social spaces in the virtual world. This paper reports on an ethnographic study of one of the largest virtual communities for seniors in the world at the present time. In particular the focus is on one aspect of sociability, namely the move from virtual social interaction to face to face interaction. The latter may also involve virtual or physical social interaction.

This paper begins by showing why studies of seniors are important. It then goes on to describe the online community called GreyPath, which was the basis of this study. It then briefly reviews human computer interaction (HCI) literature and places the

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 131–141, 2010.

literature on values in design, which was the focus of this study, within that broader context. Next it describes the interpretivist, constructivist approach that was taken and how the results led to this discussion of social inclusion. Lastly the results of the study are reported and their implications for design explored.

2 Studies of Virtual Sociability amongst Seniors Are Important

The combination of decreasing rates of mortality and birth rates, means that the number of seniors in Western nations is projected to increase significantly over the next several decades. McDonald and Kippen [5] showed that in 1870 only 2% of Australians were aged 65 and over, and that by 1998 this had increased to 12%, with forward projections showing a marked increase in the percentage of older people in the Australian population. According to the Australian Bureau of Statistics (ABS) [6] one in four Australians (23 to 25%) will be over 65 by 2056, up from 13% in 2007. By 2056, there will be twice as many pensioners as now with half as many people supporting the social security system, which provides pensions and health care along with other benefits to seniors. This is a function of a general trend in the developed world of lower birth rates and people living longer. According to Britain's Office of National Statistics:

> Over the last 25 years the percentage of the population aged 65 and over increased from 15 per cent in 1983 to 16 per cent in 2008, an increase of 1.5 million people in this age group. Over the same period, the percentage of the population aged 16 and under decreased from 21 per cent to 19 per cent. This trend is projected to continue. [7]

As in Australia and Britain, so it is in other Western nations. Belsky [8] said that only 4% of Americans were elderly in 1900, whilst by 1999 that figure had risen to 13%. In 1999 the proportion of elderly Americans was 1 in 8, and this was forecast to rise to 1 in 5 by 2030.

In Australia the majority of seniors live independently at home, either with a partner only (46%), family (17%) or alone (28%) [9]. With the demands these forecasts are expected to place on aged-care provisions, governments around the world are looking for ways to keep seniors in their homes and out of institutions as long as possible.

This study contributed to knowledge regarding the social interaction needs of seniors. It achieved this through a focus on Australia's largest online community for seniors [10], greypath.com (GreyPath).

2.1 The GreyPath Virtual Community

GreyPath Pty. Ltd. manages the portal greypath.com. Membership is restricted to seniors, which it defines as 50 years of age and over. In sociological terms, participation is not spatially determined, as traditional communities have been [11], but ubiquitous [12]. The community has members in every state and territory of Australia, including some who are travelling (have no fixed address) and overseas members (their chat rooms regularly have seniors participating from Europe, the Middle East,

Asia, and North America). GreyPath has 35 volunteers who freely give of their time and skills to maintain the site. All contributors, management, administrators, technical support personnel and ordinary members are seniors.

A significant feature of the GreyPath portal is its hybridity [13], that is, its multi-faceted approach. It allows for all manner of users, from novice technology users, to people very technologically literate. It has members who rarely use the site and then only to find specific information, and others who use the site for many hours every day for social interaction with other members. GreyPathians (as several interviewees in this study called themselves) can enroll in free or nominal cost courses, and they can contribute to or receive information on a wide variety of topics. The online destinations of GreyPath members are dictated by their interests and time constraints. GreyPath is also a safe place, in that it is moderated by volunteer contributors who each have placed their name and face on the site.

As at August 2009 there were approximately 100 million web sites worldwide. GreyPath traffic ranked approximately 1.3 millionth according to the web information organisation Alexa [14], placing it in the top 1.5 percent of world-wide sites by traffic. As at August 2009 it had more traffic, as defined by Alexa [14], than any other seniors site in the world at that time.

GreyPath is accessed by groups of people who participate in a number of the various options available, such as the forums, blogs and chat rooms. GreyPath management continue to innovate, with the development of video editorials, a new multimedia seniors course development engine, and a possibly unique approach to a three-dimensional (3D) seniors game currently under development. The most recent innovation has been the first simple broadcasts of GreyPath Internet TV. It is this Australian portal for seniors that was the basis of this study.

3 Value Studies

This study was focused on the initial stages of HCI design methodologies called Value Sensitive Design (VSD) and Values at Play (VAP). That is, it focused on discovering the things that GreyPath seniors valued most about their online social interaction.

There had been some thought given to the idea that values were reflected in technology prior the advent of VSD, with some of the earliest work by Winner [15] referring to artifacts having “political qualities”, but described in ways that later researchers discussed as values. No explicit attempts had been made to discover values that impinge on design until the first references to VSD appeared [16]. Since that time numerous publications have arisen in related areas [17, 18, 19]. A fundamental premise of VSD is that technology artifacts embody values.

Two main research avenues have been pursued. Having started on the road to researching how values can and should be incorporated in design, Friedman and Nissenbaum, though sharing a common research purpose, have developed their research into incorporating values in the design process along different lines. Friedman has continued along the lines of VSD, expanding the methodology, defining it and together with other researchers, has attempted to prove its efficacy in the design process [17, 20]. Nissenbaum has built on the foundations laid by VSD, together with other

researchers to develop Values at Play (VAP) [21]. Like Friedman, Nissenbaum has attempted to define the methodology involved and prove the concepts in design examples.

In putting forward new design considerations, these researchers were not seeking to usurp existing design methodologies, but rather to extend them. Flanagan, Howe and Nissenbaum [22] stated their goal as supplementing existing, well-established design methodologies. They sought to have values considered as one part of what constitutes technical design excellence. They argued that measures of design excellence included terms such as reliability, usability, functional efficiency, and safety; values were not considered, but should be. In various ways these HCI researchers espoused that the current research into value considerations will one day see value considerations become an integral part of the criteria for design excellence.

The brief sketch of values in design gives the background against which this study took place. This study sought to discover the values that were important to seniors in their online social interaction.

4 Research Design and Method

The main research question was: What do participants in the GreyPath community value about their online social interaction? An interpretivist, constructivist philosophy was chosen to help answer this question, based on the nature of the data to be collected and the purpose for the study. It was a study to discover the values of seniors in a chosen online community and therefore their perceptions of their values were crucial. The nature of this study meant that a positivist approach was inappropriate as it would necessarily entail an emphasis on quantitative data. Such an approach might have sought to survey members of the online community, to elicit their values. Given no prior studies had been reported of seniors' values when using technology, such a survey could not have been reliably scripted. In order to quantify and then generalise the findings of a survey, the values themselves first need to be established. Therefore in order to discover those values, an inductive approach involving observation and in-depth interviews with seniors was seen as more appropriate.

Interpretivist constructivists emphasise the meanings of participants within the social phenomenon under study [23, 24]. This was appropriate to the present study of an online community, because the aim was to understand the 'meanings' of participants with regard to their values. Furthermore, interpretivist constructivist researchers use an inductive approach, where "researchers develop concepts, insights and understanding from patterns in the data" [25]. Patton [26] distinguished inductive analyses from hypothetical-deductive approaches, based on the latter requiring variable specification before data collection. Since this study was to explore descriptions of values not previously identified in other studies, making such variable specification would have been inappropriate. Instead, the nature of the study required an inductive approach, one in which themes related to values would emerge during analysis, and would be grounded in, and checked against, observations and interview transcripts.

The 30 interviewees for the study were chosen on the basis of purposive sampling, which is appropriate to interpretive research. Patton [26] describes various types of purposive sampling. Because no prior study in the domain existed and there were no

known specific variables to focus on, the one most appropriate to this study was 'criterion sampling'. Criterion sampling uses a particular set of criteria to guide sample selection. In this study, the criteria for selection of participants were determined prior to the commencement of the sample selection, in order to aid as widely as possible the understanding of GreyPath members' social interaction values.

Analysis of data was a continuous process, using an inductive approach for thematic analysis. The analysis process was informed by grounded theory approaches to analysing data. The initial themes and categories, determined both during the observation phase and after the initial interviews, were continually reassessed and expanded as more data was collected. During interviews the interviewer was open to the meanings of interviewees. Values that were thus discovered, were then structured and organised into themes.

One theme that emerged during the course of the research was that of values related to the different types of social interaction experienced by GreyPath membersand within that theme the key value was the move from 'forum to face'. That is, the move from various forms of virtual interaction, such as text based forums, or text and audio based chat rooms, to some form of social interaction that involved face to face communication.

5 Results

Many participants valued being able to interact with GreyPathians and others in ways that did not necessarily involve a GreyPath facility. They used Voice over IP (VoIP), instant messaging (IM), personal email and the normal postal main system (snail mail). Predominantly they valued extending their GreyPath contacts in ways that created lasting, personal contact, that extended the online GreyPath experiences to deeper involvement with the people they had met. Closely associated with the value 'Forum to face' were other ways of extending the GreyPath experience, in particular 'Personal email' and 'Snail mail'.

Extending online relationships into other situations has been recognised particularly in sociological research. The online environment does not lure people away from face-to-face contact, making them less sociable, less able to relate to other people [27]. Instead research has shown that online community involvement encourages greater social contact via other means, especially face-to-face and telephone [28, 29].

Forum to face is valued by GreyPath management. Several times each year they organise seminars on different topics of interest to seniors. The seminars are open to all seniors, but are particularly run for the benefit of GreyPath members. All the seminars are held in Melbourne, which is where GreyPath started and where the GreyPath office is located. This is illustrated below by the GreyPath web master (note that participants are only identified as [gender, location, age]):

> [The chief administrator] is preparing a seminar ... I guess some of them [GreyPath members] will attend that or quite a few of them we hope, so that will be a new experience for me. [Male, VIC, 55-59]

Forum to face is valued by GreyPath members too. This is seen in the following two quotations concerning a physical meeting of GreyPathians, organised months in

advance. The second quotation is from an unsolicited email an interviewee sent the researcher after the meeting.

> Next month we're going to meet at Mt Barker, which is a place about [number] odd mile away from here, for a coffee morning … There's going to be a couple there, I'm single now, otherwise I'd be taking my wife, I'm not sure how many, three or four will be there, five or six maybe. It's something to do, and besides it's nice to be able to put a face to the name. [Male, SA, 70-74]

> [Post interview email about the Mt Barker meeting:] We had the GreyPath morning coffee meeting today. Five of us show up and a good time had by all. We started at 11 am, had coffee then stayed for lunch and on our way home by 1:15 pm or so. [Male, SA, 65-69]

Other studies have similarly shown that for seniors online social interaction frequently leads to offline interaction, as is seen in the above quotation. Xie's ethnographic study of the OldKids online community in China [30, 31, 32] showed that this online to offline interaction greatly affected the overall relationships of those seniors [31] and she went on to say that such movement to offline interaction strengthened later, further online interaction. Similarly, she found that when relationships began offline and then moved to online, it resulted in stronger social bonding. Her summation was that: "In general, those who interact with one another both online and offline are more likely to develop closer, stronger relationships than those who interact only online." [31] However, while Xie's 'offline' results are supported by this study, her conclusion about 'only online' were not supported. Xie only looked at the online-offline relationship. This study of the GreyPath community confirmed Xie's findings in regards to the offline influences on strengthening relationships. However, this study found the same was true when forum to face meant webcam type interaction, which arguably contradicts her conclusion that 'only online' interaction does not strengthen overall relationships in the same way physical offline interaction does. When forum to face interaction means moving from forum to webcam, it is still online interaction, even if it is not taking place through the GreyPath portal. In this study all forms of forum to face movement were valued by members and seen to strengthen relationships and community building.

Other examples of forum to face are illustrated below:

> I know … the names, addresses, phone numbers … one lady who … came to the funeral [of his wife], and she had been before once to stay with us for a weekend when my wife was alive, and then when my wife died, she found out when the funeral was, she asked me, and then she came to the funeral, and she went straight home of course, because I don't want any kind of, complications, shall we say, well certainly not yet I mean. Next year who knows, but I doubt it. [Male, SA, 70-74]

> A lady called [Name] who comes from Western Australia, and whenever she comes over here, she makes a point of finding out, if she's going to stay at whoop whoop, does anyone live near whoop whoop, could I meet you and have a coffee. [Male, NSW, 70-74]

> This girl [a younger GreyPathian] … I don't know how long she's been a member it was just that we had the big fete here yesterday and she came up to me then … I didn't realise that she'd gone onto GreyPath but she saw my name there. [Female, WA, 70-74]

> An Adelaide girl [a younger GreyPathian] … she says: "Come and stay with us" … I stayed with her, and she arranged a dinner … And, well she introduces me to all these other people that are on GreyPath. [Female, NT, 75-79]

> I'll go out to locals here in Brisbane, I meet quite a few regularly, but individually, not as a group, we have never done that. [Male, QLD, 65-69]

> A couple of times a year I meet up with two of them and we have lunch together that's the husband and wife. The husband and I are both very much into computing so we often send emails back and forth about that, even a few jokes go back and forth between the three of us, messages come across, emails and I try to change ideas with [Name] and things like that and we get together a couple of times a year and have lunch. [Male, SA, 65-69]

> Amongst the people that I personally know, I've had a visit as well from a chatter [GreyPath Chat room contact], it's just like talking over the garden fence, you know, I can't add it any stronger than that. [Male, OVERSEAS, 75-79]

An interesting observation arises from this last quotation. The author of the last quotation lives overseas, is house-bound and most of the time room-bound, due to a disability, and he has met not one, but several GreyPath members. These were people who while vacationing in Europe made a deliberate effort to include this man in their itinerary.

The next two quotations are from the same person. She and her husband use the GreyPath site to source house sitting opportunities. As one might expect, this has led to her getting to know the GreyPathians whose houses she and her husband look after. In several cases they 'sat' the same houses repeatedly over time:

> Well most of them have turned out to be very close relationships. This one here that we're at the moment, they're a doctor and his wife and we, as opposed to being house sitters three years ago, we are now really the best of friends sort of thing … We don't get sort of totally involved with people, because we're never there long enough to do that, and while we're there, they're not sort of thing. [Female, MOVE, 65-69]

> When we went down to South Australia again through that [GreyPath] Coffee Shop forum, two or three families, GreyPathers down there, organised a coffee morning … We all met up at a pub just out of Elizabeth, up the road, and we all sort of had lunch together, and through that … we were house sitting down there. We used to phone these different ones up and it was a great friendship, because we knew nobody in Adelaide and we were able to phone them up and we went round to their places and had coffee and afternoons out and they took us around. As far as I'm concerned, that part of GreyPath was excellent, you know? They really opened their homes up to us,

> because we were gypsies, after all, that they didn't know. And they were just quite welcoming, it was great. [Female, MOVE, 65-69]

As previously stated, the value 'forum to face' was supported by related values of extending contact to personal email and snail mail. The following examples illustrate this:

> A lot of months ago, I entered my name [in the GreyPath ePals] and a lady sent me an email from Victoria, from around Geelong, and we got talking …I send her jokes, we often interact and talk about the weather, or, she's quite surprised, as a New South Welshman that I was aware of what happened at AFL … We don't interact on a weekly or daily basis, it might a couple of times a month and then it might be a couple of times a week sometimes. [Male, NSW, 70-74]

> Three that I send emails to and, no phone calls, no snail mail, just emails yeah, interact with them on emails. [Male, NSW, 70-74]

> I did get a few non-replies with that ePals one, but of the ones that did reply, we've sort of kept in touch and it's been, to me, it's been absolutely brilliant. I've really enjoyed it. [Female, MOVE, 65-69]

The above quotations illustrate that like forum to face, personal email, including with people they met in the GreyPath ePals section, extends online social interaction beyond that available through GreyPath facilities. The following two quotations illustrate this through the use of snail mail:

> At least half a dozen of them write to me privately. [Female, NT, 75-79]

> She's a German immigrant, been in Australia some years I believe, very friendly with her, and my wife, we swap DVD's, we swap news. [Male, OVERSEAS, 75-79]

Whilst the dominant views expressed by participants favoured 'forum to face' relationship progression, there were some objections. The following three quotations exemplify the concerns raised by some participants:

> The good thing is you don't have to rush and do your hair…You don't have to worry, you don't have to worry about your wrinkles either. [Female, VIC, 60-64]

> I don't know whether I want to know anyone on GreyPath within my town, I don't want that sort of relationship. [Male, NSW, 70-74]

> I haven't met anyone personally and I'd be very very reluctant to do that, I'm a fairly slow person and face to face meetings are harder. [Female, VIC, 70-74]

The first of these three responses shows that some female participants (no male participants made similar comments) were concerned about their appearance. Comments included needing to fix their hair, change out of their bed clothes and having to put make-up on, if webcam or face to face meetings became more common with GreyPath.

The second response typified the reluctance many seniors expressed about having people visit them in their home. It was too close. They were happy to travel to a larger gathering, but didn't want close contact near where they lived.

The third response is more difficult to interpret. In one sense it is related to the first one. It is not about appearance in the sense of one's looks, but rather about age-related problems and disabilities. One participant said that she had won national dancing awards in previous years, but that she was constantly in and out of hospital and had just come out of hospital (at the time of the interview). She had age-related disabilities that not only meant she could no longer dance, but that she could barely walk and she was reluctant to allow people she regularly communicated with on GreyPath to see her as she is now. She wanted to interact using text only, so that she appeared 'normal' to everyone she corresponded with.

Despite these last three quotations against extending relationships beyond the GreyPath venues, the overwhelming views of most participants were in favour of extending the relationships, of deepening online friendships by extending contact to include the telephone, IM, VoIP, webcam, email, snail mail and personal visits.

6 Conclusion

The feedback loop identified by Xie's earlier studies of Chinese seniors was confirmed in this study of Australian seniors. Relationships that began online and were extended into offline settings, resulted in stronger online relationships. However this study extended Xie's findings to show that the same was also true for relationships that stayed online, but moved from text-based interaction to some other form of face to face meeting, such as the use of webcam.

Psychological and sociological studies have shown the need to have society promote ways of encouraging social inclusion amongst seniors, for their overall well being [2, 33, 34]. This paper built on prior work that showed that virtual communities can help promote social inclusion amongst seniors [31, 35], by showing that seniors highly value virtual social interaction and the friendship building opportunities it provides them. Of the 30 participants in the study, 27 accessed GreyPath from home, showing further that efforts by governments around the world to keep older people in their homes longer, need not mean social isolation. Virtual sociability amongst seniors increases their ability to maintain their mental and overall well being while at home.

References

1. Baltes, M.M., Carstensen, L.L.: The process of successful aging. Aging and Society 16, 397–422 (1996)
2. Baltes, P.B., Staudinger, U.M., Lindenberger, U.: Lifespan Psychology: Theory and Application to Intellectual Functioning. Annu. Rev. Psychol. 50, 471–507 (1999)
3. Baltes, P.B., Smith, J.: New frontiers in the future of ageing: From successful ageing of the young old to the dilemmas of the fourth age. In: Valencia Forum, Valencia, Spain (2002)
4. Christophidis, N.: Physical and mental changes during lifetime. In: First National Conference, Life Long Learning. University of the Third Age/University of Melbourne (1991)

5. McDonald, P., Kippen, R.: Ageing: the social and demographic dimensions. In: Policy Implications of the Ageing of Australia's Population, pp. 47–70. Productivity Commission, Melbourne (1999)
6. ABS. One in four Australians aged 65 years and over by 2056. Australian Federal Government (2008)
7. ONS, Ageing, Office of National Statistics (Editor). Crown Copyright: Surrey, UK (2008), http://www.statistics.gov.uk/cci/nugget.asp?id=949
8. Belsky, J.K.: The Psychology of Ageing: Theory, Research, and Interventions, 3rd edn. ITP, Melbourne (1999)
9. ABS. ABS report profiles Australia's older people. Australian Bureau of Statistics (1999)
10. Burmeister, O.K.: What 45,000 seniors value about online social interaction. In: IFIP WG9.5 Conference on Massive Virtual Communities. Leuphana University, Luneburg (2008)
11. Wellman, B., Leighton, B.: Networks, Neighborhoods, and Communities: Approaches to the Study of the Community Question. Urban Affairs Quarterly 14(3), 363–390 (1979)
12. Wellman, B., Hogan, B.: The Immanent Internet. In: McKay, J. (ed.) Netting Citizens: Exploring Citizenship in the Internet Age, pp. 54–80. Saint Andrew Press, Edinburgh (2004)
13. Arnold, M.V.: The concept of community and the character of networks. The Journal of Community Informatics 3(2) (2007), http://ci-journal.net/index.php/ciej/article/view/327/355
14. Alexa. Alexa The Wed Information Company (2009), http://www.alexa.com/
15. Winner, L.: Do Artefacts Have Politics. Daedalus 109, 121–136 (1980)
16. Friedman, B.: Value-sensitive design. Interactions 3(6), 17–23 (1996)
17. Miller, J.K., Friedman, B., Jancke, G.: Value tensions in design: the value sensitive design, development, and appropriation of a corporation's groupware system. In: Proceedings of the 2007 International ACM Conference on Supporting Group Work. ACM, Sanibel Island (2007)
18. Brey, P.: Disclosive Computer Ethics. Computers and Society 30(4), 10–16 (2000)
19. Leitner, M., Wolkerstorfer, P., Tscheligi, M.: How online communities support human values. In: 5th Nordic Conference on Human-Computer Interaction: Building Bridges. ACM, Lund (2008)
20. Friedman, B., Borning, A., Davis, J.L., Gill, B.T., Kahn, P.H.J., Kriplean, T., Lin, P.: Laying the foundations for public participation and value advocacy: interaction design for a large scale urban simulation. In: Chun, S.A., Janssen, M., Gil-Garcia, J.R. (eds.) Proceedings of the 2008 International Conference on Digital Government Research, pp. 305–314. Digital Government Society of North America, Montreal (2008)
21. Flanagan, M., Howe, D., Nissenbaum, H.: Values in Design: Theory and Practice. In: Van Den Hoven, J., Weckert, J. (eds.) Information Technology and Moral Philosophy. Cambridge University Press, Cambridge (2007)
22. Flanagan, M., Howe, D.C., Nissenbaum, H.: Values at play: design tradeoffs in socially-oriented game design. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, Portland (2005)
23. Williamson, K.: Research in Constructivist Frameworks Using Ethnographic Techniques. Library Trends 55(1), 83–101 (2006)
24. Sudweeks, F., Simoff, S.J.: Complementary Explorative Data Analysis: The Reconciliation of Quantitative and Qualitative Principles. In: Jones, S.G. (ed.) Doing Internet Research: Critical Issues and Methods for Examining the Net. Sage, Thousand Oaks (1999)

25. Reneker, M.H.: A qualitative study of information seeking among members of an academic community: methodological issues and problems. Library Quarterly 63(4), 487–507 (1993)
26. Patton, M.Q.: Qualitative Research and Evaluation Methods, 3rd edn. Sage, Thousand Oaks (2002)
27. Boase, J., Wellman, B.: Personal Relationships: On and Off the Internet. In: Perlman, D., Vangelisti, A.L. (eds.) Handbook of Personal Relations. Cambridge University Press, Cambridge (2004)
28. Wellman, B.: An Electronic Group is Virtually a Social Network. In: Kiesler, S. (ed.) Culture of the Internet, pp. 179–205. Lawrence Erlbaum, Hillsdale (1997)
29. Hampton, K., Wellman, B.: Neighboring in Netville: How the Internet Supports Community and Social Capital in a Wired Suburb. City and Community 2(4), 277–311 (2003)
30. Xie, B.: Multimodal Computer-Mediated Communication and Social Support among Older Chinese Internet Users. Journal of Computer-Mediated Communication 13(3), 728–750 (2008)
31. Xie, B.: The mutual shaping of online and offline social relationships. Information Research: An Electronic Journal 13(3) (2008), http://informationr.net/ir/13-3/paper350.html
32. Xie, B.: Using the Internet for Offline Relationship Formation. Social Science Computer Review 25(3), 396–404 (2007)
33. Marsiske, M., Lang, F.R., Baltes, P.B.: Selective optimization with compensation: Lifespan perspectives on successful human development. In: Dixon, R.A., Baeckman, L. (eds.) Compensation for Psychological Defects and Declines: Managing Losses and Promoting Gains, pp. 35–79. Erlbaum, Hillsdale (1995)
34. Park, D.C., Reuter-Lorenz, P.: The adaptive brain: aging and neurocognitive scaffolding. Annual Review of Psychology 60, 173–196 (2009)
35. Pfeil, U., Zaphiris, P.: Investigating social network patterns within an empathic online community for older people. Computers in Human Behavior 25(5), 1139–1155 (2010)

The Tragedy of the Virtual Commons as Manifested in the Death of Blogs

John Lenarcic and Pradipta Sarkar

School of Business IT and Logistics, RMIT University, Melbourne, Australia
john.lenarcic@rmit.edu.au, pradipta.sarkar@rmit.edu.au

Abstract. The life span of weblogs is investigated with reference to Lanham's view of the "Economics of Attention" and Hardin's conception of the "Tragedy of the Commons." It is advanced that the unfettered buildup of inactive blogs is leading to a surfeit of information which effectively disables potential readers due to an excess of choice. One factor indicating healthy activity in a blog is postulated as being sufficient feedback from readers that leads to the emergence of an ongoing social network. This is viewed as an example of a virtual technology shaping social groups. Research-in-progress is outlined that refers to observations of various film music blogs derived via the case study method, featuring a focused commentary on one that has subsequently been a victim of death in the blogosphere. In this case, the forced extinction of a blog is taken to be an example of human foibles influencing the download spiral of one instance of a virtual technology.

Keywords: Blogging, Sustainability, Tragedy of the Commons.

1 Introduction

Generally envisaged as a self-directed framework to publishing using third-party applications such as Blogger, weblogs (or blogs) are web sites that use a chronologically-tagged record layout to enable the broadcast of personal or topical information on a regular basis [20]. With succeeding items displayed in a reverse time-stamped manner, blogs can be considered as either filters for information aggregation or personal journals and are often a hybrid of the two. In their guise as filters they act to accumulate and put on view links to other web sites that may include subject matter of mutual interest. Those blogs that function as journals are often a conduit for an author's soliloquies to the assumed massed readership of the virtual universe known as the blogosphere.

Blogging is a pastime that is similar to that of keeping a physical diary but one that is drastically more transparent in its one-to-many dialogue format via an interlinked hypertext network [1]. Some have argued that the on-going production of a diary has therapeutic benefits to the self given that reflective writing can anchor one with a sense of place [30]. If the solitary pursuit of diary-keeping can nurture a community of one through internal dialogue, what would the consequences be with the implementation of a networked incarnation? Indeed, this factor could be one of the driving

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 142–149, 2010.

forces underpinning the boom in blogging as a pastime: The weblog is a tool that is an inadvertent design tool in the creation of ad-hoc social networks where the shared sense of place forges a community bonded by a collective, often idiosyncratic, forte.

2 Blogging and the Economics of Attention

It has been stated that almost 10 percent of Internet users in the USA maintain their own blogs and 40 percent of this population read them, indicating that the Web is gravitating towards becoming a medium where anyone with appropriate access and the right motivation can become a publisher [31]. However, in 2007, "The Age" newspaper in Melbourne, Australia, reported that despite the meteoric rise in the number of blogs, there were apparently millions that were dormant to the point of fading into oblivion [20]. What motivates actions to ensure the sustainability of a blog? Blogging is a democratic means for an individual to express their views to an audience and to obtain feedback from readers on these opinions [25]. Feedback either as comments posted, or even peripheral approbation via other channels (e.g. word of mouth), has been advanced as a key factor in ensuring that a blog does not dwindle into inactivity [21].

Feedback of either a positive or negative nature can be thought of as reinforcement to sustain or modify an activity: Affirmative responses can instill confidence in the emerging mission of the blog to both the initiator and the readership at large, whereas downbeat postings can evoke a vigorous discussion in retaliation which also accentuates the vivacity of a blog. In effect, the ideal blog environment from a routine performance aspect is one that resembles a kind of interlaced Socratic dialogue between many contributors, rather than it being a one-to-many presentation, with occasional reader reactions, where the originally blogger always seems to be in supreme control.

Economics as a field of endeavour is primarily concerned with the allocation of resources, conventionally of the tangible variety. There are some who would contend that the most prized resource in the present information economy is not information per se, rather it is the capacity to draw attention to make sense of information [15]. Much has been written about the crippling effects of "information anxiety" in society whereby one can virtually drown in a glut of data [28, 32, 33]. Information is plentiful but critical awareness of it is not. We believe that this line of reasoning can be extended into the blogosphere: It is possible that the most precious resource in this domain is the set of attributes that would attract a sustained interest in a blog.

3 Blogging and the "Tragedy of the Commons"

In economic terms, the "Tragedy of the Commons" (TC) defines a social scenario where there exists a dispute between the interests of the individual and that of the common public good [10]. This tension can impinge upon the sustainability of freely-available public resources. Research findings have indicated that reputation can alleviate the TC [23]. Indirect reciprocity of the "give and you shall receive" variety rests upon social standing and can sustain a high degree of co-operation within communities. It has been shown that the need to maintain a reputation for indirect reciprocity

can also have the side-effect of keeping contributions to freely-available public goods at a high level [23]. How does this relate to the blogosphere? Li and Walejko [19] highlight the problems posed by "splogs" (or spam blogs) and abandoned blogs in the blogosphere. Splogs post bogus links and content pointing to a single site [14] and estimates indicate that one in five blogs is actually a splog [24]. One source reckons that as many as two-thirds of blogs are abandoned and constitute a new kind of flotsam and jetsam for the digital age [17].

The public goods that constitute the content of blogs can only be sustained by the indirect reciprocity of contributors, be they the authors of postings or those who submit comments to postings. Whereas the notion of TC in the physical sense is dependent on limited resources being desecrated to non-existence, in the blogosphere there is effectively no limitation on quantity or content. On the other hand, we posit that since "dead" blogs never actually decay into nothingness but linger effectively forever, this ever-increasing accumulation is an example of what we deem to be the "Tragedy of the Virtual Commons" analogous to that of the flood of information associated with the spam problem [14].

The paradox of choice afforded by the unchecked generation of blogs could lead to a situation where readers are faced with a myriad of information sources, with varying degrees of activity levels, but without the personal time to assess the authenticity in a selection [27]. To test the assumption that vigorous traffic in posted comments sustains the life span of a blog we are currently tracking the behavioural machinations of a cohort of film music blogs, with particular analysis given to a prototype within this group. These represent a niche area of interest that we believe would foster an online community of those with a deep fascination with movie soundtracks.

Lessig [15] introduces the notion of the "intellectual commons", which advocates the sharing of ideas amongst the public, though they may have originated from the minds of creative individuals. It is believed that the sharing of the ideas will be for the public good. This notion is at odds with Hardin's [9] view of the depletion of public resources owing to "overgrazing" by individuals. However, Keen [12] believes that user-generated media such as blogs or YouTube are a disruptive influence in society from economic, cultural and value-centric perspectives. Web 2.0, in other words, facilitates mediocrity as cultural ideal. Echoing these sentiments, Lanier [14] is of the opinion that that internet has become a platform that stifles creativity and a tool that is destroying middle-class professions due to activities such as file-sharing.

Gotterbarn [9], on the other hand, claims that the TC may not be applied to Web 2.0 in its original sense due to increasing computing power. Instead, he describes the situation as the "Soiling of the Commons", whereby a rising number of dead blogs and splogs contaminate the blogosphere. The latter argument, though, fails to realize that the TC concept is actually a metaphor that has been applied in a variety of contexts outside of its original inception to describe an ecological scenario [3].

4 Research Methodology

We adopted a qualitative research methodology as we were interested in finding out "how social experience" was generated and given meaning in relation to the blogs [7]. Therefore, an "interpretive, naturalistic" approach was deemed appropriate for the

study [2]. To facilitate this research tactic the case study method was adopted for this project [6, 34]. Case studies are considered to be appropriate when a phenomenon is inadequately substantiated in theory, or when contextual factors need to be captured. The focus of case study research is on developing a detailed account analysis of one or more cases. It involves the exploration of a case (or multiple cases) over a period of time by means of elaborate and in-depth data collection from "multiple sources of information rich in context" and presents rich empirical findings and discussions of the phenomenon under study [5]. Furthermore, the “how” and “why” aspects of the study warrant the use of case studies [6].

Initially, we have chosen to focus on one paradigmatic case study of a music blog which for this exercise has been dubbed “Blog X”. This has been done to respect the anonymity of members of this blog community who are primarily referred to by nom-de-plumes when posting comments, including the originator of the blog. (Anonymous comments are permitted in this blog how most visitors to Blog X posted comments signed by the writer’s alias.) Upon inspection of the limited cohort of blogs devoted to film music, Blog X was considered to be a cultural prototype within the spectrum of movie soundtrack appreciation. (During its short history, Blog X changed from being a dedicated film music forum to one that catered to more eclectic tastes, however it never entirely discarded its roots.)

Given significant longitudinal scrutiny of the blog, it was felt that this developing case study would provide valid generalizations that would shed light on the issues raised earlier in the paper [6]. What occurred in our observations was that we witnessed the death of a blog. Most blogs would probably become abandoned due to the cessation of comments by readers and the lack of fresh posts by the initiator. However, in this instance, the initiator composed a final post announcing the termination of Blog X. So far, 90 readers have responded with condolence comments. The next section features the final post in its entirety, interspersed with critical commentary where appropriate.

5 Requiem for a Blog: An Interpretation of a Final Post

The following text is the final post of an atypical music blog whose life span was just over two years. It was deemed to be atypical amongst eclectic music blogs due to the perceived level of commitment bestowed upon it by the initiator of this blog. Blog X, as it is called in this paper, was a more generic weblog in that the initiator played a more dominant role in steering a course for the content posted. In other words, Blog X did not exhibit community-like behaviour in the same fashion as film music Blog X. The final post of Blog X is presented in unexpurgated form with only the blog name substituted with “Blog X” for the sake of anonymity as the initiator is still active within the blogosphere.

Blog X is an exemplar of the effects of TC within the blogosphere: A publicly-accessible film music blog evolves into a more eclectic online forum dealing with a variety of music genres, all due to a growing number of participant readers who return because of the blog initiator’s obvious passion for certain musical arts. The growing interest in the Blog X incites probable envy in one reader, whose actions eventually lead to the demise of the blog. Embedded within the text of this final blog post are

running interpretive annotations (in non-italic text within parentheses after the word 'Commentary'):

Monday, December 14, 2009
Thank You All, See You Around...
Dear Friends,
It is with great regret that I announce the official demise of this blog.
Blog X was my labor (sic) of love for more than two years, offering the opportunity to sample obscure and often-impossible to find music: music that is ignored and buried by recording companies, and otherwise unavailable to people in most parts of the world. It was a place of discovery, both for its visitors and for me, as I delighted in learning more about the music I love and share.

(Commentary: Here the initiator of Blog X offers a justification for its inception based in part on his deep interest in eclectic music as well as his contempt for the cultural hegemony sustained by the recording companies use of copyright law. Blog X was originally a film music forum but it expanded to include non-mainstream esoteric content from the jazz, easy-listening and classical genres. Meticulously assembled, download links to full compact disc or LP albums were posted on the site and these were exclusively available in lossless FLAC file format along with scans of the compact disc itself, associated album artwork and accompanying booklet. No music was stored at the Blog X site itself as these download links redirected to a commonly used file-sharing website. Donations of the monetary kind were not sought by Blog X in exchange for the downloading of music. The only currency actively encouraged was the posting of a comment signaling gratitude.)

In choosing material to feature (almost on a daily basis), I always sought to make Blog X a place that I, myself, would enjoy spending some time at. In accordance with my own musical tastes, I strove to include diverse genres, hence Blog X's familiar slogan "superb music of all kinds".

I guess I was doing something right as Blog X attracted a considerable following and I received e-mails and friendly comments on a daily basis. In addition to the stimulating interaction generated by Blog X readers, a group of friendly collectors generously contributed their own shares of hard to find, out-of-print discs and rare LP's. It all seemed like a win-win proposition for all involved, especially since the vast majority of the items on offer were not commercially available in 95% of the world. However, some blog-troll out there in cyber(looney)space was not pleased.

(Commentary: The use of pejoratives in the last sentence is an indication of the level of emotion. In Norse mythology a troll was a generally an unfavourable supernatural being, either manifesting itself as a dwarf or a giant. In contemporary vernacular, the word "troll" refers to anyone who appropriates a property that they have no original claim to and then misuses it in their name, one example being "patent trolls"[15])

A few months ago, a series of abusive, harassing (sic) and threatening e-mails were sent to me, often obscene and confusing. Obviously, a disturbed mind was at work and his attention was aimed at my blog. He also made hundreds of comments in my name, "impersonating" me at many music blogs worldwide. However, this strategy backfired on him as it attracted many more visitors to my site than before his assault

started. I also refused to acknowledge his actions or existence. This must have infuriated (sic) and enraged him, so dearly craving attention as he does.

(Commentary: The initiator of Blog X had developed a positive reputation within other film music blogs and the "blog-troll" in question may have been driven by envy in his or her behaviour as outlined.)

After a few months, my online "stalker" apparently went away (maybe he found a real job instead, I thought). Unfortunately for all the people who enjoyed discovering new musical treasures at Blog X, Mr. Troll was planning instead to eliminate all access to these by destroying the actual links to the files. He succeeded two weeks ago, and for this reason I have decided to close down all blogging activities permanently.

(Commentary: Acting as a whistleblower with possibly more selfish motives than is normally characteristic of such actions [10], the "blog-troll" reported the music content that Blog X had posted to its file-sharing site, thus resulting in the download links being made invalid over time until they were all extinct.)

I had hoped to retool and re-emerge in some alternate form and had communicated same to the many of you that had written me. I regret having to disappoint you but it seems I have little choice in the matter. I am sure the moron thinks he has punished me in some way... whatever.

I want to thank all of you who made this project a personal joy for me, all those who commented enthusiastically, and especially to those that contributed their own rare music in their own generous fashion. These people include (hope I don't leave anyone out): Buster, Derwent, Grumpy, Jamie, Alternate Athos, Jonathan F. and especially Beppo. MY DEEPEST AND SINCEREST THANKS.

Farewell, goodbye, and good luck! Hope to meet you all again somewhere soon...

6 Conclusion and Implications

In an account of the recent modest revival of interest in the analogue LP record, it has been observed that part of its appeal as a musical artefact is the social experience factor: Congregating around a record player is a physical act conducive to discussion about the shared listening event [4] Live concerts of all musical genres evoke a similar communal passion channeled towards a directed interest. Music blogs would appear to be a similar social platform for appreciative expression. In our ongoing study of film music blogs and allied online forums we have observed this passion, either from the self-evident enthusiasm of moderators or in the fervent debate, artistic exchanges that take place within emergent communities that arise from readers who come to post comments and end up creating camaraderie.

However, Blog X is an exemplary case of the negative side of social networking in the blogosphere. The final post of Blog X as discussed above is a digital "tombstone" that offers an extended epitaph of its own reason for extinction. We believe that the TC was instrumental in leading to the end of Blog X. Rather than being destroyed by the apathetic misuse of a population of individuals, the blog was effectively terminated because of the malicious actions of a single person, the so called "blog troll." This person may have been motivated through greed or envy or there may have been other more pathological reasons for the obsession. Whatever the causal reasons may

be, it does weakly suggest a non-linear manifestation of the TC in the blogosphere, namely in the potential destructive power that a lone individual can wield in this "Virtual Commons."

Natural languages emerge, evolve over time and can decay to extinction. Blogs are a conduit for natural language and they too can be subject to a similar life-cycle. The case described in this paper provides an instance of the dissolution of a community owing to the depletion of a common resource – in this case Blog X, a technological artefact shaped by societal influence and terminated because of it.

References

1. Bolter, J.D.: Writing Space: The Computer, Hypertext and the History of Writing. L. Erlbaum Associates, Hillsdale (1991)
2. Creswell, J.: Qualitative Inquiry and Research Design: Choosing Among Five Traditions. Sage Publications, Thousand Oaks (1998)
3. Deese, R.S.: A Metaphor at Midlife: 'Tragedy of the Commons' turns 40. Endeavour 32(4), 152–155 (2008)
4. Dell, K.: Vinyl Gets its Groove Back. Time, pp. 47–48 (January 10, 2008)
5. Denzin, N.K., Lincoln, Y.S.: Introduction: The Discipline and Practice of Qualitative Research. In: Denzin, N.K., Lincoln, Y.W. (eds.) The SAGE Handbook of Qualitative Research, pp. 1–32. Sage, Thousand Oaks (2006)
6. Eisenhardt, K.M., Graebner, M.E.: Theory Building From Cases: Opportunities And Challenges. Academy of Management Journal 50(1), 25–32 (2007)
7. Gephart Jr., R.P.: Qualitative Research and the Academy of Management Journal. Academy of Management Journal 47(4), 454–462 (2004)
8. Greco, G.M., Floridi, L.: The Tragedy of the Digital Commons. Ethics and Information Technology 6, 73–81 (2004)
9. Gotterbarn, D.: Dont't Soil the Commons: Turning the Blogosphere into the Clogosphere. Inroads – SIGCSE Bulletin 29(4), 12–13 (2007)
10. Hardin, G.: The Tragedy of the Commons. Science 162, 1243–1248 (1968)
11. Herring, J.: The Blogging Iceberg: Of 4.12 Million Weblogs, Most Little Seen and Quickly Abandoned. Business Wire, October 6 (2003)
12. Jubb, P.B.: Whistleblowing: A Restrictive Definition and Interpretation. Journal of Business Ethics 21, 77–94 (1999)
13. Keen, A.: The Cult of the Amateur: How Today's Internet is Killing our Culture. Doubleday, New York (2007)
14. Kolari, P., Finin, T., Joshi, A.: SVMs for the Blogosphere: Blog Identification and Splog Detection. In: AAAI Spring Symposium on Computational Approaches to Analyzing Weblogs, Stanford, CA (2006)
15. Lanham, R.A.: The Economics of Attention: Style and Substance in the Age of Information. University of Chicago Press, Chicago (2006)
16. Lanier, J.: You are not a Gadget: A Manifesto. Alfred A. Knopf, New York (2010)
17. Lenhart, A., Fox, S.: Bloggers: A Portrait of the Internet's New Storytellers (2006), http://www.pewinternet.org/Reports/2006/Bloggers.aspx (accessed on 9th February, 2010)
18. Lessig, L.: The Future of Ideas: The Fate of the Commons in a Connected World. Random House, New York (2001)

19. Li, D., Walejko, G.: Splogs and Abandoned Blogs: The Perils of Sampling Bloggers and their Blogs. Information, Communication & Society 11(2), 279–296 (2008)
20. Lindahl, C., Blount, E.: Weblogs: Simplifying Web Publishing. IEEE Computer 36(11), 114–116 (2003)
21. Lovink, G.: Zero Comments: Blogging and Critical Internet Culture. Routledge, New York (2008)
22. McDonough III, J.F.: The Myth of the Patent Troll: An Alternative View of the Function of Patent Dealers in an Idea Economy. Emory Law Journal 56, 189–228 (2006)
23. Milinski, M., Semmann, D., Krambeck, H.-J.: Reputation Helps Solve the 'Tragedy of the Commons'. Nature 415, 424–426 (2002)
24. Morrisey, B.: One in Five Blogs is Spam (2005), http://www.adweek.com/aw/search/article_display.jsp?vnu_content_id=1001736416 (accessed on 10th February, 2010)
25. Nardi, B.A., Schiano, D.J., Gumbrecht, M., Swartz, L.: Why we Blog. Communications of the ACM 47(12), 41–46 (2004)
26. Pavlov, O.V., Melville, N., Plice, R.K.: Mitigating the Tragedy of the Digital Commons: The Problem of Unsolicited Commercial E-mail. Communications of the Association for Information Systems 16, 1–20 (2005)
27. Schwartz, B.: The Paradox of Choice: Why More is Less. ECCO, New York (2004)
28. Shenk, D.: Data Smog: Surviving the Information Glut. Harper Edge, San Francisco (1997)
29. Silkstone, D.: The Blogs that ate Cyberspace. The Age (April 7, 2007)
30. Stone, B.: Diaries, Self-talk, and Psychosis: Writing as a Place to Live. Auto/Biography 14, 41–58 (2006)
31. Weitzner, D.J.: Twelve Billion Bargaining Chips: The Web Side of the Net Neutrality Debate. IEEE Internet Computing 11(1), 78–81 (2007)
32. Wright, D.J.: Glut: Mastering Information Through the Ages. Joseph Henry Press, Washington (2007)
33. Wurman, R.S.: Information Anxiety 2. Que, Indianapolis, IN (2001)
34. Yin, R.: Case Study Research: Design and Methods, 2nd edn. Sage Publishing, Beverly Hills (1994)

How to Measure Public Opinion in the Networked Age: Working in a Googleocracy or a Googlearchy?

Sean J. Westwood

Department of Communication, Stanford University,
McClatchy Hall, 450 Serra Mall, Stanford, CA 94305, USA
seanjw@stanford.edu

Abstract. The rise of the internet has transformed information acquisition from a top-down process originating from media elites to a process of self-selection and searching. This raises a fundamental question about the relationship between information acquisition and opinion formation: do the processes occur in parallel or as part of a self-directed feedback loop? That is, do we look for information to make opinions, do we look for information to support our opinions, or do we do both simultaneously? Analysis using Google search results and polling information from the 2008 US presidential election suggests that public information queries are reflective of polling data and election outcomes. The sheer quantity of search data on political terms also suggests that public information desires may surpass standard assumptions of public political sophistication.

Keywords: Internet, Search, Public Opinion, New Media, Information Acquisition.

1 Introduction

There is a well-documented relationship between the availability of information and public opinion formation: the more information that is available, the more reasoned public opinion is generally believed to be [1]. Traditional models for the process of information acquisition utilize word-of-mouth or directed search. The mediated structure of internet search engines, however, embeds the concept of algorithmic search as an almost intrinsically inseparable component of the process of information access. The prominence of search engines in ranking and filtering data raises a critical question on the relationship between information acquisition and opinion formation: do the processes occur in parallel or as part of a self-directed feedback loop? In a mediated environment, do we search for information to make opinions, do we search for information to support our opinions, or do we do both simultaneously? Moreover, if public opinion is formed through mediated information acquisition does the power of Google and other search engines impose a threat to public knowledge? There are suggestions on the possible threats [2, 3, 4] and advantages [5] to society's reliance on Google and other search engines, but an investigation of the structure of opinion formation in networked societies is needed to justify the threat of a Googlearhcy or the

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 150–160, 2010.

promise of a Googleocracy. This study examined the relationship between Google search records and traditional public opinion measures during the 2008 presidential election, comparing daily measures of both search volume and public opinion. These data do much to highlight the strong relationship between public opinion and information queries, and suggest that in the networked age opinion formation is part of a socially driven feedback loop and not constrained by search information. If anything, the data from this study suggest greater deviation from average opinion preferences in online news searches (i.e., the internet facilitates research on both sides of an issue even for those with set opinions).

The transition from the absolute monopoly of information by top-down media systems to interactive and user-driven information acquisition theoretically increases the amount of available information, but the design of the internet makes locating relevant information difficult without the assistance of search engines and peer recommendation. Although past research shows limited diversity in the websites that users access from search engines, the much more rapid pace at which modern search engines update their indexes, the tendency for Google to promote web pages linked to by highly ranked pages, and the growth of alternative sources such as blogs that frequently update may offer additional breadth of information. At the least, information is more current in search results. Outside controlled laboratory experiments, the first step to gauging how people search for political information is to look at the relative popularity of search terms related to specific measures. For this paper, searches for "Obama" and "McCain" are considered in comparison to polling data and major campaign events.

Prior to formal discussion of search results and the 2008 campaign, there are several important considerations regarding online searches that need further elaboration. Knowledge of how search engines evaluate sites on the internet is general, with the specific implementations of each search engine's algorithm kept as proprietary information. At the simplest level, Google and most modern search engines rank data by relative popularity on the internet. Early analysis of the Google PageRank algorithm by Hindmen et al. [2] suggests that Google limits user exposure to political information on the web to a small set of popular websites. Further work suggests that although search results are algorithmically generated, there is ingrained bias [3] that restricts information access and distribution [4]. This analysis is useful, but as an experimental study it has two modern problems: advancements to the structure of the Google algorithm and the decrease in the interval time between index updates.

First, Google's algorithm prioritizes quality of links over quantity of links in rating websites, so by design Google promotes listings for relatively unpopular websites that are linked to by websites that are highly ranked in Google's existing database [5]. For rapidly changing political information, this means that the Googlearchy may function more like a Googlocracy, where new political information deemed relevant by important peers is promoted in Google's rankings despite a low total number of links to the new information. This may not dilute the dominance currently exerted by the top websites in Google search queries, but the tendency for highly ranked political websites to link to relevant new sources based on content injects new sources into the top of Google by quasi "community action" and not solely through random assessment of internet content by the GoogleBot. Secondly, Google data for many of the most popular areas of the internet is updated in increments less than one hour constantly

changing the index to reflect the most recent structure of the internet, whereas the Hindmen et al. study described a state where Google updated its index every few days or even weekly. While users tend to place great trust in search results [6], the more dynamic and rapid structure of the current Google algorithm may offer great responsiveness than is otherwise assumed in existing literature.

The size of the internet is exponentially growing, and some filtering and selection occurs in the compression of nearly limitless search results to a smaller and more manageable list. Some argue that this compression artificially constrains the information available to the people [7], so the question of 'where does Google's data come from?' becomes critical in understanding how people interact with information filtered through the Google search engine. Detailed studies have discussed the transition of the print media onto the internet [8], the evolution of internet-based news organizations [9], and the relationships between information sources within the blogosphere [10], but to understand the flow of political information on the internet all three sources are necessary. While sources from each category vary in popularity within Google search results, Google includes all three together in a single index that is available to all users.

2 Methodology

Two datasets were used for this project. The first dataset captures search engine traffic and the second captures polling data for the period under study.

Search data. Data from the three major search engines would be most complete, but at present data is only readily available from Google. Using only Google data does present limitations, but as Google commands well over 50% of the search market and has demographics similar to the other two major search engines [11], Google represents a reasonable sample for internet search activity. The Google data used in this project was gathered through Google Trends. Google Trends is a web applet that provides information on search queries by geographic location and by time. This project used the search terms "Obama" and "McCain" to approximate interest in the two candidates in the Google search engine. In the configuration used for this project, Google Trends includes all queries containing the specified terms, so requests for data on "Obama" include searches such as "Obama's tax policy."

Other search engines have received criticism for result manipulation, and while Google has been criticized for advertisements placing, core search results are unaltered. Google reports data as standardized and normalized values. Data is normalized by the total number of Google queries in the selected period of time and within the selected geographic area, and is standardized by the average number of searches for a term since January 2004. For multiple search terms, the average number of searches for the first search term standardizes the values for the other search terms. Data is therefore easily comparable between search terms as a function of relative popularity.

Relative interest in political candidates is hard to assess from the Google data, as raw search volume is unavailable, but relative popularity was approximated with the inclusion of a well-known reference term. Sex, one the most consistently popular search terms used on Google since 2004 [12], was included in all data extractions from Google to provide a reference point.

Additionally, two sub-sets of data were collected from Google. To show long-term trends in interest in both Obama and McCain throughout the primary process, data from December 2007 to December 2008 was gathered. For a more targeted exploration of the influence of major campaign events on search activity and possible correlations between polling data and daily search activity, a smaller period from August 1, 2008 to November 2, 2008 was selected. The second sample captures most of the major events in the last part of the 2008 campaign and forms the basis for the majority of this paper. Data from November 2nd to November 4th is not included in the sample because the extremely high values for Obama's search popularity compresses the other data points so that visualizing differences between the graphed values is impossible without huge graphs (larger than the printed page).[1]

People also search the wide array of online information in many different ways and with high variance in methodologies [13], but the terms people search by offer insight into general intentions. Search terms including presidential candidate names likely range from searches about perceived conspiracies surrounding each candidate to searches for concrete policy details. Nonetheless, users are still searching for information related to the candidate, so grouping all searches for each candidate provides a general metric for assessing online interest in each candidate.

Polling data. All available polling data from August 1, 2008 to November 2, 2008 was collected from Pollster.com (poll n=436, response n=345,910). The majority of the polls during this period were in the field for several days, so to facilitate a more meaningful comparison between Google data and polling data, daily values were calculated from the polling data. To create daily polling averages, each poll's data was split into daily segments (sample n/days in the field) that weighted the poll's outcome for each day the poll was in the field. All values for each day were subsequently averaged, with the resulting data used exclusively in this paper.

3 Results and Discussion

Global summary: December 2007 to December 2008. Interest in both McCain and Obama grew dramatically between December of 2007 and December of 2008. Throughout this period, Obama remained more popular than McCain, with the exception of the time surrounding the RNC, when McCain surpassed Obama's popularity (scaling and rounding issues obscure this in Figure 1). McCain also remained less popular than the reference search term "sex", while Obama was more popular than sex between October 19th and November 9th. In addition to a larger number of searches for "Obama" during this period than for "sex," the relative interest in sex decreased linearly toward November. To the credit of Americans, people were searching for Obama instead of sexual material during this brief window.

Overall, interest in both Obama and McCain grew dramatically throughout the sample period. Searches for Obama grew to 6.6 times their average scaled level at Obama's peak on November 6 from .15 the average level at the sample's starting

[1] Raw Google data ranged in value from the low twenties to the hundreds, so to allow visual comparison between polling data and Google data on a single graph, all Google values were divided by 100.

point. Likewise, interest in McCain peaked at 1.5 (still less than a quarter of Obama's peek popularity) Obama's average scaled search level on November 2 from a starting point of .05 Obama's average scaled search volume[2].

Increases in Google search activity generally corresponded to important events during the campaign, though there were several peaks that are not readily explained by the events of the campaign. Discussion of specific events in each of the final three months of the election follow, but it is important to note the inexact match between campaign events and Google search fluctuations to contextualize the discussion.

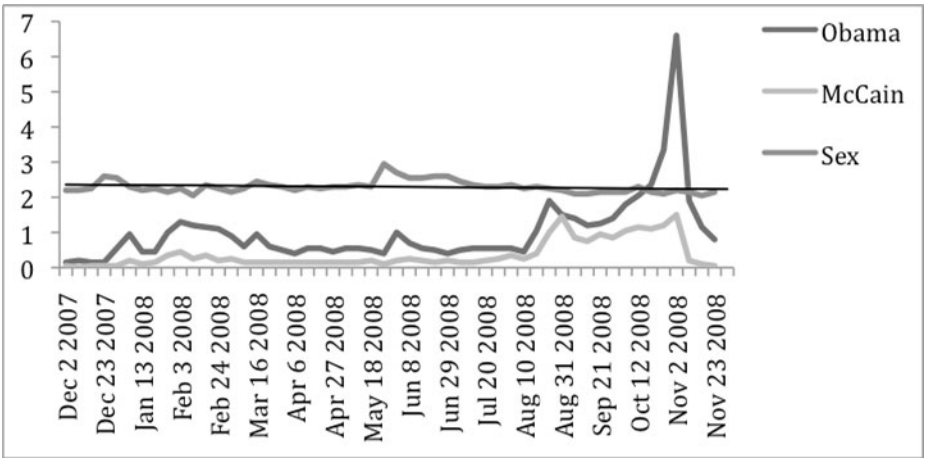


Fig. 1. Google search data December 2007 to December 2008

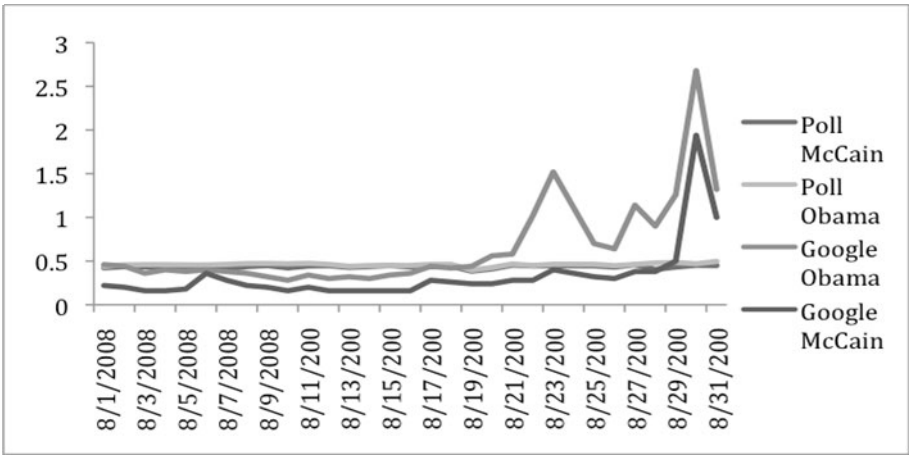


Fig. 2. Google and Polling Data August 2008

[2] All reported values are scaled by average interest in Obama over time. It is tempting to refer to the units in this paper as "Obama units," but for the sake of readability and clarity the numbers appear without this unit notation.

Table 1. Significant campaign events in August

Date	Event	Difference from Google Average Obama/McCain (Obama-McCain)[3]	Polling Difference %[4]
8/16	Saddleback Debate	-0.64/-0.84 (0.2)	1.68
8/23	Biden Announced as VP	0.52/-0.6 (1.12)	1.74
8/27	Biden Accepts Nomination	0.14/-0.62 (0.76)	0.45
8/28	Obama Accepts Nomination	-0.1/-0.62 (0.52)	7.50
8/29	Palin Announced	0.26/-0.5 (0.76)	5.29

Throughout August, several bumps and drops in search interest for both candidates occurred. Before the Saddleback appearance, search volume for "McCain" was relatively flat, while search volume for "Obama" increased moderately. Following the appearance at Saddleback a sharp rise in search volume for "McCain" and a sharper uptick for "Obama" search volume occurred, although the relative difference between Obama queries before and after Saddleback was low. Search volume for both candidates was relatively flat before the announcement of Biden as Obama's VP, while after the announcement Obama interest tripled while a noticeable jump in McCain interest appeared. Interest in Obama also increased with his formal acceptance of the nomination, although not as significantly as with the announcement of Biden.

The most interesting observation from August coincides with McCain announcing Palin as his nominee for vice president. Interest in McCain increased to its highest point for the month, but interest in Obama also increased to its highest level of the month. Obama, even during the period of Palin's announcement, was a more popular search term throughout the month than McCain. While it is reasonable to argue that Obama's popularity during the Palin announcement resulted from the buildup and bleed from his highly televised acceptance speech, interest in Obama as a search term immediately dropped after his speech before increasing at the same time as Palin's announcement. It is hard to explain this observation, but it is possible that interest in Obama increased during this time because internet users waiting for the McCain vice presidential nomination were not satisfied with Palin and wanted to look at Obama as an alternative. It is also possible than Obama loyalists were interested in the Obama response to the Palin announcement. Both explanations, while not exhaustive, might also occur because of the younger and more liberal internet audience.

During August, search interest was roughly comparable to polling data, though the increases in Obama search traffic far exceed his polling gains around the Democratic National Convention.

[3] Values show the difference between search volume on each day compared to average search volume from January 2004. The parenthetical shows the difference between the relative search popularity of Obama and McCain. Positive values show an Obama advantage.

[4] Difference in calculated daily polling numbers. Positive values show an Obama advantage. Source of event dates: New York Times.

Table 2. Significant Campaign events in September 2008

Date	Event	Difference from Google Average Obama/McCain (Obama-McCain)[1]	Polling Difference %[2]
9/3	McCain Accepts Nomination	-0.13/-0.2 (0.07)	3.10
9/4	Palin Accepts Nomination	0.35/0.21 (0.14)	5.32
9/5	Fannie Mae and Freddie Mac Bailout	0.36/0.98 (-0.62)	-1.44
9/15	Collapse of Lehman Brothers	-0.22/-0.46 (0.24)	0.20
9/23	Palin Couric Interview	-0.28/-0.56 (0.28)	2.80
9/25	McCain Suspends Campaign	-0.2/-0.28 (0.08)	1.24
9/26	WaMu Fails/Presidential Debate	-0.09/-0.17 (0.08)	6.82

Although Google interest in McCain did not surpass Obama with the initial announcement of Palin as the Republican vice presidential nominee, during the period of the Republican National Convention Google recorded more searches for "McCain" than for "Obama." This blip is the only time McCain searches outpaced Obama searches and corresponds to a brief inversion of McCain and Obama in polling data.

The period of the financial crisis between the placement of Fannie Mae and Freddie Mac into government conservatorship and the collapse of Lehman Brothers saw a minor increase in searches for Obama and McCain as compared to the period immediately before and after the events. The upswing during this time was, however, very small and relatively even between the two candidates except for September 5th, when interest in the McCain campaign was high but decreasing. The relative differences between Obama searches and McCain searches during this period were approximately consistent at around .24.

Table 3. Significant Campaign events in October and November 2008

Date	Event	Difference from Google Average Obama/McCain (Obama-McCain)[1]	Polling Difference %[2]
10/3	Stimulus Package Passed	0.12/-0.30 (0.42)	6.25
10/16	Final Debate	0.88/0.16 (0.72)	5.15
10/18	Al Smith Dinner	0.4/-0.22 (0.62)	6.81
10/21	Palin's Wardrobe	0.54/-0.24 (0.78)	7.56
10/30	Obama Infomercial	2.38/-0.06 (2.44)	6.38

As was the case with the initial announcement of Palin, the suspension of McCain's campaign and the financial sector bailout increased interest in both candidates on Google, but while the increase was roughly equal among the candidates Obama remained more popular than McCain.

For the majority of October the relative number of Obama and McCain searches rose and sank in unison and roughly in line with poll numbers, with the number of searches for Obama increasing significantly throughout the month and the number of searches for McCain remaining relatively flat. Searches for both candidates rose during the time of the third presidential debate, but other newsworthy events such as the cost of Palin's wardrobe and the relative buzz of the Al Smith dinner do not appear to show any significant change in search numbers.

Interest in Obama started to rise before the Obama infomercial and peaked during the pre-election period on the night of the broadcast. Unlike large events in the McCain campaign, where interest in Obama rose with McCain, interest in McCain in the period around the Obama infomercial did not significantly change.

The data from this project show the relative popularity of political search terms increased over time and were biased in favor of Obama. The approximate demographics of the internet favor those younger than 65 (predominantly those under 29) and those with higher incomes [11]. In this environment, the higher frequency of searches for Obama over McCain makes sense given the higher level of Democratic support among younger and more financially secure Americans. Although it is also possible that the general movement in support of Obama influenced the popularity of searches for Obama, the inability for McCain to gain more searches than Obama during any period other than the RNC suggests that demographics play a significant role in explaining search popularity. This is most probable given that when interest in McCain rose, interest in Obama usually rose to a level above McCain.

While "sex," one of the most popular search queries on the internet, was included in the initial analysis as a reference term to gauge an approximation of how frequent searches for Obama and McCain were, the selection of the term showed an interesting swing in popularity between Obama and sex. For the last week of the campaign, possibly due to the Obama infomercial and heavy press coverage suggesting an Obama victory, searches for Obama outnumbered searches for sex by a significant amount, and searches for sex decreased as compared to previous points in the year. Although no statistical test was performed to gauge the magnitude of the swap, it is possible that people who would otherwise search the internet for sex searched for information related to Obama, or that searches for Obama increased broadly enough to decrease other types of searches during the period.

4 Correlation between Polling Data and Google Searches

The observational conclusions in the previous sections of the paper are important in contextualizing how Google searches and campaign events are related. Graphs for Google data from August, September, and October included polling data as a reference, though the scale of the Google search data flattens the polling data and limits useful comparison. For the purposes of the following analysis, two graphs appropriately scaled for Google data and polling data are most useful.

Both graphs look approximately similar in shape and show similar general trends (when different scaling is accounted for), with both graphs showing a clear Obama advantage with the exception of the period surrounding the RNC. To compare the two data sets, differences between Obama and McCain were calculated for polling data and Google data. The correlation between the difference between Obama and McCain's polling numbers and the difference between the number of Google searches

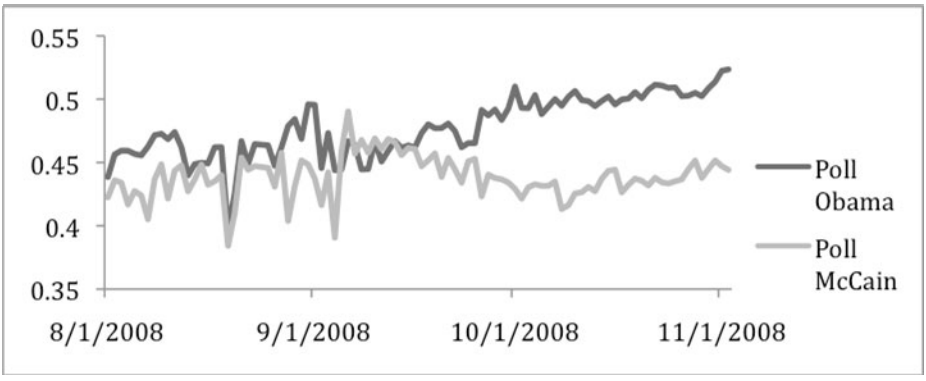


Fig. 3. Averaged daily Obama and McCain polling data

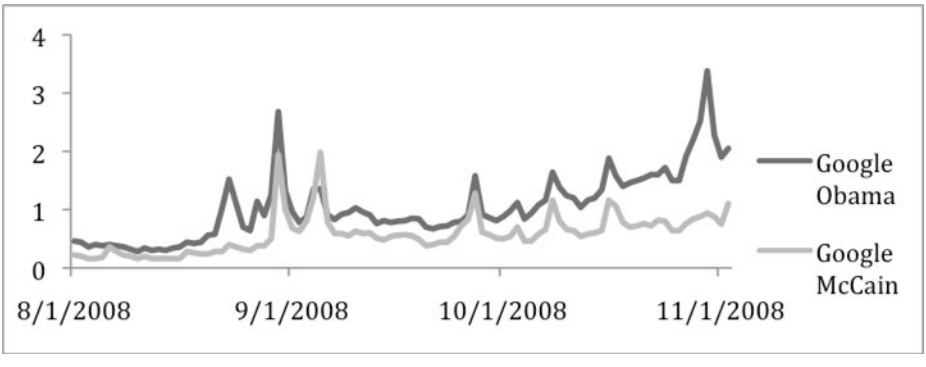


Fig. 4. Daily Obama and McCain Google searches

for Obama and McCain is highly statistically significant with r=.612 and p<.001. Despite relatively high increases in Google search volume and relatively low decreases in search volume as compared to fluctuations in polling data, this correlation makes sense. Polling data has an upper and lower bound defined by partisan voters, while the desire for information logically crosses ideological bounds that constrain more dramatic shifts in polling data.[5]

5 Implications

The proportion of Google searches conducted for each of the candidates is highly correlated to poll numbers. Considering the limitations of online search data, it

[5] As an interesting aside, a correlation between election outcome and Google search volume difference (Obama – McCain) by state is significant r=.293 (p=.018). States where Obama is more popular are more likely to support Obama in the general election. Although, this suggests that McCain victory in states is a function of the extent to which he was less popular in each state and not a result of actual superiority in search quantities as Obama had a clear advantage in all states and Washington D.C.

appears as if the swings in search volume simultaneous to polling data illustrate a relationship between campaign events, public opinion, and search volume. Further research is required to investigate the causal forces for this correlation, but these findings are suggestive of a public that forms opinions and searches for information in similar ways and volumes. The relative freedom in information acquisition compared to opinion change perhaps also magnifies jumps in search data as compared to jumps in polling data, which explains the much more significant increases in search volume compared to polling data around important campaign events. It is also possible that people are actually motivated to investigate major campaign events regardless of ideology, although since we do not know who is searching it is conceivable that political junkies are simply following the news as it happens in Google. However, it is probably less likely that the truly informed and motivated would actively search out information on Google instead of visiting trusted news websites or blogs, while it is more reasonable to assume that the less technologically skilled and political innocents would start information searches with Google.

These data further suggest that public information queries—a lá Google—are reflective of polling data and election outcomes, and that public information desires may surpass standard assumptions of public political sophistication. The high correlation between search queries and standard public opinion measures also suggest that although Google filters information, it provides information within a Googleocracy of rapidly changing information networks. That is, the information indexed by Google responds to the rise of new information networks and that these networks are driven—or at least—related to the opinion of the actual public. For rapidly changing political information, this suggests that in such a Googlocracy new political information deemed relevant by the public is presented at a higher position in Google's results[6], and that this becomes a recursive process of information demand and information provision.

References

1. Mill, J.S.: On liberty. Broadview Press, Ontario (1999)
2. Hindman, M., Tsioutsiouliklis, K., Johnson, J.A.: "Googlearchy": How a Few Heavily-Linked Sites Dominate Politics on the Web. In: Annual Meeting of the Midwest Political Science Association, Chicago, pp. 1–33 (2003)
3. Goldman, E.: Search Engine Bias and the Demise of Search Engine Utopianism. In: Spink, A., Zimmer, M. (eds.) Web Search: Multidisciplinary Perspectives, pp. 121–133. Springer, Heidelberg (2008)
4. Diaz, A.: Through the Google goggles: Sociopolitical bias in search engine design. In: Spink, A., Zimmer, M. (eds.) Web Search: Multidisciplinary Perspectives, pp. 11–34. Springer, Heidelberg (2008)

[6] The Page Rank algorithm is, roughly defined, a means of ranking based on ties between network actors (websites). More central websites, as defined network measures are more "important" in assessing content. In this model, new information relayed by highly ranked peers is promoted in rankings. Simultaneously, the calculation of network importance is a result of public action. Rankings are therefore derived from public action and used to filter future public queries.

5. Menczer, F., Fortunato, S., Flammini, A., Vespignani, A.: Googlearchy or Googlocracy? In: IEEE Spectrum Online (2006)
6. Fallows, D.: Search Engine Users. Pew Internet and American Life Project (2008)
7. Adamic, L., Huberman, B.: The Web's Hidden Order. Communications of the ACM 44(9), 55–60 (2001)
8. Boczkowski, P.J.: Digitizing the News: Innovation in Online Newspapers. MIT Press, New Bakerville (2004)
9. Blumler, J.G., Gurevitch, M.: The new media and our political communication discontents: democratizing cyberspace. Information, Communication and Society 4, 1–13 (2001)
10. Adamic, L., Glance, N.: The political blogosphere and the 2004 U.S. election: divided they blog. In: International Workshop on Link Discovery. ACM, Chicago (2005)
11. Quantcast (2008), `http://www.quantcast.com` (cited November 11, 2008)
12. Google Trends (2008), `http://www.google.com/trends` (cited November 14, 2008)
13. Hargittai, E.: Informed Web Surfing: The Social Context of User Sophistication. In: Howard, P., Jones, S. (eds.) Society Online: The Internet in Context. Sage Publications, Thousand Oaks (2004)

A Multidiscipline Approach to Governing Virtual Property Theft in Virtual Worlds

Nicholas C. Patterson and Michael Hobbs

School of Information Technology, Deakin University
Waurn Ponds, Victoria, 3217, Australia
ncp@deakin.edu.au, mick@deakin.edu.au

Abstract. The crime of virtual property theft has become a serious problem in virtual worlds in recent years. Players of these games are repeatedly falling victim to this crime, with little or no repercussion for the offender. Virtual property often has a substantial real world monetary value and the theft of such items impacts greatly on victims. The problem of virtual property theft is complex, involving many legal, regulatory and technological factors. As such, trying to address this problem in a single dimension is not sufficient, each factor need to be addressed with a multidisciplinary approach. In addressing this problem, this paper provides a model for describing the issue of virtual property trading and the issues associated with virtual property theft. The paper also proposes an approach for handling virtual property theft based on improvements to laws related to virtual property and theft, improvements to the virtual world software components and better regulation from governments.

Keywords: Virtual Property, Intellectual Property, Massively Multiplayer Online Games, Virtual Worlds, Virtual Property Theft, Real Money Trading.

1 Introduction

Virtual world games, often referred to as massively multiplayer online games, have evolved from traditional pen and paper based role playing games and that of networked multi-user dungeons or MUDs [1]. Game developers have extended the concept of MUDs, creating persistent worlds that continue to exist independent of any single player in the game, much like the real world [1]. In the context of this article the real world refers to activities that exist purely in real physical space where humans interact and a virtual world is everything that exists within digital space only. To define virtual worlds more explicitly; they are best described as an avenue for social interaction and a venue for hundreds of thousands of people to join together in exciting scenarios [2]. Virtual world games provide dynamic environments which allow individual game players to personalize their game experience through the collection of in-game items, completion of quests and the interaction with other game players. These virtual worlds usually have an active economic system [2], which provides players with an additional dimension to relate to the game. It is important to note that within the environments of virtual worlds, interaction between players is controlled

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 161–171, 2010.

by the developers and maintainers of the game and not by the players – which is both a key ingredient in the creativity of such environments but also a key cause of the problems that underlie virtual property theft.

Game developers can personalize a player's experience in a virtual world by allowing things such as a unique game character and allowing players to own virtual property; this can help promote a player's psychological bond to the game. The attachment a player has to their game character and its possessions not only holds a personal value for the game player but can also hold a real world monetary value. This value is the result of an investment of time, effort, skill and even real world money; a value that is able to be exchanged or even stolen.

Virtual property theft has been become an urgent area of research for two main reasons [2]. Firstly, player ownership of virtual property within a game can create an impact in the real world, in the form of economic and legal consequences [2]. The second reason is that there is no agreement or foundation for ownership of virtual objects gained by players [2]. Most virtual worlds games have an economic system, allowing players to trade, buy or sell virtual property and involves large amounts of real world money [2]**.** In the context of this article virtual property theft involves the theft of property that exists purely in a digital space or environment; this differs to traditional theft where it involves the theft of an actual, physical item.

There are currently over 100 virtual world games in existence, in different stages of development or operation [3]. Some of these virtual worlds have great numbers of active players, for example World of Warcraft, which is currently the most popular MMOG (massively multiplayer online game) claims to have more than 10 million users worldwide [3]. The large number of games and game players highlights the urgency of finding a solution to the problem of virtual property theft.

Within this article the enlisting of multiple strategies is proposed to achieve a solution to the problem of virtual property theft. The reasoning for this is that virtual worlds are complicated environments where a single solution may not be effective enough in defeating the problem of virtual property theft. These strategies will come in the form of legal, regulatory and software-security based solutions. The contribution of this article will give readers an informed view of how players interact with virtual world games as well as displaying how they function. Readers will discover what virtual property theft entails and what laws and regulations exist that can help protect the stakeholders from this crime. Finally, an outline of a multidiscipline approach to solving the problem of virtual property theft is presented. To achieve this goal, the paper is structured as follows. Section 2 provides a model of a virtual property trading system outlining the mechanics of virtual worlds and how players interact and trade virtual property. Section 3 discusses the issues of the game code complexity and the laws related to virtual property ownership and theft. Section 4 presents a multidisciplinary approach to addressing virtual property theft in virtual world games. While, Section 5 provides concluding remarks.

2 A Model of a Virtual Property Trading System

Virtual world games are rich, complex environments that provide the players of these games a diverse range of experiences and enjoyment. The concept of virtual property

plays an important role in the support of player enjoyment. To simplify the discussion on this topic and to help highlight the issues associated with virtual property in virtual world games, the presentation and description of a generalized model can be useful.

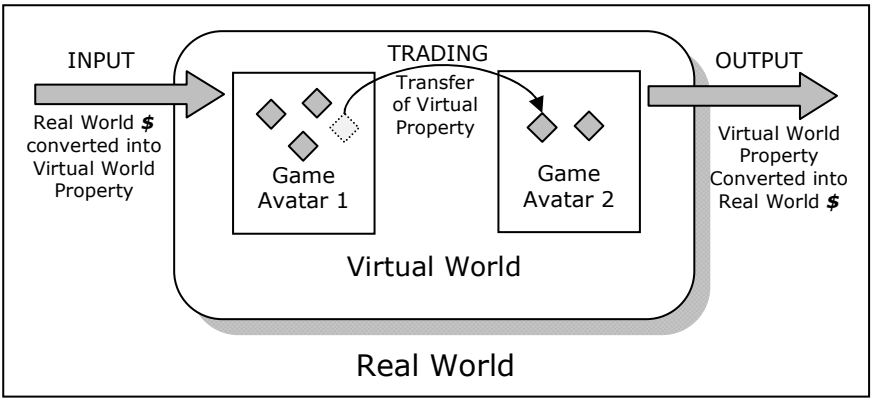


Fig. 1. A model of Virtual Property Trading in a Virtual World Game

The model presented in Figure 1 is an original representation of how the authors believe virtual property trading occurs within a virtual world game. The key features of this model include: the virtual world and the entities that represent game players in the game (referred to as Game Avatars in the figure); the possessions of the game players (Virtual Property); the mechanisms to transfer virtual property between players (Trading); and finally, the interface between the virtual and real worlds (Input and Output). The following sub-sections will expand and elaborate on each of these features, highlighting the potential risks for game players of experiencing virtual property theft.

2.1 Virtual Worlds and Avatars

The virtual world, represented in games such as World of Warcraft [4] and virtual environments such as Entropia [5] and SecondLife [6] is the result of the creative and technical efforts of game designers and developers. These environments are large, complex software applications that are specifically designed to support many hundreds of thousands of concurrently active game players in the virtual world. The game designers and developers provide the environment or platform in which game players can interact. The game play rules and permitted activities are written in software code and controlled through system configuration parameters (e.g., availability of game resources, difficulty levels of in-game tasks, challenges and or opponents).

The level of detail of these virtual worlds, along with the ability for players to customize their avatars and existence in the virtual worlds, are among the key factors which attract people to such environments. The level of attachment players have to their avatars and the virtual property items they acquire forms the foundation for the degree of impact a player can experience when virtual property they possess (in which

they have a great personal or financial investment in) is taken away from them. The methods of how virtual property is acquired and transferred between players (which are core to the issue of virtual property theft) are detailed in the following sub-sections.

2.2 Virtual Property Acquisition

There are two possible methods a player is able to gain possession of virtual property in a virtual world game. In the first case, a player can earn virtual property through activities performed in the game. These relate to the game play rules determined by the games designers and can take a variety of forms, including: defeating various in-game enemies, where the defeated opponent drops various virtual property items that can be collected by the victor and performing in-game quests or missions which can be rewarded with virtual property items once finished successfully. Most virtual world games also have non-player characters who sell virtual items, so a player can buy these directly for a set amount of virtual currency. The last means of acquiring items involves real world currency and buying specific items off an auction website.

The second method game players acquire virtual property is through making virtual property items using in-game tools. Once made, these virtual assets are introduced into the virtual world to be utilized by the game player or by other players; examples of these can range from avatar clothes or even buildings. Another means by which virtual property can be made (specific to some virtual world games) is through profession based skills of the avatars, such as a tailor or blacksmith. These skills allow the avatars to collect raw materials and be able to make virtual items for themselves or other players.

The investment in terms of time, effort, skill and even real world money, results in great value being placed on the virtual property items acquired by game players. Ku & Gupta [7] support this position by stating that they strongly believe that virtual property gathered within these games such as currency, swords, armor and jewelry not only contain an in-game value but also have value in real world economic markets. They also provide an indication [7] of the 'value' of virtual property, examples include a high level virtual character in the world of the popular game Lineage [8] can fetch upwards of $800 USD and in a Yahoo [9] auction for a Mahjong account with 3 million Mahjong currency will fetch around the same price of $800 USD. In the first week of January 2010 a virtual space station in the virtual universe Entropia sold for $330,000 USD [10].

2.3 Transfer Mechanics of Virtual Property

It is common for game play rules that govern a virtual world game, to support the transfer of virtual property from one avatar to another. Normally performed through a consenting trade mechanism these transactions are done with a benefit to both players. In some cases this transfer of virtual property is conducted without the consent of the virtual property owner, usually through deceit or by compromising the game players account. The methods available to the game players to trade virtual property, either with or without consent, vary between games and environments. These methods of trade are implemented as core features to the software code but not intended to enable

virtual property theft; they simply allow for it to happen in the right scenario without any code modifications on a criminal's part.

In their book Intelligence and Security Informatics; Ku and Gupta [7] categorize online gaming crime to include: virtual property theft and robbery, fraud, kidnapping, threat, assault and battery, destruction of property, counterfeiting, receipt of stolen property, privacy violations, software piracy, extortion and gambling [7]. In an examination of 613 online gaming criminal cases, occurring during 2002 in Taiwan it was found that theft and fraud were the major type of online gaming crimes [11]. 73.7% of cases were charged with theft, while 20.2% were charged with fraud [11]. These criminal cases came from official crime reports, from different judicial or investigative authorities [11].

The implications of game players owning virtual property (that hold a real world value) combined with the potential for that property to be stolen highlights the need for some method of recourse if such a situation occurs. In the real world, such circumstances are governed by rules of law covering theft and crime – the application of these laws or the creation of new laws to cover virtual worlds is in its infancy. The issues related to laws governing virtual property theft are explored in Section 3.

2.4 Interfaces between Virtual Worlds and the Real World

Players have discovered that there is a real world value for virtual property items in online marketplaces [7]. Large amounts of real world money is paid to obtain specific virtual items they can use within the game [7], usually to gain some kind of advantage within the game, such as a harder hitting sword. The market place for virtual property has created the potential for profit through the bidding, selling, trading and exchanging those virtual items [7]. This is where the problem of virtual property theft arises, due to the large amounts of virtual property transactions within these virtual worlds, it has attracted the attention of computer criminals [7]. These computer criminals develop methods to perpetrate these virtual worlds through hacking, cheating and scamming to make money from the sale of virtual property [7].

The trade of virtual property items has become a lucrative business in South Korea [12], and many other countries, due to the increase in popularity of online games. Dozens of companies such as PlayerAuctions [13] and ItemBay [14] in the past few years have been established to provide a secure means to perform virtual property exchanges; whether it is paying real money for virtual property or simply trading one item for another [15]. PlayerAuctions deals purely in virtual objects mainly from the game EverQuest [16] and receives over two million hits a day and ItemBay which is the dominant virtual object trading site for the Korean market (from over 130 similar sites) is reported to have an annual revenue greater than that of the combined virtual worlds it services [17]. ItemBay take around 5 percent of the virtual property sales price purely as commission; in the year of 2006 they earned $18.6 million USD in commission alone and $5.8 million USD in net profit [12].

From 2002, the crimes associated with online gaming have become a significant problem. In Taiwan more than 37% of all criminal cases relate to online gaming [18]. This crime has spread across many Asian countries including China, South Korea, Japan and Singapore [18].

3 Factors Relating to Virtual Property Ownership

As shown in the previous section, the features of virtual worlds and the virtual property that can be acquired provide players with great enjoyment as well as the potential for real world financial rewards. These financial rewards also provide criminals with motivation to obtain virtual property without consent, known as virtual property theft. The issue of virtual property theft is complex because virtual world games not only contain game developer made property but also property that the players can acquire/create; a situation that blurs the ownership of these items. Compounding this problem, the complexity of the software code that implements the virtual worlds game play that supports both intentional and unintentional transfer of virtual property between game players. These issues of the game code complexity and the laws related to virtual property ownership and theft are detailed in the following sub-sections.

3.1 Virtual World Software Issues

Virtual world games have become a target for criminals who are looking for virtual items (such as in-game gold) because it contains real world value. These criminals deliberately break into players accounts, steal virtual property and virtual characters in the game and then sell them, usually on the black market, for thousands of dollars [19].

One plausible reason why computer criminals have opted into virtual world crime is that it brings less risk than traditional forms of crime, as there is little chance that police will be able to prosecute them for stealing a *magic potion* for example [19], even if they are caught. In the United States, among other countries, these criminals also benefit greatly from very loose or nonexistent virtual property laws [19]. It is believed game designers are reluctant to push for legal recognition of virtual property for fear of being held liable for theft [19].

Virtual world games inherent issues of any software based application. The authentication procedures of many of these games are often antiquated at best; they consist of two fields, login and password which are typed in manually and then a login button is pressed. These forms of authentication can be broken quite easily. Recovery of virtual property within these virtual worlds can also be quite difficult. This often is the result of just not having the functionality within the game to do this or when an item is lost or stolen it has to be tracked from the original source to the new source which can involve detailed and complex database operations. The last issue that is problematic on the software mechanics is not being able to detect when virtual property theft is occurring or when it has occurred for that matter; the alarm is often only raised when a player realizes their account has been broken into and virtual property has been stolen.

3.2 Increasing Popularity of Virtual World Games

The last few years have seen a massive spike in the popularity of virtual world games, there are reports stating that in the order of 100 million people worldwide are logging on to play within them [20]. The issue of virtual property theft becomes important mainly due to the huge growth in the video game market, it is stated in the DFC

Intelligence report [21] that the worldwide online games market will grow from $3.4 billion in 2005 to be well over $13 billion in 2011.

3.3 Laws and Regulations Related to the Governing of Virtual Worlds

There are few laws and regulations that are specifically written to cover actions that occur in virtual worlds, due primarily to the relatively new and evolving environment they present. Although there are a number of traditional areas of law that have a close relationship to virtual property ownership, which include laws that relate to the game developers, such as end user license agreements (EULA), and those that are related to the game player, such as intellectual property rights and unfair competition. Governments are also interested in real world money being turned over, with the view of applying traditional taxation regulations to virtual world transactions.

Chinese Law Case Study

To add an extra dimension of complexity to this issue**,** virtual worlds are commonly accessible over the internet, meaning that the virtual world may be hosted in another country to you, raising the question of which country has jurisdiction when a crime is committed. China for example, has developed laws that cater specifically to the virtual property theft as shown in the case Li Hongchen vs. Beijing Arctic Ice Technology Development Co. In 2003, a Chinese gamer sued the game company Beijing Arctic Ice Technology Development Co. and won after the virtual world game company which runs Red Moon (Hongyue) refused to restore his stolen virtual property [22]. Hongchen spent years and thousands of dollars building up a virtual arsenal in the game Red Moon and claimed that his virtual property was stolen by hackers [22]. The end result of this court case which was held in Chaoyang District Peoples Court in Beijing was that Arctic Ice was found negligent for allowing a hacker to access Li Hongchen's game account and alter the *data* that represented his virtual property. Therefore the court ordered Artctic Ice to replace the virtual property, so Hongchen could go ahead and use them again in the context of the game [22].

End User License Agreements (EULA)

The EULA (End User Licensing Agreement) is an agreement and set of terms the player must agree to and abide by before they can play the game. World of Warcraft [4] and Entropia [5] both enlisted the use of a EULA to manage virtual property and any other possible issues; for example not only are all game developer components owned by the game developers but they also own any content created by the players inside or outside of the game [3]. The virtual environment Second Life is different, in that players who create content can begin selling it to other players inside the game because they control the intellectual property rights of their creations. However Linden Labs [6] the creators of Second Life still impose some limitation such as having the right to delete any or all of your content and requiring you to license it to them and every other user of the game for free [3]. MacInnes [23] argues that game companies use the EULA in the hope that will protect themselves against litigation (the action of taking out a lawsuit against an individual); by stating in the agreement that “virtual property has no real world value”. These agreements could easily be voided by the court system if they determine that the EULA is too one sided [24] or the virtual property obtained and earned by the player holds value or theft of virtual property caused by game security flaws.

Intellectual Property Rights and Laws of Unfair Competition
Companies that are in the business of developing massively multiplayer online games receive copyright protection for their games and graphics, but this same copyright protection does not allow them to stop players from selling parts of the game; such as their character, currency or other virtual property [25]. In fact intellectual property law actually grants players property rights and the permission to sell the game characters they own and have established over time, along with any property those characters own [25].

One other avenue for players to take is trade dress protection which falls under the intellectual property umbrella and refers to how a product looks and feels or its packaging. It is defined as the entire image or overall impression of the packaging or presentation of a product or service that identifies the source or good or services [25]. Essentially if a product has a unique look in its packaging, it can be protected. So essentially if a virtual character or virtual property item has a unique look established by the player, they could potentially own the rights to it.

This law of unfair competition protects unregistered trademarks and also trade dress, allowing for a player's game character to qualify as an unregistered trademark or receive trade dress protection [25].

In order for a player to qualify for protection, they have to identify the source of the goods and services in the minds of the consuming public; it is important to note that the actual identity of the source is not needed only that the goods or services originated from a single anonymous source [25].

Government Taxation Laws
The United States Internal Revenue Service has declared it would be very difficult to administer the taxation of virtual property transactions [26], for two reasons**.** Firstly, the need to be able to track and reconstruct many small transactions and the second is placing a value on virtual transactions would be quite hard; many of these items have an in-game value which is controlled by the game designers; adapting the value of virtual property to the real world is difficult.

The U.S. Congress and other governmental entities are close to determining how to establish policies and regulations regarding the income that is made by these game players performing real money trading (turning virtual property into real money) [27]. One country in particular that has implemented a virtual property tax law is China. In 2005 it was reported that as many as 100,000 people were employed as professional virtual currency 'farmers' [28] and no doubt that number has increased now in 2009. The Chinese government declared that it will tax profits where transactions involve virtual currency [28]. This tax law enforces a 20% tax on the income from virtual currency sales by each individual seller.

4 Proposal for a Multidisciplinary Approach to Addressing Virtual Property Theft

In order to prevent instances of virtual property theft, there has to be some kind of deterrent. The role of a deterrent is to assist in stopping these individuals from performing future acts involving malicious activity. Deterrents can be in the form of taxation, government laws, end-user licensing agreements or private regulations. The

more deterrents in place; the harder it can be for potential criminals to ignore them. The whole goal behind deterrents in criminal law is to discourage members of the public from committing criminal acts, purely through fear of punishment.

The governance of virtual worlds and stopping the crime of virtual property theft has to come in a multi disciplined approach as it is a complicated problem. Governing virtual worlds through legal and regulatory avenues is only part of an overall solution. There is still a need for other distinct software based security methods to be produced in further work. Should software based solutions be produced they will hopefully aim to improve the security of these virtual world games through a variety of methods, for example through more secure authentication techniques, the ability to detect and identify when virtual property theft has occurred possibly before the player even realises, and lastly, where the other modules fail; the ability to recover stolen virtual property by game administration staff in an efficient manner.

Regarding the legal options; firstly there needs to be property rights established for virtual property. Property rights to protect players property from being stolen by other players and loss of virtual property due to negligence or confiscation by game developers [3].

On the regulatory side, there needs to be clear cut rules and regulations when it comes to the EULA and game administrators who deal with complaints and breaches in the EULA need to be informed on the action to take in each specific offence**,** there should be no grey areas.

Lastly the legal system should be improved in order to be able to deal with the complexities of virtual worlds and virtual property. This would involve developing specific virtual world laws that deal with every possible crime that can occur within these worlds, whether it is the theft of virtual property or one of the other crimes discussed in section 2.3; in-game assault and battery for example.

5 Conclusion

Virtual world games and environments are vast and contain many virtual items that carry great economic value. Criminal perpetrators leave a trail of virtual and real world destruction in their wake; whether it is stealing another player's entire account, stealing virtual property or forcing game administrators to ban compromised accounts.

As real money trading of virtual property continues to increase in terms of economic growth; governments are starting to take notice and no longer ignore the issue. Governments may actually realize now that individuals are making significant untaxed revenue from selling in-game virtual property. There is strong motivation for legislation which can prohibit and deter individuals from performing virtual property theft and the sale of virtual property. The proposal presented in this article outlines a multidiscipline approach to the problem of virtual property theft in virtual world games. It covers the legal and regulatory side of the problem and also covers methods to combat the software side of the problem and to improve security; through improved authentication techniques, introduction of detection methods and lastly the ability to recover lost or stolen property back to the original owner. There needs to be a solution to this problem sooner rather than later to protect both individual players, game

developers and any corporate entities who invest into virtual worlds. The proposal presented in this article and the future work in the form of the software based solutions to improve security and the ability to handle virtual property theft discussed above are to be conducted by the authors and could potentially diminish the problem significantly if not completely.

References[1]

1. White, E.E.: Massively Multiplayer Online Fraud: Why the Introduction of Real World Law in a Virtual Context Is Good for Everyone. Northwestern Journal of Technology and Intellectual Property 6(2), 228–243 (2008)
2. Eriksson, A., Grill, K.: Who owns my avatar? Rights in virtual property. In: DiGRA Conference, pp. 1–7 (2005)
3. DaCunha, N.S.: Virtual Property, Real Concerns. ExpressO (2009), http://works.bepress.com/nelson_dacunha/1/
4. Blizzard.Entertainment. World of Warcraft Community Site (1991), http://www.worldofwarcraft.com
5. MindArk. Entropia Universe (2009), http://www.mindark.com/entropia-universe/
6. Linden.Research.Inc. Second Life Official Site (1999), http://lindenlab.com/
7. Ku, Y., Gupta, S.: Online Gaming Perpetrators Model. In: Yang, C.C., et al. (eds.) Intelligence and Security Informatics, ISI 2008 Workshops, pp. 428–433. Springer, Heidelberg (2008)
8. NCSoft. Lineage - Popular fantasy MMORPG from NCSoft (2009), http://www.lineage.com/
9. Yahoo.Inc. Yahoo! (1994), http://us.yahoo.com/
10. Thier, D.: Virtual Space Station Sells for Price of an Actual House (2010), http://www.aolnews.com/nation/article/virtual-space-station-sells-for-price-of-an-actual-house/19305309
11. Chen, Y.-C., et al.: An analysis of online gaming crime characteristics. Internet Research 15(3), 246–261 (2005)
12. Jin-seo, C.: Hackers Paralyze Web Sites of Game Money Trading Firms (2007), http://www.koreatimes.co.kr/www/news/biz/biz_view.asp?newsIdx=11821&categoryCode=123
13. PlayerAuctions. PlayerAuctions - Play. Trade. Dominate (2009), http://www.playerauctions.com/
14. ItemBay. Professional online game virtual currency supplier and buyer and seller of game accounts (2005), http://www.itembay.ca/
15. White, E.E.: When Pretend Money Has Real Value: A Study of Virtual Property in Online Gaming. Northwestern Journal of Technology and Intellectual Property & Technology Law Journal 6(2), 228–243 (2008)
16. Sony.Online.Entertainment. Sony Online Entertainment LLC (SOE) (1995), http://www.station.sony.com/sonyonline/
17. Bartle, D.R.A.: Pitfalls of Virtual Property. The Themis Group, pp. 1-22. The Themis Group Incorporated. Durham, North Carolina (white paper) (2004)

[1] All websites checked and accessed on 1st February 2010.

18. Chen, Y.-C., et al.: Online Gaming Cheating and Security Issue. In: Cantarella, J.D. (ed.) Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC 2005), vol. I(1), pp. 1–2. IEEE Computer Society, Los Alamitos (2005)
19. Spring, S.: Virtual Thievery. Newsweek (Atlantic Edition) 148(24), 10 (2006)
20. Kane, S.F.: Virtually Lawless: Legal & Economic Issues in Virtual Worlds. Computer & Internet Lawyer 25(6), 13–24 (2008)
21. DFC.Intelligence, Virtual Property and Real Money Trade: A Business and Legal Survey, pp. 1-55. DFC Intelligence, San Diego, (2009)
22. Meehan, M.: Virtual Property: Protecting Bits in Context. In: Richmond Journal of Law and Technology, pp. 7–48. University of Richmond School of Law (2006)
23. MacInnes, I.: The Implications of Property Rights in Virtual Worlds. In: 10th Americas Conference on Information Systems, New York, pp. 2727–2723 (2004)
24. Dougherty, C., Linden, B.v.: Virtual Property Rights Litigation. E-Commerce Law & Policy 9(7), 1–5 (2007)
25. Stephens, M.: Sales of in-game assets: An illustration of the continuing failure of intellectual property law to protect digital-content creators. Texas Law Review 1513(80) (2002)
26. Internal. Revenue. Service, National Taxpayer Advocate. In: 2008 Annual Report to Congress, pp. 336. Internal Revenue Service (2008)
27. Mennecke, B., et al.: It's Just a Game, or is It? Real Money, Real Income, and Real Taxes in Virtual Worlds. Social Science Research Network (2007)
28. Zhang, B., et al.: China Taxes Real Profits from Virutal World Transactions. In: Pillsbury Winthrop Shaw Pittman LLP. Pillsbury Law, New York (white paper) (2008)

Section 3

Surveillance and Privacy

Surveillance and Privacy

Yola Georgiadou[1] and Simone Fischer-Hübner[2]

[1] Faculty of Geo-Information Science and Earth Observation (ITC),
University of Twente, PO Box 6, 7500 AA Enschede - The Netherlands
[2] Karlstad University, Department of Computer Science,
Universitetsgatan 2, S 651 88 Karlstad / Sweden
georgiadou@itc.nl, simone.fischer-huebner@kau.se

Recent social and technical developments are expanding surveillance by the government and private sector and intensifying privacy concerns, resulting in a surveillance-privacy dilemma. Governments establish surveillance schemes to fight terrorism and crime. Private organizations use profiling and data mining techniques to target marketing endeavors, to analyze customer behavior and monitor the work practices of employees. Social networks bring to the fore new means for the surveillance of individuals, publishing intimate details about themselves. Individuals are usually unaware of the constant data collection and processing in their surroundings. They are effectively losing control over their personal spheres. The aim of the conference track "Surveillance and Privacy" is to discuss and analyze, from multi-disciplinary perspectives, the privacy risks of surveillance for individuals and society, as well as solutions for protecting an individual's right to informational self-determination.

As argued by Edwards et al. [1] the key question is "*whether we choose, for any given problem, a social or a technical solution, or some combination. It is the distribution of solutions that is the object of study. An everyday example comes from the problem of email security. How do I distribute my trust? I can delegate it to my machine, and use Pretty Good Encryption for all my email messages. Or I can work socially and organizationally to make certain that sysops, the government, and others who might have access to my email internalize a value of my right to privacy. Or I can change my own beliefs about the need for privacy – arguably a necessity with the new infrastructure*" (p.6).

The Track 3 on "Surveillance and Privacy" at HCC9 is introduced by a keynote presentation by Klaus Brunnstein on the future of Privacy and Surveillance in the Information Society.

In the four articles of this track, authors either inscribe privacy solutions in technical artifacts (Hoepman and Kuntze & Rudolph) or argue and advocate for a more social solution to the privacy-surveillance dilemma (Clarke and Verplanke et al.). In the panel, the members dissect and debate the future of privacy for the millennial generation.

In "Privacy enhanced fraud resistant road pricing", Hoepman presents an architecture for a road pricing system where privacy is achieved by implementing two technical design principles: (i) splitting of trips into short segments (so-called legs) that are non-linkable to each other and (ii) distributing the process steps needed to determine the overall road charge over several system components, so that no single component has enough information to reconstruct a particular route travelled. Invoices contain

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 175–177, 2010.

aggregated information, while the charging details are available only to the vehicle driver. Fraud is avoided by integrating random spot checks in a novel enforcement protocol.

In “Privacy in distributed commercial applications”, Kuntze and Rudolph analyze the different and possibly conflicting security and privacy requirements of multiple stakeholders in distributed commercial applications. They propose pseudonymous or anonymous attestation of the state of a device installed in a user’s home as a building block towards privacy-preserving, secure, distributed commercial applications. They discuss two possibilities for pseudonymous and anonymous attestation. The first uses a generic approach of deep attestation through virtual machine to the hardware TPM. The second relies on the mutual attestation of nodes in the network.

In “Civil Society Must Publish Standards Documents”, Roger Clarke argues for social solutions to the privacy-surveillance dilemma, and puts the onus squarely on the shoulders of civil society. He advocates for public interest NGOs to invest more in 'practical activism' by establishing Standards and Process Descriptions, which clearly communicate their expectations and provide benchmarks against which the inadequacies of processes and the unacceptable dangers of projects and schemes can be delineated. Using examples of public interest standards development, he demonstrates that public interest NGOs can emulate industry and government in playing the standards game.

In “Citizen Surveillance of the State: A mirror for eGovernment?”, Verplanke and co-authors also advance a social solution to the privacy-surveillance dilemma, a case of what has come to be called “sousveillance.’ They outline an approach where citizens invert surveillance tools (e.g. Google Earth), made available by global corporations, to hold government accountable for the delivery of basic public services. Commercial virtual globes act as a mirror to the traditional eGovernment framework and make visible to all, in real time, both the performance of government services and localized citizens’ needs.

In the panel “Privacy...going, going, gone?” Ianella and other panelists show how social networks have put the media spotlight on privacy, as new and old web companies vie for the attention of an increasingly polarized global web community. The panel debates issues arising from the social web, including privacy dramas on social networks, technical challenges to privacy, the redefinition of privacy norms and solutions to address these issues in terms of law, enforcement, practice, design and technology and the future survival of privacy as a concept.

Acknowledgments. We want to thanks the track 3 programme committee very much, who contributed with helpful reviews, comments and who help us to select the papers for track 3. In this context, we especially want to acknowledge the programme committee contributions by Roger Clarke, George Danezis, Marit Hansen, Francis Harvey, David-Olivier Jaquet-Chiffelle, Eleni Kosta, Andreas Pfitzmann, Kai Rannenberg, Morton Swimmer, Jozef Vyskoc and Diane Whitehouse and well as the help by the sub reviewer Matthias Kirchner.

Reference

1. Edwards, P.N., Jackson, S.J., Bowker, G.C., Knobel, C.P.: Report of a Workshop on "History & Theory of Infrastructure: Lessons for New Scientific Cyberinfrastructures, NSF Grant 0630263, Human and Social Dynamics, Computer and Information Science and Engineering, Office of Cyberinfrastructure (January 2007), http://deepblue.lib.umich.edu/bitstream/2027.42/49353/3/UnderstandingInfrastructure2007.pdf

Trends of Privacy and Surveillance in the Information Society
Extended Abstract

Klaus Brunnstein

Department for Informatics, University of Hamburg, Germany
brunnstein@informatik.uni-hamburg.de

In the late 1980s, when large computers still dominated the application of Information Technologies to enterprise, industrial development and university research, and when small computers and networks had only begun to develop, some experts (mainly from the USA) predicted that future IT could be applied to government agencies as "Community Information Utilities (CIUs)". As contemporary IT was regarded inadequate (insufficient process and storage capacities, no remote access, missing system and software application), a moratorium for applications was suggested until the adequate IT would be available. Visions included many advantages for the citizen, such as availability and accessibility of public information and direct access for citizens to services from governments and agencies, to support "Free Flow of Information (FFO)" (as enshrined in the constitution of the USA). Experts suggested developments to related software, but technical matters concerning protection in hardware, systems and application programs were not addressed, and protection of the citizens private information – aka privacy – was not sufficiently discussed.

Indeed, both the technical capacities of small, distributed and connected computers and manifold applications, developed much faster than anticipated. These developments were governed by the principle "Enable Global Free Flow of Information", which has been realized in contemporary Internet services, social networks and mobile technologies. As provisions for protection of information (both data representing possibly sensitive information, as well as methods to work with such data) were not sufficiently designed and implemented into systems and applications. Service providers (e.g. in telecom and communication industries and social networks) today use available data without reference to the needs and interests of customers who use "their" data. Not surprisingly, customers begin to adapt their understanding to technical options: although a user "profile" contains potentially sensitive data that may be used against the respective person at some later stage, many users don't use minimal measures to inhibit illicit usage of related data (e.g. by using protective options), and worse, customers use methods of remote surveillance inherent in their personal IT (mobile search for "friends").

As in the past, technical developments will continue to shape the usage of IT in the future, following the principle: "All that is technically possible, will also be realized and used". Technical trends will support the storage and processing of much larger amounts of data, globally accessible and consequently stored in globally available storage ("clouds"). Significant growth of data streams and storages will essentially come from enabling physical actors (from sensors to multiple devices, including

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 178–179, 2010.

heartbeat controllers, machines and factories) to communicate over global communication lines, for example: a suitably (e.g. IP3 protocol) equipped Internet/Web 3.0 interface. With the demand to remotely control processes (thus enhancing possibilities for surveillance) and to store growing masses of data, system and application software will become more complex and more difficult to analyse (including certification). With equally growing opportunities for new kinds of applications and services, the demand for more specific data will also lead to less control by users and customers and therefore to less protection of sensitive data. As data and processes will also be sensitive for enterprises, there is some hope that their interest and request for data protection will also help users and customers to protect sensitive personal information (aka “privacy”).

Civil Society Must Publish Standards Documents

Roger Clarke

Xamax Consultancy Pty Ltd, Canberra
Visiting Professor, Australian National University
Visiting Professor, University of N.S.W
roger.clarke@xamax.com.au

Abstract. A great deal of energy is wasted by civil society anguishing over the harm done to people by corporations, governments and technologies. Far too little effort is invested by public interest NGOs in 'practical activism'. This paper argues that civil society must establish Standards and Process Descriptions which clearly communicate their expectations, and which provide benchmarks against which the inadequacies of processes and the unacceptable dangers of projects and schemes can be delineated. The paper provides several examples of policy statements and templates of the kind that it is argued need to be provided.

Keywords: NGO, Public Interest Organisation, Privacy, Consumer Rights.

1 Introduction

Civil society is being overrun by the 'imperatives' of economics, technology and politics. Non-Government Organisations (NGOs) that represent the public interest score small wins from time to time. Overall, however, the last 50 years have seen massive encroachments into human freedoms in what has variously been referred to as 'the free world' and 'the advanced western economies'. Worse, the scene is set for public-private partnerships between large, powerful, transnational corporations and small, weak nation-states, to lead to a 21st century version of feudalism.

Part of the reason for this state of affairs is the failure of civil society institutions to harness their resources to good effect. A very large proportion of the energies of 'concerned citizens', and of organisations that represent them and advocate for their interests, is frittered away on dinner conversations, submissions to institutions that have no intention of taking any notice of them, conference presentations and posts to bulletin-boards that preach to the converted, and most recently those utterly ineffectual forms of vanity-press – the blogosphere and twitterdom.

In order to have real impacts on the processes of businesses and governments, civil society needs to articulate its requirements, and publish its demands as formal Standards against which the actions of businesses and governments can be assessed. Progress will have been made when the media routinely reports that a particular government proposal scores only, say, 27/100 on the Civil Society Human Rights Impact Assessment scale, and that a business project fails on, say, 10 of the 24 mandatory features of the NGOs' Business Project Assessment Standard.

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 180–184, 2010.

2 Standards and Standards Processes

During the early twentieth century, the engineering professions developed documents that declared safe thresholds for technical measures in areas such as construction. This gave rise to series of formal Standards in various national series such as those of the British Standards Institution (BSI, since 1901), the American National Standards Institute (ANSI, since 1916) and Deutsche Industrielle Normen (DIN, since 1917), and in some international contexts, such as the association of Institute of Electrical and Electronics Engineers (IEEE, since 1884/1912/1963).

Umbrella organisations emerged, in some cases to develop standards, and in others to anoint and re-publish selected national and international Standards. The International Organization for Standardization (but commonly referred to as ISO), which was established in 1947, complements several other organisations that focus on particular domains.

The large numbers of technical Standards have underpinned technological progress and many aspects of public safety. A second form emerged to complement the technical Standards. So-called 'process standards' describe organisational business processes such as complaints-handling mechanisms and quality certification.

Institutions grew up around the processes whereby Standards were developed, adopted and published. As the scale of activities grew, and their competitive significance increased, corporations and industry associations became larger players. By the last quarter of the 20th century, many standards processes were entirely dominated by corporate interests.

Even where standardisation processes are conducted by engineers in their professional rather than their corporate capacities, such as those of the Internet Engineering Task Force (IETF), non-engineering perspectives are largely excluded. One reason for this is the the highly technical nature of much of the work and the intellectual dominance, and single-mindedness, of the engineers who do it. Another is the lack of funding support for NGOs to participate in meaningful ways in standards development processes.

NGOs that represent and advocate for the interests of consumers and citizens have achieved, at best, token participation in standards processes.

3 Examples

This section provides brief overviews of four examples of public interest standards with which the author has been deeply involved. There is of course a range of other examples that require study in order to provide a more substantial empirical base, including documents of Consumers International, the Electronic Privacy Information Center (EPIC) in Washington DC, and London-based Privacy International.

3.1 CCTV

The Australian Privacy Foundation (APF) is that country's primary public interest NGO focusing on privacy. Since 1987, it has worked variously alone, and in conjunction with civil liberties and consumer associations. Its activities were reviewed in [4].

For many years, APF's policy contributions were primarily reactive, in the form of submissions to governments and parliaments relating to particular projects and schemes. Since 2006, it has been moving towards a more proactive stance, by formulating and publicly declaring its policy positions on particular topics, and communicating those positions in advance of projects being announced, rather than just when projects are well-advanced.

One example of an APF Policy Statement is that on 'Visual Surveillance, including CCTV' [3]. The elements of the Policy Statement are:

- a declaration of the policy's scope;
- a set of principles that projects need to comply with;
- a list of resources of value in conducting assessments.

Much of the Policy Statement is obvious to public interest advocates with knowledge of Closed-Circuit Television (CCTV). Its value lies not in any claims of originality, but in its provision of clear statements, its existence as a reference-point against which each particular project can be evaluated, and its availability as a standard against which the media can report project proposals to be tenable (few) or unjustified failures-in-waiting (most).

The adoption by civil society of such a document as a formal Standard would provide community groups worldwide with a focal point for their efforts against the excesses of image and video surveillance, and a reference-point for academics and the media.

3.2 ANPR

The APF has also published a Policy Statement regarding the related topic of Automated Number Plate Recognition (ANPR) [2].

This represents a counter-balance against the joint positions of the security industry and the national security extremists who grasped for control of law enforcement communities on 12 September 2001.

Crucially, the Policy Statement does more than just point out the dangers, and rail against the opacity of process, the lack of justification, and the continual presentation of projects as *faits accomplis*. It presents a specific alternative, referred to as 'black-list-in-camera' architecture, which balances the public interests in surveillance of miscreants and in non-surveillance of everyone else. Such Policy Statements can be complemented by deeper analyses, e.g. [10].

3.3 Privacy Policy Statements

Privacy Policy Statements (PPS) are a creature of the U.S. political scene. In the absence of effective privacy laws, such protections as consumers enjoy derive from commitments entered into by the service-provider, and a PPS enables those commitments to be kept separate from the Terms of Service document. PPS may also be relevant in some other countries that have little or no privacy law.

In countries that have data protection laws in place, PPS sit oddly, and are little more than window-dressing. On the other hand, there are some benefits in organisations confronting the question of what they actually do with personal data. Industry

associations provide templates, but they of course are self-serving, not privacy-protective. Law firms prepare precedents, but they are proprietary rather than published, are inevitably legalistic and difficult to understand, and serve the interests of the client not the public. Data protection commissioners publish guidelines, but these are inevitably jurisdiction-specific, and limited by both the terms of the local legislation and the imaginations and levels of commitment of the commissioner and their staff. Remarkably, however, there appear to have been few attempts by civil society to express the public's expectations of a PPS.

A Privacy Statement Template was published in [5], with an accompanying guide in [6]. During the first 4 years after its publication, the template gathered over 17,000 hits. It has been used by a number of organisations in preparing their own PPS. Its primary benefit, however, is as a standard against which the PPS of particular companies can be compared, in order to expose weaknesses. In a study of a sample of 6 representative organisations reported on in [7], the Statements were found to fall far short of the norms that consumers would reasonably expect in relation to the handling of personal data.

3.4 Consumer-Marketer Communications

The Terms of Service that are imposed by international consumer marketing corporations are generally based on the permissive laws of the U.S.A., and fall far short of both the consumer protection laws in some other countries, and the reasonable expectations of consumers.

In 2005, I looked for an authoritative statement by the consumer movement of what they expected from marketers. I found no such document. In order to assess the Terms of Service of the same 6 companies whose PPS I had studied [7], I had to prepare what I referred to as a 'Normative Template for Marketer-Prosumer Communications'. This was first presented in [8], and a revised version is in Appendix A of [9].

The Template is currently being used in research into the state of consumer protection laws in Australian jurisdictions [11]. Its value can be far greater than that of a mere research tool, however. If this (or some variant of it, or replacement for it) were to be adopted by major institutions of civil society, it would provide at the very least a Checklist of the matters that companies need to address. With some further articulation, it is capable of becoming a formal declaration of expectations, and a Standard against which marketing organisations' Terms of Service can be measured – and (in almost all cases) found to be seriously wanting.

4 Conclusions

These examples of Policy Statements and Templates demonstrate that documents can be assembled that codify public expectations in relation to particular activities, and particular technologies. Several advantageous features of such documents have been highlighted.

The argument is not that these specific documents should be adopted by consumer bodies as Standards. What these mini-cases demonstrate is the feasibility of civil society Standards. They can be drafted by individuals or small working parties. The

two APF documents were not only drafted but were also then negotiated, amended and adopted by a national NGO. To date, these quite recent Policy Statements have had only modest impact. On the other hand, the APF's track record is strong, having succeeded in altering the framework within which discussions of privacy law take place in Australia, through its lead-role in the promulgation of the Australian Privacy Charter [1]. This included the Anonymity Principle, which is progressively being implemented within the Privacy Principles in all jurisdictions within that country.

Industry and government have been playing the Standards game for many years. By publishing Documents that have capital letters, economic and political institutions have inculcated acceptance by the media and the public that all is well, and have thereby been able to avoid critical examination of their initiatives.

Community institutions must raise themselves from their torpor, stop wasting their time grizzling, adopt the well-proven technique of promulgating Standards, match the bravado with which business and government announce their initiatives, and attract the media into reporting the positions of civil society with the same enthusiasm that they show when they re-print media releases distributed by corporations and government agencies.

References

1. APCC: Australian Privacy Charter. Australian Privacy Charter Council (December 1994), http://www.privacy.org.au/apcc/
2. APF: Automated Number Plate Recognition (ANPR). Policy Statement, Australian Privacy Foundation (March 2008), http://www.privacy.org.au/Papers/ANPR-0803.html
3. APF: Visual Surveillance, incl. CCTV. Policy Statement, Australian Privacy Foundation (October 2009), http://www.privacy.org.au/Papers/CCTV-1001.html
4. Bennett, C.: The Privacy Advocates: Resisting the Spread of Surveillance. MIT Press, Boston (2008)
5. Clarke, R.: Privacy Statement Template. Xamax Consultancy Pty. Ltd. (December 2005a), http://www.rogerclarke.com/DV/PST.html
6. Clarke, R.: About the Privacy Statement Template. Xamax Consultancy Pty. Ltd. (December 2005b), http://www.rogerclarke.com/DV/PSTAbt.html
7. Clarke, R.: A Pilot Study of the Effectiveness of Privacy Policy Statements. In: Proc. 19th Bled eCommerce Conf., Slovenia, June 5-7 (2006a), http://www.rogerclarke.com/EC/PPSE0601.html
8. Clarke, R.: A Major Impediment to B2C Success is ... the Concept 'B2C'. In: Proc. ICEC 2006, Fredericton NB, Canada, August 14-16 (2006b), http://www.rogerclarke.com/EC/ICEC06.html
9. Clarke, R.: B2C Distrust Factors in the Prosumer Era. In: Proc. CollECTeR Iberoamerica, Madrid, June 25-28, pp. 1–12 (2008), Invited Keynote Paper, http://www.rogerclarke.com/EC/Collecter08.html
10. Clarke, R.: The Covert Implementation of Mass Vehicle Surveillance in Australia. In: Proc. 4th Workshop on the Social Implications of National Security: Covert Policing, Canberra, April 7 (2009), http://www.rogerclarke.com/DV/ANPR-Surv.html
11. Svantesson, D., Clarke, R.: A Best Practice Model for eConsumer Protection. Computer Law & Security Review 26(1), 31–37 (2010)

Citizen Surveillance of the State: A Mirror for eGovernment?

Jeroen Verplanke[1], Javier Martinez[1], Gianluca Miscione[1], Yola Georgiadou[1], David Coleman[2], and Abdishakur Awil Hassan[1]

[1] University of Twente, Faculty of Geo-information Science and Earth Observation – ITC, P.O. Box 6, 7500AA Enschede, The Netherlands
[2] University of New Brunswick, Canada
verplanke@itc.nl, martinez@itc.nl, miscione@itc.nl, georgiadou@itc.nl, dcoleman@unb.ca, hassan22386@itc.nl

Abstract. This paper discusses, conceptually and empirically, the role of geographic ICT (geoICT) and virtual globes (e.g. Google Earth) at the interface of public policy and citizens. Our preliminary findings from on-going field work in an Indian city and in Zanzibar suggest that virtual globe technology can potentially transfer to citizens surveillance power, traditionally held by the government. Starting from the traditional electronic government framework, where bureaucracy acts as a filter between policy makers and citizens with grievances, we outline an emerging framework where commercial virtual globes act as mediators between policy-makers and citizens. We show that the emerging framework holds the potential of allowing citizens concerned, in our case, about the quality of water services, to influence policy makers directly. The virtual globe acts as a mirror to the traditional eGovernment framework and lends a different societal visibility both to public services provision, and to localized citizens' needs.

Keywords: Geographic ICT (geoICT), Electronic Government (eGovernment), Electronic Grievance (eGrievance), Virtual Globe, Google Earth (GE), Volunteered Geographic Information (VGI).

1 Introduction

Electronic government (eGovernment) research has focused mainly on individual government organizations and on the impacts of information and communication technology (ICT) on the capabilities of single government units [1]. Zouridis and Thaens [2] argue that the four spheres of traditional government—policy, politics, organization, citizens—have been affected only partly by ICT.

Table 1 summarizes the spheres of government and the rather limited loci of eGovernment. In the policy sphere, eGovernment concentrates mainly on policy implementation, not on agenda setting and policy development. In politics, ICT's role is mainly in democratic supervision (online access to laws and regulations). In public sector organizations, ICT plays a role only at the operational core of public administration,

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 185–201, 2010.

Table 1. Locus of traditional government and of eGovernment, adapted from Zouridis and Thaens [2]

Spheres	Traditional Government	Electronic Government
Policy	Problem acknowledgement and agenda setting, policy development and decision making, policy implementation, policy control	Policy implementation
Politics	Representation, idea generation and consideration, decision making and deliberation in parliament, democratic supervision	Democratic supervision
(Public) Organization	Executives; Strategic top; Operating Core; Technostructure; Support Staff	Operating core
Citizens	Citizens as rulers (voters & participants in policy processes); Citizens as ruled (subject to authority, consumers of services)	Citizens as consumers of services

due to the emphasis on service delivery. In the citizens' sphere, eGovernment is mostly concerned with citizens as passive consumers of services.

eGovernment has been studied mainly in the North. In the South, research on this topic is scarce, and the situation of such efforts is uncertain. Heeks [3] estimates that eGovernment projects are 35% total failures, 50% partial failures and 15% successes. He attributes failure to the gap between hard rational design and soft political realities caused by the three-way association of IT, universalist modernization and Western rationalism. His argument resembles Avgerou's [68], who claims that different rationalities coexisting within and around ICT projects are a major issue for their understanding, and development.

Despite their narrow focus and the limited success to date, eGovernment initiatives around the world still aim to transform all spheres of government, especially the interface between different stages of the policy cycle—problem acknowledgement and agenda setting, policy development and decision making, policy implementation, policy control—and citizens. In problem acknowledgement and agenda setting, significant visibility gains may accrue to citizens and policy makers alike if they can collectively "visualize" places identified as problem areas—places signaled and tagged by citizens' grievance reports or places where complaints are acknowledged. Locating and visualizing these places requires geographic ICT (geoICT) to be integrated to the eGovernment system.

Since the launch in June 2005 of Google Earth (GE), commercial virtual globes have been hailed for providing the "benefits of accessibility, interactivity, and engagement in landscape visualisation to millions, with the promise of greater representativeness in the views seen by users, improved accuracy of 3D imagery, and accelerated learning" [42, p. 14]. Citizens stand a realistic chance to influence policy & decision making, not because of intended government action, but due to unintended consequences [71] of action taken by global market actors, driven by advertising revenue and market share. Are these developments inverting the panoptic power of the state and vesting surveillance power to citizens? What are the social and political implications? Due to the novelty of virtual globes, empirical research, especially in the South, is practically non-existent.

Here, we discuss the extent to which virtual globes can expand the limited focus of eGovernment, based on preliminary findings and insights from our own research in

two empirical cases; in an Indian city and on Zanzibar. We focus on the potential role of geoICT and virtual globes in improving citizen participation in problem acknowledgement and agenda setting.

2 eGrievance Systems, Virtual Globes and Volunteered Geographic Information (VGI)

eGovernment initiatives in industrialized and developing countries hold the promise of a more citizen-centric government with reduced operational costs [4]. Governments use ICT to deliver efficient and cost effective services, information and knowledge [5]. Some authors claim that the adoption of a private sector management model, emphasizing the accountability of managers and a results orientation, will transform the public sector [6]. With online public services, especially through the internet, increasingly seen as part of a broader service (improvement) strategy, citizen dissatisfaction with the quality of the services may quickly become a major political issue [7, 8]. Although the telephone and face-to-face contact are still more frequently used, and are rated higher than internet contacts [9], many studies reveal the increasing use of the internet for service provision to citizens [10, 11], as well as improved citizens' interaction with government [12, 13].

Citizens usually contact local government to request a service or information, lodge a complaint or voice their opinions, among other reasons. The contacts tend to be "geared toward matters of everyday service delivery rather than large-scale policy" [22]. Good contact experiences are important to both citizens and governments. The government may learn about the concerns of its citizens, their "contents and discontents." Citizens may learn of government services and benefits, how government functions, who is responsible for certain decisions. A satisfactory contact experience may improve a citizen's feeling of trust towards their government [20].

Other values hailed as constituting "good governance", such as participation, transparency, responsiveness, equity and inclusiveness, effectiveness, efficiency, and accountability may also be upheld in government-citizen contacts [23, 10].

Specifically, one of the ways ICT is expected to change the relationship between citizens and local governments is by facilitating participation. Citizen participation in local governance is significant in two respects: citizen participation reveals their collective preferences, ensures that local government is responsive to their needs, strengthens representative institutions and enhances democratic legitimacy [14, 15]. Out of the two main streams identified for eGovernment adoption—the supply side (government to citizen) and the demand side (citizen to government)—only the supply side is well documented in the literature [16, 17, 18, 19]. The demand side of eGovernment adoption is less explored [20, 21].

2.1 eGrievance Systems

Grievance (redressal) systems are a particular type of citizen-initiated contact within eGovernment [24, 25]. Other terms, including complaint handling mechanisms [26], citizens' complaints [27, 28, 26] and public feedback mechanisms [29] are regarded as synonymous to, and interchangeable with, grievance systems. Grievances can be

defined as "an expression of dissatisfaction […] about […] action or lack of action or about the standard of a service", as suggested by the British Local government Ombudsman [30].

Seneviratne and Cracknell [31] summarized four characteristics of clearly defined procedures of complaint handling in local governments: "bottom up" accountability of the grievance system, rational decision making of local governments, non-exit options for citizens unlike business consumers, and the political nature of liberal democracies, positing legitimacy and accountability as the ultimate test of successful government transformation.

Several local governments, both in the North and in the South[1], have adopted electronic versions of complaint handling, in other words electronic Grievance (eGrievance) systems. In India, citizens register their complaints via the internet or use SMS over their mobile phone for urgent complaints [32]. Generally, eGrievance systems are viewed positively [25], in particular their potential to increase openness and transparency within the public administration [32]. Another example is the public service monitoring system in Tanzania, on Zanzibar, supported by UN-Habitat [33]. Here a system depending entirely on mobile communications technology has been set up as a pilot to monitor public water services. The system promotes transparency by visualizing citizens' complaints regarding water quality and availability directly through a web-client on a dedicated website using Google Maps.

It is because of these abilities that eGrievance systems are considered the key to increase transparency in e-Government initiatives [29]. The level of complaints can be expressed in a range of indicators— including measures of citizen satisfaction, accuracy, quality and reliability of services—that together indicate whether citizens are getting the service that they need and want [34]. This is well documented in environmental complaints where the complaint is seen as the perception of existing environmental problems [35, 36, 25]. This distinction is fundamental: the systems being discussed here are not intended to monitor the actual status of service delivery, but citizens' needs and the distance between expectations and provision.

Brewer [26] argues that "accountability may be weakened when service recipients are defined less in terms of their citizenship and more on the basis of a narrowly defined status as a marketplace consumer." When citizens are framed as electronic consumers, government may be more responsive only to certain groups in society [37], citizens with an electronic link to government, thus weakening overall government accountability. The inherent "responsiveness bias" in traditional government-citizen contacts, which Schumaker and Getter [38] defined as "the degree to which governments respond unequally to the preferences of various subpopulations in their communities", may become a "digital divide" between categories of people and the differences between people who are connected and people who are not connected [39].

Complaint handling, or service recovery, is central to customer service operations. Complaints comprise an important form of data and show firms where service quality falls below the standards of customer expectations [40]. Does responsiveness to complaints (or complainers) constitute better service to the public? And when public

[1] With "North and South" we refer in this document to the traditional division between the industrialized countries in the Northern hemisphere and the lesser developed countries that are mostly situated in the Southern hemisphere.

servants are encouraged to "listen to the customer," what arrangements will ensure that they listen to those customers less able to exercise their voice, who cannot or do not express their preferences well or clearly, and who may receive poorer quality service if greater discretion is given to frontline personnel? And are there ways in which a customer service focus ignores—or worse, exacerbates—inequalities among customers? The above mentioned questions pose critical aspects of electronic grievance systems that could exacerbate the inequality of citizens if not managed properly. Theoretically, what is in question here is the rationalization function that the bureaucracy is supposed to exercise on society. Bureaucracy is intended to transform political problems into administrative problems by applying formal procedures equally for all. Is it going in that direction?

2.2 Virtual Globes and Volunteered Geographic Information (VGI)

The emergence of commercial virtual globes and the advent of web 2.0 open new possibilities for citizens to interact with other citizens and government. Web 2.0 allows collaboration in which users are able to interact with each other, to provide information to central sites, and to see that information is collated and made available to others [41]. Combining Web 2.0 functionalities with virtual globes, such as Google Earth, is meaningful for issues where place and spatial information are at the forefront, either for citizens or service providers. Web 2.0 combined with Google Earth allows earlier participation and multiple views in planning processes, possibilities for online feedback and dialogue, multiple views of the world expressed simultaneously, especially in environmental issues [42]. It also offers NGOs the ability to do technical analyses, causing shifts in the epistemic balance of power between civil society and the state as a result [43].

While Google Earth is foremost a commercial internet application, driven by marketing share and advertising revenue, people use it to explore the world, to look for well documented anomalies [44], derive pleasure from searching for black helicopters, engage in virtual tourism and creatively make subversive mash-ups [45]. Volunteers produce, use and 'produse' [69] geographic information in social networking and collaborative web-based efforts like *Open Street Map, Tagzania, Wayfaring.com,* the *People's Map,* and *Platial: The People's Atlas.* Volunteered geographic information (VGI) provided by citizens redistributes the rights to define and judge the value of the geographic information and of a new production system in general [65].

On the other hand, creativity and active sites of resistance (counter-mapping) to military secrecy by a conscious re-purposing of mapping and satellite imagery have consequences. Counter-mapping practices show how panoptical power can be reclaimed by those formerly cast as subject to the gaze of the state [45]. This in turn leads to concerns of legitimacy. Visualizations and graphics created by lay people may be seen as less dangerous, because they carry less authority. However, when such 'unofficial' graphics find their way into the public discourse or decision-making, they can raise difficult issues for society, such as "who has a legitimate voice?", "whose visualization is right, or more legitimate?" [42]. Kingsbury and Jones [44] and Parks [46] provide examples from Google Earth to illustrate different versions of ''truth" or emphasis on "urgency to act" for example with regard to thematic coverage of the crisis in Darfur. Spatial-temporal discrepancies between added media and

underlying maps and images can (willingly or not) create a picture that appears more realistic than it actually is.

Trust issues are for instance raised about the absence of metadata [47] for geographic information supplied through Google Earth (and most other virtual globes) regarding the commercial actors controlling the data, its quality and accessibility. International organizations and citizens are dependent on (a limited number of) third party commercial wares to share geographic information in a user friendly fashion. Google is quite willing to exercise control over data access that has never been freely communicated. In trusting commercial companies, we may be running the risk of developing public delusion over what is happening in the world [48], since image currency and resolution reflect perceptions of market potential and not of public interest [49]. Also scientific information is shared through virtual globes and 'cloud based' collaboration software. Concerns over control and access to scientific information in turn can raise questions about the credibility of science similar to the way these questions are asked with regard to third-party financing of research. Pursuing it blindly risks entering into a Faustian bargain expedited with privatized corporate data, which may place scientific endeavors under great restrictions, and, in the end, may replace scientific fact with corporate and government fictions and undermine the creditability of science [49].

2.3 Reflection

eGovernment was spurned by the need to regain public trust in government. Much of the effort however has gone into electronically connecting different parts of government to improve efficiency and effectiveness (G2G). To reclaim public trust eGovernment provides services to citizens (G2C) and the business (private) sector (G2B) (see table 2). Schematically, eGovernment = G2G + G2C + G2B.

In principle, eGovernment is also offering citizens an opportunity (platform) to voice their issues and complaints (grievances). Feedback mechanisms from both the public and private sector fall under eGrievance systems, which we represent schematically as eGrievance = G2C + G2B. eGrievance systems enable societal actors to voice their concerns. Some of them were designed years ago from a top-down perspective, therefore we label them G2C. More recent ones, adopting Web 2.0 approach and tools, can be labelled C2G because the initiative comes from users; we introduce an example later. Citizens are in general responsive to questions that governments ask about policies or societal issues. eGrievance also facilitates feedback mechanisms that redress complaints on the malfunctioning of a pre-defined set of services.

On the other hand, when citizens seize initiative and confront government with issues, it is not commonly done through e-channels. Social networks and mass media play a role in collecting grievances and pooling them. Particularly, the media play an important role in raising public attention to grievances. Media visibility is essential for grievances to reach government. But currently more and more social issues are pooled through electronic social networks and brought to the attention of international agencies. Interest groups and (multinational) NGOs are also using these same social networks to push or pull at the relevant issues for their own agenda setting.

Table 2. Key features of information flows, adapted from Craglia et al. [47]

	Lead Actors	Key Drivers	Main Target Audience	Implementation mechanism
eGovernment	Public sector	Public trust	Citizens + private sector	Services to citizens
Virtual globes	Private sector	Market share & Advertising Revenue	Mass market	Market + voluntary
VGI	Citizens	Social networking	Citizens	Voluntary

3 Surveillance Power from the State to the Citizens?

Traditionally, bureaucracy has the role of bridging the gap between the formal political sphere and citizens. Its main legitimation lays in the aim of rationalizing society by channelling social relations in formal procedures that are based on formal rationality rather than value rationality. Ideally, it guarantees equal and universal access to public administration and downplays the role of tradition and charismatic figures. Weber (in "The Protestant Sects and the Spirit of Capitalism" 1920) expresses his concerns about the bureaucratization of society with his famous metaphor of the "iron cage". The last century showed that such a modernization path is not necessary, as different rationalities continue to exist and proliferate, Foucault being an exemplar author on this line.

Indeed, the universal institutionalization of formal rationality is not likely to happen any time soon. Information systems such as those being discussed here -based on perceived needs and wants that may sideline bureaucracy- do not seem to bring us towards an iron cage. Rather, mutual visibility and continuous negotiation appear as the way ahead for citizens and decision makers. Hoogenboom and Ossewaarde [70] argue that such a relation between state and citizens was legitimized by a 'legal-rational authority' which cannot be taken for granted in 'late modernity', characterized by different and competing rationalities. Late modernity sees the rise of reflexive organizations that are more dependent on their actual environments. "Reflexive organizations further democratization because they force a bureaucratic elite to take the personal and social needs of the lay people seriously and they force them to communicate openly" [70]. On the other hand, these kind of organizations risk being less universalistic, and more affected by individual qualities. With this framework in mind, we will introduce two examples of eGovernment efforts that are in line with the idea of reflexive authority.

Citizen empowerment through eGovernment would entail the inversion of the grievance system ($eGrievance^{-1}$). Such a bottom up approach depends on citizens or the private sector taking initiative and finding a platform to confront government with their grievance ($eGrievance^{-1}$ = C2G + B2G). Few examples exist of such inverted systems and there are several consequences to take into account if such a system is to work.

Traditional eGovernment and eGrievance structures in particular can be represented with a classic top down scheme where information travels down and up between policy makers and citizens through the bureaucratic filter of public administration (figure 1). With the constitution of a more visible and vocal citizenship,

where information exchange between citizens is growing increasingly through accessible and easy to use applications, the individuality of citizen grievance can be pooled through platforms by themes and preferably also location. International agencies set these themes as well, concerning wide issues ranging from water and sanitation, to women's emancipation and health. On the one hand International agencies follow MDG's to set their agendas, on the other hand they can follow citizen inputs [58].

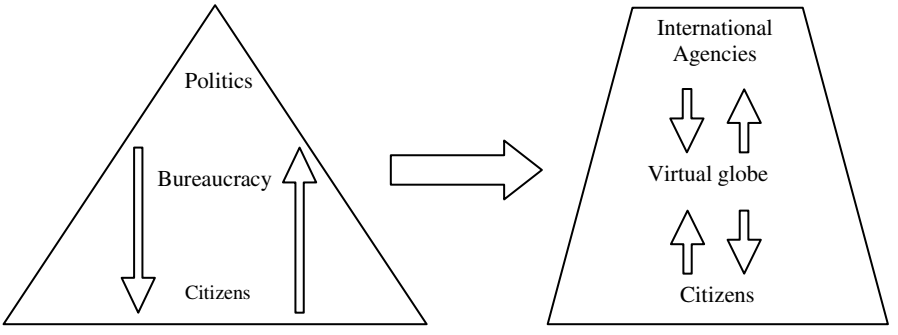


Fig. 1. An emerging setting for eGovernment, from traditional to a setting with geoICT acting as an intermediary

This emerging setting fits well with the concept of eParticipation. eParticipation uses ICT as a utility to get citizens more involved in improving the public service, public administration and social cohesion. More and more links are made between governments and citizen communities. Poelmans and Van der Linde [50] differentiate three forms of eParticipation:

1. *Political participation*. How to involve citizens in the decision-making process?
2. *Policy participation*. Citizens and governments cooperate together at the implementation and maintenance of policy.
3. *Social participation*. How to reinforce the mutual involvement of citizens?

On the traditional (left) side of figure 1 these three forms of participation are dependent on the bureaucratic ability to govern information flows. Particularly social participation depends on the agility and transparency of that bureaucracy. If the bureaucracy is not equipped to captivate citizens, eParticipation will lose its momentum and its effect. Even if bureaucracy is functioning optimally it can act as a filter to both sides of the system. Probably not a deliberate filter, but the eGovernment system is not equipped to organize all citizen demands into policy input, nor can it give enough transparency to policy objectives.

Moving to eParticipation with a wider perspective, citizen interests and international agendas become interdependent drivers for political and social participation. The relative ease of providing location information with complaints through embedded GPS devices offers interesting opportunities for organising information spatially through virtual globes. Virtual globes are places where citizens and the private sector

gather to provide and acquire geo-located knowledge, experiences and information about services. The specific nature of information provided on virtual globes is the spatial information attached to all available data. Combining data sources provides possibilities for discovering business opportunities or enabling the identification of hotspots [51, 52] for all sorts of purposes.

Visualization of localized themes of grievances could provide citizens and policy-makers with a different view into objectives and demands.

3.1 An eGrievance System in India

The implementation of the eGrievance system in Kalyan-Dombivili (India) was triggered and framed under the pro-poor policies and reforms in urban areas required by the Jawaharlal Nehru National Urban Renewal Mission Programme (JNNURM), which mandates the implementation of ICT and eGovernment tools. In Kalyan-Dombivili this is listed in the approved City Development Plan as the "introduction of a system of e-governance" [53]. One of the components is a module called "Complaints and Redressal System". The program was initiated by the Kalyan Dombivili Municipal Corporation (KDMC) in 1999 and implemented in 2002 [54]. The objective was to create "a system driven by Municipal Corporation with highest levels of transparency, accountability and citizen servicing standards." The benefits claimed for the citizens were: time bound service delivery, transparency and accountability in the corporation's functioning; hassle free interactions with quicker response time for all the services; objectivity in decision making, leading to more impartial and transparent governance.

Both the public and private sector participate in the development and implementation of the programme. This includes the Indian Institute of Technology, National Centre for Science and Technology and TATA Institute of Fundamental Research, VJTI (engineering college in Mumbai) and Mumbai based ABM Knowledgeware Ltd [54].

Citizens can formally submit grievances through a complaint handling mechanism that offers several access points. The procedure can be initiated via the Internet, via the phone but also via a group of public offices called "citizen facilitation centres" (CFCs). An analysis of the mode of delivery of the complaints in 2007 showed that more than 90% of all complaints in KDMC are delivered by hand, only 6% are submitted online and a negligible proportion by phone [25]. The eGrievance system allows the formal filing of complaints and captures from bottom-up the grievances of the citizens. However, when it comes to specifying the sort of grievance, the citizen is limited to a top-down pre-defined list of possible categories or to the interpretation of the phone operator who finally codifies the complaint. The eGrievance system is designed to direct the complaint to the department responsible for the solution of the complaint. In principle citizens are able to trace the complaint.

Some typical categories in the eGrievance refer to needs that -if not satisfied- might affect the quality-of-life of the most deprived (e.g. no water supply) but others just reflect the "wants" and discontent of some citizens (the better off, as data shows) with what they perceive as urban blight (e.g. encroachments, slums, hawkers, beggars). Research on the composition and spatial distribution of complaints showed that the eGrievance system favors citizen participation only of a particular citizen group, the

middle class [25]. A visual comparison of maps showing the concentration of complaints and the different levels of multiple deprivation (Figure 2) indicates that the complaints do not necessarily concentrate in the most deprived areas. These maps were also shown to city officials, politicians and self-help groups from poorer areas. From this it was also found that no one felt that the concentration of complaints accurately reflected the areas in the city with the greatest need for water and drainage improvements.

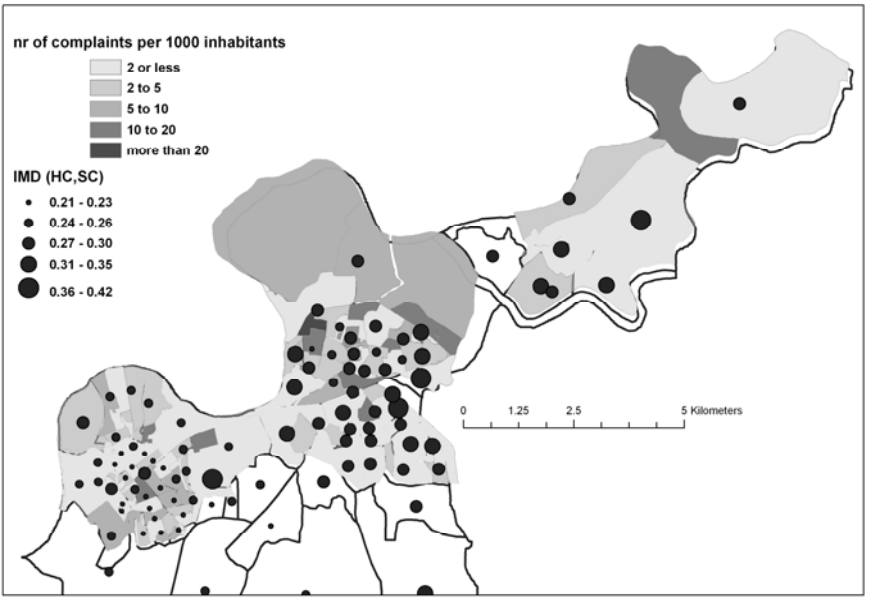


Fig. 2. Overlay of complaints (grays) and Index of Multiple Deprivation (IMD) (symbols). Note: High values in IMD indicate a high multiple deprivation index [25].

The system is biased towards the middle class agenda. In terms of its capacity for "problem acknowledgement and agenda setting" the system captures the wants (of the better-off) rather than the needs of all the citizens and in particular those who are worst-off.

Some of the usual potentials of eGovernment are being claimed for KDMC's eGrievance system. Despite receiving several awards and being replicated in other municipalities, an analysis of local newspapers reinforce the limitations. The system does not necessarily speed up the resolution of complaints. Some people still prefer to have face-to-face interaction when placing a complaint or they are not aware of the existence of the system [55, 56].

3.2 A Human Sensor Web in Zanzibar

In Tanzania, UN-Habitat and Google.org, the philanthropic arm of Google.com, entered a partnership in 2009 aiming at improving water services offered by the Zanzibar Water Authority. The project aims at improving access to information on

water coverage, assessing the level of satisfaction by citizens and evaluating efficiency in the delivery of services by the water authority. The complaint handling mechanism and platform is still in the research phase, being administered by different researchers [57], but is operational to the extent that local actors can manage the system. The only external facilitator envisioned for the system is Google, which provides the technical infrastructure and hosts the web-based system.

The initiative, at its initial prototyping and testing stages, is experimenting with the use of mobile phone networks to report deficiencies in water supply and to track efficiency in maintenance response through a web-based information system. It is a novel approach in which citizen generated information is provided to decision and policy makers (possibly in a focused, timely, and effective manner). Information received from cell phones is stored on servers and linked to a virtual globe for public visualization on the internet. The novelty is the accountability possibly achieved through publicly available, aggregated information on the status of, and relative performance in, water services provision. The project aims to deliver essential information 'up the pipe' directly from consumer to provider and decision maker through the use of standard mobile devices, and 'down the pipe' to the consumer and to society in the form of community groups, political representatives and the media [33].

The Human Sensor Web (HSW) is a combination of a community of individuals who report observations through existing, widespread mobile communication technology and a set of (web) services that provide means to disseminate observations made by the community and means to receive feedback from individuals, specific user groups and civil society. Citizens use their mobile phones to report about a malfunction. These reports are received by the (public) service provider and simultaneously visualized in a virtual globe environment. Not only the service provider responsible for fixing the malfunction can see these reports but all interested parties - citizens and the state - can access the spatial representation of grievances online and observe the quality of services (malfunctions and also speed of repair) [72].

Mobile phones are becoming the most widespread sensor device in the world offering the possibility of capturing voice, pictures, video and location data in combination with a versatile interface that connects to global communication networks.[2] Goodchild [41] has proposed using "human sensors" and web2.0 to unlock the vast pool of local spatial knowledge as Volunteered Geographic Information (VGI). The emerging framework in figure 3 is particularly appealing for this idea. Virtual globes offer a wide variety of ways to include VGI as is shown by the Amazonian example from Google Earth Outreach [58]. Several other examples of eGrievance systems exist which could easily be used or adapted to use the concept of VGI in the emerging framework.

Success of the HSW depends to an extent on the accessibility of mobile telecommunications. The availability of the technology is an important issue [59] but accessibility, as in ownership of mobile phones, can also manifest itself as a shortcoming in

[2] Mobile phone users are mostly "equal" to the point that there is just a financial obstacle that denies its ownership or use. Phone ownership for instance can be limited to certain societal classes (wealthy businessmen) in its early adoption. In some societies however this is not so straight forward. Certainly in traditional societies in lesser developed countries there are cultural factors that govern the use and ownership of mobile phones.

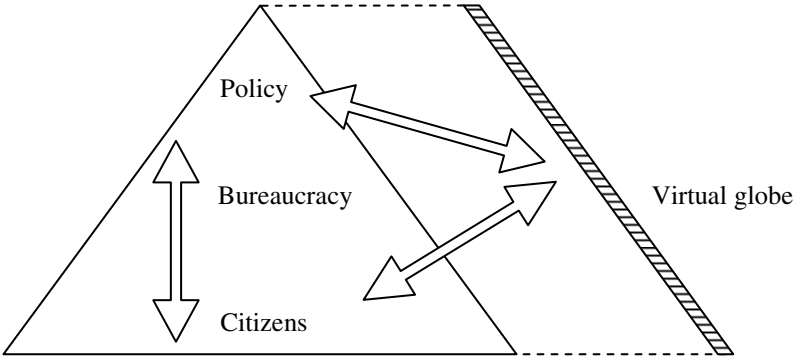


Fig. 3. Virtual globe as a mirror for citizen surveillance of the state

representation. According to Sung [60] gender issues play a role in this case on Zanzibar. In many rural areas it is men who have phones but women who have grievances to report because they are usually in charge of collecting water. This issue causes delays in responses and makes information transmitted by a third party less reliable. To what extent this HSW project therefore reflects wants, needs or rights and whether it also favours the middle class, or any specific part of society is not yet known.

4 Discussion and Conclusions

VGI can be dubbed "participatory sensing" given the nature of geo-data generation by dispersed volunteers, where the voluntary aspect and the personal interest and motivation to contribute information are central. The cases presented show how volunteered geographic information (VGI) can become a relevant aspect of an eGrievance^{-1} system [65]. VGI is usually generated to inform other citizens and is not by itself specifically purposeful. VGI can be none other than blogged references to great places to visit. But it might as well be geo-tagged pictures of illegal activities (deforestation, waste dumps etc.) directly submitted to authorities [58]. As argued by Craglia et al. [47], platforms like Google Maps and Google Earth are combining both voluntary and institutional data. Without a mechanism to clearly distinguish the different nature of the data (through metadata), it will be difficult for citizens to take action and for administrators and policy makers to make accountable decisions on the basis of such data. If citizens are to be engaged or involved more in government decisions by sharing their knowledge (data, information and understanding) it should be done in a manner that maintains accessibility but also improves reliability and backs trust. It is of course not only trust in the platform and whether that platform displays the "truth" [46]. Governance innovations are required for VGI to be put to good use and citizens must be trusted to provide the right information reciprocally.

Rather than going into the details of systems that are under continuous development, we stress how our cases aim at affecting service provision activities by managing stakeholders' mutual and external visibility differently. Indeed, the eGrievance systems and the early steps of the human sensor web that we presented show the

emergence of a different framework for eGovernment (figure 1). With respect to eGrievance, the Human Sensor Web example (or eGrievance^{-1}) positions the interactions it mediates and data hereby produced, outside of the conventional bureaucratic procedures that eGrievance systems are designed upon. With this the old idea of control [66] is possibly reverted, or becoming exploitable by the controlled.

By becoming a side addition to the existing tools like eGrievance, human sensed data on virtual globes act as a mirror through which policy-makers and citizens become more visible to each other. Accountability lines are therefore affected. Bureaucracy is likely to keep filtering citizen pressure, and the same citizens are likely to find workarounds to affect agenda setting. The virtual globe as a mirror (figure 3) acts on the well known mechanism of showing and blaming: facilitating the public visualization of public interest issues like service provision, they leverage public opinion in a less ad-hoc fashion than mass media. It is quite likely that corporations or groups of citizens will be able to exploit the virtual globe to "sell" their point of view or product to a potentially broader audience. On the other hand, citizens become more visible to the state. The mediating role of the private sector is expected to focus itself on the transparent development and management of such platforms.

The expansion to live satellite feeds in the near future for instance will have dramatic consequences for the identification, tracking and sorting of individuals. With CCTV the controlling power of surveillance is in few hands, while massive surveillance with live satellite feeds is available to everybody [62]. So, we sketch some concerns and possible risks related to development of VGI towards unintended uses of user generated data. This concept is mentioned by Lane et al. [63] who also describe "opportunistic sensing". Opportunistic means in this case not volunteered information but automated extraction from possibly the same sensors (mobile phones) as used for VGI. The earlier examples of Swine flu and traffic hotspots [51, 52, 64] are typical examples of opportunistic sensing but one can also continue this line of thinking to include Google's analysis of search engine data [67]. This type of sensing is bothersome as it does not require consent from the "sensor owner" to access or use the data. In the light of the control discussion this gives an important dimension to consider.

Nevertheless, when vested interests are at play, concerns over private corporations owning a virtual globe give reason to debate, even concern. Entrusting a mediating role between citizens and public authorities to the private sector opens important discussions about free speech and media. Potential for using a virtual globe to access and disseminate spatial information have been presented. On the other hand, virtual globes have become very popular, and more voices stress the disadvantages or risks of leaving them to commercial partners. Parks [46], Kingsbury and Jones [44] and Harvey [48] critically analyze the risks that corporate ownership of these platforms in most cases also means corporate ownership or copyright of the information disseminated through these platforms. These issues have been voiced earlier about the handling of spatial information in general [61].

So, what is happening to the 'iron cage' of formal rationality that Weber envisioned one century ago? By becoming more allowed to see the state, citizens may engage in negotiations with public administrations that may lead to more alertness and accountability, but also to unequal responsiveness from public administrations. In such a context, we see the possibility for "reflexive authority, which can be defined as the belief in the ability of institutions and actors to negotiate, reconcile and represent

arguments, interests, identities and abilities." [70] For now, as it goes beyond the scope of this paper, we leave it open for discussion if state visibility mediated by geoICT goes more in the direction of the reflexive modernity proposed by Ulrich Beck and Anthony Giddens, or if it substantiates the postmodern paradigm.

Acknowledgement. The authors wish to recognize the following organizations for the financial support they provide for the ongoing research projects on which this paper is partly based. The "eGrievance system in India" is supported by the NWO-Wotro Integrated Programme: using spatial information infrastructure in urban governance networks: reducing urban deprivations in Indian cities? The "Human Sensor Web on Zanzibar" is supported by UN-Habitat and Google.org under the h2.0 Monitoring Services to Inform and Empower initiative.

References

1. Danzinger, J.N., Andersen, V.K.: The impacts of information technology on public administration: an analysis of empirical research from the 'golden age' of transformation. International Journal of Public Administration 25(5), 591–627 (2002)
2. Zouridis, S., Thaens, M.: Reflections on the Anatomy of E-Government. In: Bekkers, V.H.V. (ed.) The Information Ecology of E-Government. E-Government as Institutional and Technological Innovation in Public Administration, pp. 21–36. IOS Press, Amsterdam (2005)
3. Heeks, R.: eGovernment in Africa: Promise and Practice. Information Polity 7(2-3), 97–114 (2003)
4. Saxena, K.: Towards excellence in e-governance. International Journal of Public Sector Management 18(6), 498–513 (2005)
5. Fang, Z.: E-government in digital era: concept, practice, and development. International Journal of The Computer. The Internet and Management 10(2), 1–22 (2002)
6. Criado, J., Hughes, O., et al.: e-Government and Managerialism: A Second Revolution in Public Management. In: 6th International Research Symposium on Public Management University of Edinburgh, April 8-10 (2002)
7. Verdegem, P., Verleye, G.: User-centered E-Government in practice: A comprehensive model for measuring user satisfaction. Government Information Quarterly 26(3), 487–497 (2009)
8. Ho, A.T.K.: Reinventing local governments and the e-government initiative. Public Administration Review 62, 434–444 (2002)
9. Van Deursen, A., Pieterson, W.: The Internet as a Service Channel in the Public Sector. In: Proceedings of the ICA Conference, Dresden, Germany (2006)
10. Thomas, J., Streib, G.: The new face of government: Citizen-initiated contacts in the era of e-government. Journal of Public Administration Research and Theory 13(1), 83–101 (2003)
11. Horrigan, J.: How Americans get in touch with government. Pew Internet & American Life Project: 9 (2004)
12. Reddick, C.G.: Citizen interaction with e-government: From the streets to servers? Government Information Quarterly 22(1), 38–57 (2005)
13. McNeal, R., Hale, K., Dotterweich, L.: Citizen-Government Interaction and the Internet: Expectations and Accomplishments in Contact, Quality and Trust. Journal of Information Technology and Politics 5(2), 213–229 (2008)

14. Chen, D., Huang, T., et al.: Citizen Participation, E-government, and Public Management: A Case of Taipei City Mayor's E-mail Box International Symposium of Digital Divide and Digital Opportunity, pp. 157–176. Yuan Ze University, Taiwan (2004), http://www.infosoc.yzu.edu.tw/conference/paper/6_02Public%20Participation%20E-government%20and%20KM_draft_.pdf (accessed in June 2010)
15. OECD: The e-Government Imperative. OECD. Paris (2003)
16. Moon, M.: The evolution of e-government among municipalities: rhetoric or reality? Public Administration Review 62(4), 424–433 (2002)
17. Edmiston, K.: State and local e-government: Prospects and challenges. The American Review of Public Administration 33(1), 20–45 (2003)
18. Gil-Garcia, J., Martinez-Moyano, I.: Understanding the evolution of e-government: The influence of systems of rules on public sector dynamics. Government Information Quarterly 24(2), 266–290 (2007)
19. Kumar, V., Mukerji, B., et al.: Factors for successful e-government adoption: a conceptual framework. The Electronic Journal of e-Government 5(1), 63–76 (2007)
20. Cohen, J.: Citizen satisfaction with contacting government on the internet. Information Policy 11(1), 51–65 (2006)
21. Pieterson, W., van Dijk, J.: Channel Choice Determinants; An exploration of the factors that determine the choice of a service channel in citizen initiated contacts. In: Proceedings of the 8th Annual International Conference on Digital Government Research: Bridging Disciplines & Domains, pp. 173–182. Digital Government Society of North America, Philadelphia (2007)
22. Sharp, E.B.: Citizen-Demand Making in the Urban Context. American Journal of Political Science 28(4), 654–670 (1984)
23. Parigi, V.K., Geeta, P., Kailasam, R.: Ushering in Transparency for Good Governance. Working Paper, Centre for Good Governance, Hyderabad (2005)
24. Ranganathan, M.: Grievance Redressal Processes in Urban Service Delivery: How Effective Are They? ADB The Governance Brief, Capacity Development and Governance Division, Regional and Sustainable Development Department, Issue 17 (2008)
25. Martínez, J.A., Pfeffer, K.H., van Dijk, T.: The capacity of e-government tools: claimed potentials, unnamed limitations. In: Proceeding of the 10th N-AERUS Conference: Challenges to Open Cities in Africa, Asia, Latin America and the Middle East: Shared Spaces within and Beyond, IHS Rotterdam, October 1-3 (2009)
26. Brewer, B.: Delivering Better Service to Citizens- Addressing Citizens Complaints Effectively: What? How? Why? In: The CAPAM 2006 Biennial Conference Rising to the Challenge: Enhancing Public Sector Capability Sydney, Australia (2006)
27. Mulgan, R.: Comparing accountability in the public and private sectors. Australian Journal of Public Administration 59(1), 87–97 (2000)
28. Brewer, B.: Citizen or customer? Complaints handling in the public sector. International Review of Administrative Sciences 73(4), 549–556 (2007)
29. UNDP: The key to increasing Transparency in e-Government deployements. Public Feedback Mechanism. APDIP e-Note 3/2005 UNDP (2005)
30. Hance, L.: (How) Are You Being Served? A Good Practice Guide on Complaints Handling in Housing Association. Housing Corporation. Tottenham (2002), http://www.housingcorp.gov.uk/upload/pdf/SERVED.pdf (accessed in June 2010)
31. Seneviratne, M., Cracknell, S.: Consumer Complaints in Public Sector Services. Public Administration 66(2), 181–193 (1988)

32. Wallack, J., Nadhamuni, S.: User Innovation and eGovernance Design. In: Forthcoming in Hidden Successes: Urban Reforms in India. MIT Press, Cambridge (2007)
33. UN-Habitat: h2.0 Monitoring Services to Inform and Empower (2009), http://www.unhabitat.org/categories.asp?catid=635 (accessed January 22, 2010)
34. Bourn, J.: Citizen Redress: What citizens can do if things go wrong with public services. National Audit Office (NOA), London (2005)
35. Carvalho, D., Fidélis, T.: Environmental complaints in Aveiro, Portugal: actors, concerns, territorial pattern, and resolutions. Sociedade & Natureza (Online) 21, 51–70 (2009a)
36. Carvalho, D., Fidélis, T.: The perception of environmental quality in Aveiro, Portugal: a study of complaints on environmental issues submitted to the City Council. Local Environment 14(10), 939–961 (2009b)
37. Meijer, A., Burger, N., et al.: Citizens4Citizens: Mapping Participatory Practices on the Internet. Electronic Journal of e-Government 7(1), 99–112 (2009)
38. Schumaker, P.D., Getter, R.W.: Responsiveness Bias in 51 American Communities. American Journal of Political Science 21(2), 247–281 (1977)
39. Van Dijk, J., Hacker, K.: The digital divide as a complex and dynamic phenomenon. The Information Society 19(4), 315–326 (2003)
40. Fountain, J.: Paradoxes of public sector customer service. Governance 14(1), 55–73 (2001)
41. Goodchild, M.F.: Editorial: Citizens as Voluntary Sensors: Spatial Data Infrastructure in the World of Web 2.0. International Journal of Spatial Data Infrastructures Research 2, 24–32 (2007)
42. Sheppard, S.R.J., Cizek, P.: The ethics of Google Earth: Crossing thresholds from spatial data to landscape visualisation. Journal of Environmental Management 90(6), 2102–2117 (2009)
43. Livingston, S., Aday, S.: NGOs as Intelligence Agencies: The Empowerment of Transnational Advocacy Networks and the Media by Commercial Remote Sensing. Paper Presented at the Annual Meeting of the Association of American Geographers, San Francisco, April 17-21 (2007)
44. Kingsbury, P., Jones III, J.P.: Walter Benjamin's Dionysian Adventures on Google Earth. Geoforum 40, 502–513 (2009)
45. Dodge, M., Perkins, C.: Reclaiming the Map: British Geography and Ambivalent Cartographic Practice. Environment and Planning A 40(6), 1271–1276 (2008)
46. Parks, L.: Digging into Google Earth: An analysis of "Crisis in Darfur". Geoforum 40, 535–545 (2009)
47. Craglia, M., et al.: Next-Generation Digital Earth. International Journal of Spatial Data Infrastructures Research 3, 146–167 (2008)
48. Harvey, F.: Just another private - public partnership? Possible constraints on scientific information in virtual map browsers. Environment and Planning B: Planning and Design 2007 34, 761–764 (2007)
49. Perkins, C., Dodge, M.: Satellite Imagery and the Spectacle of Secret Spaces. Geoforum 40(4), 546–560 (2009)
50. Poelmans, M., Van der Linde, X.: The e-Citizen Charter as a Tool for Measuring Citizen Satisfaction on the Basis of Life Events. In: Cunningham, P., Cunningham, M. (eds.) eChallenges e-2009 Conference Proceedings, IIMC International Information Management Corporation (2009)
51. Thorp, J., Just Landed: Processing, Twitter, MetaCarta & Hidden Data (2009), http://blog.blprnt.com/blog/blprnt/just-landed-processing-twitter-metacarta-hidden-data (accessed on January 22, 2010)

52. McNeil Jr., D.G.: Predicting Flu With the Aid of (George) Washington. Article Published in the New York Times, May 4, page A1 (2009)
53. Kalyan Dombivli Municipal Corporation: City Development Plan for Kalyan Dombivli Municipal Corporation. Kalyan Dombivli Municipal Corporation, Kalyan Dombivli (2006)
54. ABM: Project KDMC (2009), http://www.abmindia.com/kdmc.html
55. Dolare, S.: MSEDC upsets Old Kalyan consumers Dombivali Kalyan Plus, Saturday (September 29, 2007)
56. Sharma, S.: KDMC's e-governance misleading, complains Kalyan resident Dombivali Kalyan Plus, Saturday (June 7, 2008)
57. Jürrens, E.H., Bröring, A., et al.: A Human Sensor Web for Water Availability Monitoring. In: OneSpace 2009 - 2nd International Workshop on Blending Physical and Digital Spaces on the Internet, Berlin, Germany (2009)
58. Google Earth Outreach: Trading bows and arrows for laptops (2008), http://www.youtube.com/watch?v=tNp9j1O3CKk (accessed on January 22, 2010)
59. Howard, P.N., Mazaheri, N.: Telecommunications Reform, Internet Use and Mobile Phone Adoption in the Developing World. World Development 37(7), 1159–1169 (2009)
60. Sung, C.Y.: Understanding of data quality in human sensor web. University of Twente, Enschede (2010)
61. Wegener, M., Masser, I.: Brave new GIS worlds. In: Masser, I., Campbell, H., Craglia, M. (eds.) GIS Diffusion: The Adoption and Use of Geographical Information Systems in Local Government in Europe. Taylor & Francis, London (1996)
62. Albrechtslund, A.: In the Eyes of the Beholder: Introducing participation and ethics to surveillance. Aalborg University, Aalborg (2008)
63. Lane, N.D., Eisenman, S.B., Miluzzo, E., Musolesi, M., Campbell, A.T.: Urban Sensing: Opportunistic or Participatory? In: ACM SenSys 2007, Sydney, Australia (2007)
64. Tomtom: How TomTom's HD Traffic™ and IQ Routes™ data provides the very best routing; Travel Time Measurements using GSM and GPS Probe Data. Whitepaper (2009), http://www.tomtom.com/lib/doc/download/HDT_White_Paper.pdf (accessed on January 22, 2010)
65. Coleman, D.J., Georgiadou, Y., Labonte, J.: Volunteered geographic information: the nature and motivation of producers. International Journal of Spatial Data Infrastructures Research 4, 332–358 (2009)
66. Mansell, R.: The information society and ICT policy; A critique of the mainstream vision and an alternative research framework. Journal of Information, Communication & Ethics in Society 8(1), 22–41 (2010)
67. Ginsberg, J., Mohebbi, M.H., Patel, R.S., Brammer, L., Smolinski, M.S., Brilliant, L.: Detecting influenza epidemics using search engine query data. Nature 457, 1012–1014 (2009)
68. Avgerou, C.: Information Systems and Global Diversity. Oxford University Press, Oxford (2002)
69. Bruns, A.: Blogs, Wikipedia, Second Life, and Beyond: From Production to Produsage. In: Digital Formations, vol. 45. Peter Lang, New York (2008)
70. Hoogenboom, M., Ossewaarde, R.: From Iron Cage to Pigeon House: The Birth of Reflexive Authority. Organization Studies 26(4), 601–619 (2005)
71. Beck, U.: Risk Society, Towards a New Modernity. Sage Publications, London (1992)
72. H2.0 – Human Sensor Web – Client (2010), http://geoserver.itc.nl/zanzibar/ (accessed on May 15, 2010)

Privacy Enhanced Fraud Resistant Road Pricing
(Extended Abstract)

Jaap-Henk Hoepman[1,2] and George Huitema[1,3]

[1] TNO Information and Communication Technology, Eemsgolaan 3,
9701 BK, Groningen, The Netherlands
[2] Institute for Computing and Information Sciences,
Radboud University Nijmegen, Nijmegen, The Netherlands
[3] Faculty of Economics and Business,
University of Groningen, The Netherlands
jaap-henk.hoepman@tno.nl, jhh@cs.ru.nl, george.huitema@tno.nl,
g.b.huitema@rug.nl

Abstract. A naive implementation of a road pricing system will collect an enormous amount of personal location data. In this paper we present a sophisticated system that is privacy friendly, i.e. where the invoices contain aggregated pricing information and where only the driver has insight into all the underlying details. Enforcement based on spot checking is used to keep drivers honest, and to make the system fraud resistant. These spot checks are integrated in the system in a novel way that does not impair the privacy of the overall system, as is the case in systems previously proposed. Our solution can easily be applied to other privacy sensitive contexts such as smart metering and e-ticketing in public transport.

Keywords: Privacy, Road Pricing, Accountability, Security.

1 Introduction

For many years, many European governments have been discussing the introduction of some type of road pricing in order to reduce both the number of kilometres driven (thereby avoiding traffic jams and congestion), as well as carbon emissions. Road pricing can be achieved in many different ways depending on the size of the area covered and the level of road usage details that need to be collected. Here we focus on the full mode case where a nationwide scheme is applied and detailed road usage details, such as precise locations and time of day, are registered by means of a navigation satellite system together with a tracking device in the car, also called an On Board Unit (OBU). As an example, in the last category the Dutch government recently proposed an overall kilometre charging system for drivers as a replacement for the current road tax. This announcement by the Dutch authorities stirred a large public debate that still continues and mainly focuses on the costs for driving and privacy. This case inspired us to come up with an improved privacy friendly road pricing system.

In the full mode case where detailed usage information has to be gathered in order to compose a correct invoice for vehicle owners, there seems to be a conflict between

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 202–213, 2010.

privacy friendliness on the one hand (not everybody should have access to all the details) and on the other, the necessity of enforcement where details are necessary to combat fraud. In this paper we present a balanced solution that is both privacy friendly and fraud resistant. The first is assured by distributing the necessary information over all the parties involved in the process of road pricing, so that no party can combine personal data with location data, while fraud is avoided by integrating random spot checks in a novel way.

The rest of this paper is organised as follows. In Section 2, we describe the assumptions and the requirements that will form the basics of our proposed road pricing system. In Section 3 related work is explained. The design principles we use are listed in Section 4 followed by Section 5 describing the architecture of the proposed system. In Section 6 the level of security and privacy of the proposed solution is analysed, followed by Section 7 concluding the paper together with some issues for further research.

2 Assumptions and Requirements

We make the following assumptions for our proposed road pricing system. *Business parties*: besides vehicle owners and vehicle drivers, business parties related to the back office processes - aggregation and pricing of usage details – will also be present. *Personal responsibility*: drivers will be held personally responsible for the generation of correct road usage details. *Enforcement*: an enforcement party tries to detect fraud and malfunctioning by spot checking. The spot checks will be secret, but not for long (cf. [9]). *Pricing function*: the so-called pricing function that assigns the charge for the distance driven is linear in its argument, (cf. [11]). *OBU setup*: the OBU will be 'thin', a relatively simple device that does not need to store complex maps. It will submit its registered location data in near real time to related road pricing parties. The OBU is not required to be a trusted element.

Furthermore we set the following requirements. *Correctness*: the road pricing system generates invoices for vehicles based on actual road usage. *Privacy friendliness*: only the driver has access to the detailed road usage information. Other business parties only see partial or aggregated information that does not reveal the full picture. *Fraud resistance*: enforcement will apply checks at random spots and time frames to ensure that correct usage details have been generated at the OBU.

3 Related Work

Road pricing systems are an example of the use of smart vehicle technology [8] with potential privacy ramifications [7]. Several proposals for cryptographic protocols based on generic secure multi-party computations have been proposed [3, 13]. According to Popa [12] these systems run several orders of magnitude slower than necessary, and scale poorly with increasing number of users. Therefore they propose a simpler scheme, where *thin* OBUs submit their location, labelled with a pseudonymous tag, to a server at regular time intervals. Using a zero-knowledge protocol, the vehicle owner collects the charges corresponding to their vehicle, and proves to the

server they collected the right ones. They also propose an enforcement protocol by random and secret spot checks. All vehicles spotted are reported to the server, and the enforcement essentially requires all spotted vehicles to prove that they submitted a record for the spot check location. This presents a privacy leak though: the protocol allows a server to query a vehicle whether it was present at a certain place at a certain time while the vehicle has no way to determine the validity of this query. The same privacy leak is present in the work of de Jonge and Jacobs [9] (see also [6]) and the PrETP system [2]. In these solutions a *thick* OBU is capable of computing the road charges based on repeated sampling of its current location. Vehicles have to commit to the trips they made during a day. Each recorded vehicle is asked by a server to reveal the pre-image of the committed hash value corresponding to the spot check location. If a vehicle cannot comply, this indicates a possible case of fraud. Again, a vehicle has no way to verify the validity of the server request.

Related to this are systems for pay-as-you-drive insurance, for example, the Pri-PAYD system [15]. In this system privacy is protected because the OBU in the vehicle locally computes the aggregated insurance premium based on sampled GPS locations. The OBU needs to be trusted and tamper proof though to ensure correct computation of the premium and to prevent fraud by users.

In summary, current proposals for a full-mode road pricing system do not fully guarantee privacy and accountability while relying on a thin, untrusted, OBU only.

4 Design Principles for Achieving Privacy in Road Pricing

In our proposal, privacy is achieved using the following two design principles. First of all, we use a novel way of splitting up *trips* (the trajectory followed by a car from its place of departure to its destination) into short segments, so-called *legs*, that are not linkable to each other. Secondly, the different process steps needed to determine the overall road charge are distributed over several system components. This way, no single component has enough information to reconstruct a particular route travelled.

4.1 Trips and Legs

Since a pricing function is assumed to be linear, trips can be split into shorter legs, and the charge for the trip equals the sum of the charges for the legs (cf. [11]). Therefore if we ensure that legs are not linkable (it cannot be determined whether two legs are part of the same trip), this approach is a first step to achieving privacy.

Traditionally, road pricing systems charge for the distance travelled on a particular road. The problem with this approach is that when splitting a trip into legs, one needs to make the last location in the previous leg equal to the location in the next leg, in order not to lose information needed to compute the charge. In order to keep legs non-linkable then, locations (and their associated visiting times) need to be rounded rather coarsely, and even then the same combination of location and time will not occur that often.

To overcome this problem we propose to charge for road use slightly differently.; namely, to charge for travelling in a certain area instead. To this end, the ground surface is divided into cells (for instance using a so called Voronoi diagram [1], but other

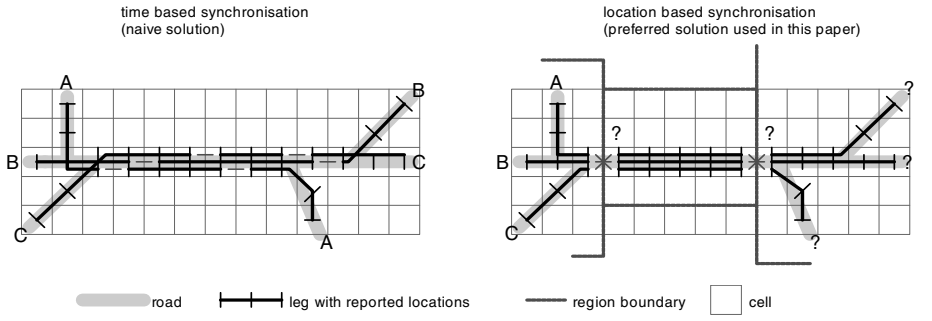


Fig. 1. Dividing a trip of a vehicle into legs can be done time-based (left) or location-based (right)

methods can also be used). The location of a vehicle is recorded as the 'centre' point of such a cell. In urban areas these cells may be small, to differentiate ring roads, congested roads, etc. A trip then, is defined as a sequence of *different* but consecutive cells (together with the time the cell is entered). A leg consists of a subsequence of this sequence, and the pricing function assigns a charge to each cell (depending on the time the cell was visited). With this setup, the first cell in a leg does not have to equal the last cell in the previous leg.

By splitting trips in short non-linkable legs, the point of entry of a particular car that enters a busy highway cannot be linked to its point of exit[1]. However, the effectiveness of this 'hiding in the crowd' depends on the way trips are subdivided in legs (see Fig. 1). Synchronisation on time, i.e., starting a leg at globally predefined times, is not a good idea. In such a setup the last location of the previous leg is correlated with the first location of the next leg. Therefore it is better to synchronise on location: whenever you cross the boundary region (a collection of cells), you start a new leg.

Privacy is improved by increasing the size of a cell, and by reporting visiting times in multiples of a sufficiently high step value (e.g., several seconds to a few minutes). Ideally, cell sizes should be chosen such that a relatively large amount of cars will be reported within such a cell within every fixed time interval (at least during normal traffic conditions). On the other hand, if cells are big, short trips within one cell essentially consist of one leg, reducing the privacy. For the purpose of this paper we simply note that the division of trips into legs increases the privacy of the average user considerably.

4.2 System Components

We distinguish the following components in the system (see also Figure 2):

– **On Board Unit (OBU).** Equipment installed in each vehicle. Contains all the hardware and software needed to interface the vehicle with the road pricing system. Contains a GNSN (Global Navigation Satellite System) receiver, or an external connection to it.

[1] Clearly a single car on a quiet country road can be followed. But even in this case the system guarantees that the identity of the car is not revealed.

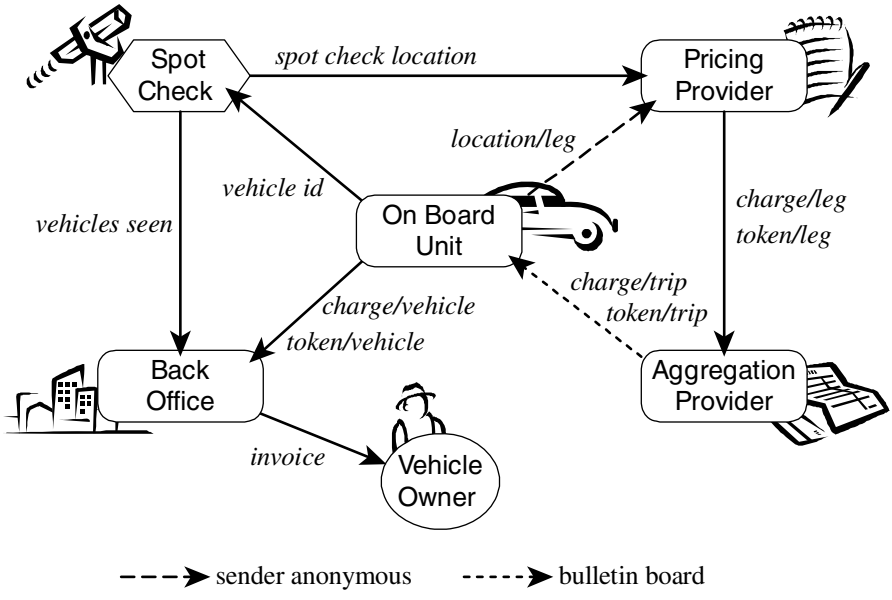


Fig. 2. Road pricing system components with related information flows

- **Pricing Provider (PP).** A service provider that computes the charge for a particular leg (of a trip). Privacy is assured because the PP cannot determine whether two legs belong to the same trip or not.
- **Aggregation Provider (AP).** A service provider that aggregates the leg charges to compute the total trip charge. Privacy is assured because the AP does not see the trajectory (cells visited) that corresponds to a particular leg.
- **Back Office (BO).** The road pricing back office receives the submitted trip reports from the OBUs, verifies this with spot check data, and sends out the invoices to the vehicle owners.
- **Spot Check (SC).** Actual road activity is measured using Spot Checks that record vehicles seen at certain road locations (cells).
- **Vehicle Owner (VO).** The owner of the vehicle that will receive the invoice for the road usage charges to be paid.

The description and analysis in this paper assumes that the pricing and aggregation service is offered by separate entities. We assume that in our business context there may be more pricing providers and aggregation providers, which vehicle owners are free to choose.

Note that we need to take some precautions regarding the communication from and to the OBU in order to ensure privacy. In particular, location messages sent from the OBU to the PP must be sender anonymous. Also, the total charge records for a trip calculated by the AP cannot be sent to the OBU directly. Instead, they must be published on a bulletin board from which the OBU (knowing which trip it engaged in) can collect it in an anonymous fashion.

Table 1. Overview of the information known to each system component

Component	Knows	Does not know
On Board Unit	locations visited by vehicle	spot check location vehicles seen by spot check
Pricing Provider	locations visited during leg	link of leg to trip or vehicle locations visited by vehicle
Aggregation Provider	charge for a leg charge for a trip	link between trip and vehicle locations visited during leg locations visited by vehicle
Back Office	charge for a vehicle	link of vehicle to trips or legs[2] locations visited by vehicle
Spot Check	vehicles passing	legs, trips

5 Architecture

Having discussed the assumptions, requirements and design principles we are ready to discuss our architecture for a privacy friendly yet fraud-resistant road pricing system.

5.1 Definitions and Notations

We use the RSA cryptosystem [14], and write $i = (e, n)$ for the private key of entity i, and $i = (d, n)$ for the corresponding public key. The encryption of a message m with public key is denoted by $\{m\}_K$. We assume that the encryption is non-malleable [5]: any modification to the encrypted message will be detected. Because we want to use the blinding techniques from Chaum [4], we define the following variants of RSA signatures on a message m with private key $k = (e, n)$ (where we write a^k to denote a^e, i.e., we identify keys with the exponents they represent). The *normal* signature is defined similar to RSASSA-PKCS1-V1_5 from PKCS #1 [10].

$$[m_1, \ldots, m_z]_k \stackrel{\text{def}}{=} h(m_1, \ldots, m_z)^k \bmod n$$
$$[\![m \ , \ldots, m_z]\!]_k \stackrel{\text{def}}{=} m_1, \ldots, m_z, [m_1, \ldots, m_z]_k ,$$

where h is some secure cryptographic hash function. The second form is a shorthand for the message followed by its signature. A *blindable* signature is defined as follows.

$$\langle m_1, \ldots, m_z, b \rangle_k \stackrel{\text{def}}{=} (h(m_1, \ldots, m_z) \cdot b)^k \bmod n$$
$$\langle\langle m_1, \ldots, m_z, b \rangle\rangle_k \stackrel{\text{def}}{=} m_1, \ldots, m_z, b, \langle m_1, \ldots, m_z, b \rangle_k .$$

For this signature the following lemma holds.

Lemma 5.1. For any RSA key pair K, k, n and any $m_1, \ldots, m_z, x$ and r we have

$$\langle m_1, \ldots, m_z, x \cdot r^K \rangle_k = r \cdot \langle m_1, \ldots, m_z, x \rangle_k \ (\mathrm{mod} n).$$

[2] Although if an OBU submits a charge that is unique, this may be linked to the particular trip that happens to have the same charge as computed by the AP.

Each vehicle has a unique public identifier v. Trips (with identifier τ) are subdivided into legs (with identifier λ) as discussed in Sect 4. The position (i.e., the cell it is in) of vehicle v at time t is denoted $p_v(t)$. The vehicle's OBU samples a trip at regular time intervals, at least frequent enough to ensure that no 'gaps' occur in the traversed cells it records. All vehicles report the cells visited at time slots 0,1,2,3,.... If more than one cell is visited, all extra cells are reported for the same time slot.

5.2 Initial Setup

The system initialises the following private and public key pairs: k_v, K_v for the OBU, k_{BO}, K_{BO} for the Back Office, k_{PP}, K_{PP} for the Pricing Provider, k_{AP}, K_{AP} for the Aggregation Provider, and k_{SC}, K_{SC} for the Spot Check authority. A private key is only known to its owner. Public keys are known to all. Naturally, these keys change from time to time. However, key management issues are outside the scope of this paper.

Vehicle-, trip- and leg identifiers are cryptographically related, but can only be linked to each other by certain parties. This is the essential idea behind our protocol to achieve privacy while maintaining accountability and fraud resistance. They are computed by the OBU in the following way. The trip identifier τ is derived from the vehicle identifier v using randomisation similar to a blinded signature technique setting $\tau = v \cdot r_\tau^{K_{AP}}$ for some random r_τ. Because of this, using Lemma 5.1, for arbitrary message m the OBU can compute a signature $\langle m, v\rangle_{k_{AP}}$ from $\langle m, \tau\rangle_{k_{AP}}$ by dividing out r_τ. This way trip charges computed by the AP cannot be linked to reports submitted by the OBU to the back office.

The leg identifier λ is, in turn, derived from the trip identifier τ by encrypting it to the key of the aggregation provider, together with a random r_λ, i.e., $\lambda = \{\tau, r_\lambda\}_{k_{AP}}$. The AP can recover the trip identifier corresponding to a leg identifier by decrypting with k_{AP} and dropping the random (which is only included to make different legs non-linkable).

5.3 Pricing Protocol

We first describe the protocol to compute the charge for a trip. In the next section we will describe the additional messages that are exchanged to detect fraud.

We note that the messages between PP and PP and OBU and BO are encrypted to the public key of the intended receiver. This is not explicitly written in the description of the protocol messages to avoid superfluous notation.

At the start of a trip. OBU v generates a random r_τ and stores it. It computes $\tau = v \cdot r_\tau^{K_{AP}}$ and stores τ and r_τ.

At the start of a leg. The OBU generates a new random r_λ and sets $\lambda = \{\tau, r_\lambda\}_{k_{AP}}$. It initialises a message sequence counter $c_\lambda = 0$. The OBU sends a special marker message to signal the start of a new leg.

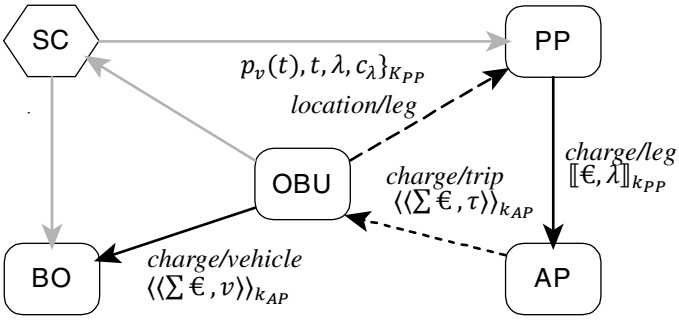


Fig. 3. Exchange of pricing messages between the system components

During a leg. The OBU anonymously[3] sends[4], at each time slot t, all visited cells during that time slot as $\{p_v(t), t, \lambda, c_\lambda\}_{K_{PP}}$ to the PP. The data is encrypted to prevent an eavesdropper collecting information about legs and locations. Because the encryption is non-malleable, secrecy of the leg identifier provides authenticity of the message. The message sequence counter c_λ is incremented by 1 for each such message sent. This prevents replay of location records. The PP receives this location record, decrypts it, verifies the expected message sequence counter for this leg, and if valid stores this record with all other location records for this particular leg λ. The expected message sequence counter is incremented by 1.

At the end of a leg. The OBU sends a special marker message to signal the end of a leg. The PP computes the total charge for the cells visited according to the location records stored for leg λ. It uses the pricing function to do so. It then sends the charge record $[\![€, \lambda]\!]_{k_{PP}}$ to the AP. The AP receives this message, verifies the signature, and, if valid, decrypts λ (which equals $\{\tau, r\}_{K_{AP}}$) to obtain τ. It stores the record with all other charge records for this particular trip τ. The AP only accepts a charge record for a particular leg once.

At the end of a trip. The OBU sends a special marker message to signal the end of a trip τ, which the PP forwards to the AP. After that, the AP no longer accepts charge records for trip τ. The AP computes the total trip charge $\sum €$ by summing all the charge records for this particular trip τ. It then computes $\langle\langle\sum €, \tau\rangle\rangle_{k_{AP}}$, and stores this on a bulletin board. At any time, the OBU can visit the bulletin board[5] (e.g. a web server), and, by knowledge of the trip identifiers it used, it can retrieve the payment

[3] For privacy reasons, the communication medium must hide the sender.

[4] We assume the communication link is reliable. This is a hard requirement in practice, because for privacy reasons the link is essentially uni-directional, which makes it impossible to send acknowledgements. The OBU may decide to send the same message several times to increase the likelihood of proper reception. The PP simply accepts the first message with the correct sequence number.

[5] Because the whole purpose of the exercise is to hide the vehicle identity from the AP, the AP cannot send the data to the right OBU directly.

records it needs from that bulletin board. The OBU then computes $\langle \sum €, \tau \rangle_{k_{AP}} / r_\tau$ for the value r_τ stored for τ. By Lemma 5.1 this equals $\langle \sum €, v \rangle_{k_{AP}}$ (because $\tau = v \cdot r_\tau^{K_{AP}}$. The OBU then sends the record $\langle \langle \sum €, v \rangle \rangle_{k_{AP}}$ to the BO for further processing.

5.4 Enforcement Protocol

In this section the enforcement protocol is presented together with the messages that are exchanged to detect fraud.

Setting up a spot check. Each spot check has a unique identifier γ. The spot check SC submits its location p and the time it starts checking vehicles and the time it stops checking vehicles to the pricing provider in the message $[\![p_\gamma, t_\gamma^s, t_\gamma^s, \gamma]\!]_{k_{SC}}$. A new γ is generated for every new location or time period of a spot check.

Checking vehicles. The spot check records all passing vehicles[6] and stores all vehicle identifiers it sees in the set V_γ. A vehicle passing multiple times is only recorded once. This set is sent to the BO when the spot check is closed.

Generating tokens. When a PP receives a location record $\{p_v(t), t, \lambda, c_\lambda\}_{k_{PP}}$, it checks for every spot check γ whether $p_v(t)$ is close to p_γ received for the spot check γ, and whether $t_\gamma^s \leq t \leq t_\gamma^s$. If this is the case, the PP generates a token $[\![\gamma, \lambda]\!]_{k_{PP}}$, testifying that this vehicle faithfully submitted its location record for this particular spot check location and time. At the end of a leg, all tokens for that leg are forwarded to the AP.

Attaching tokens to pricing messages. Tokens for a leg (and a trip, see below) are piggy bagged onto the pricing message for that leg (or trip). The pricing message contains a fixed number b of bins for this. If the number of tokens is less than b, the remaining bins are filled with random data (that look like genuine tokens except they correspond to non-existent spot checks). If the number of tokens exceeds b, then remaining tokens are sent in a next message that contains the same pricing message.

Forwarding tokens. When the AP receives a token for a leg λ, it will determine the corresponding trip τ as before, and store the spot check identifier γ with that trip. When the trip is closed, each spot check location recorded is appended to the pricing message using the fixed number of bins approach outlined above, and the AP generates the blind signature over the *whole* message: pricing data and the token bins. The OBU retrieves the charge record for the trip from the bulletin board as explained before, converting the blind signature by dividing our the value r_τ stored for τ, and forwards the result to the BO.

Matching tokens and checked vehicles. For each trip charge record, the BO verifies the signature. It discards any tokens that contain invalid spot check identifiers γ, and stores the remaining tokens as tuples (γ, v). The BO also receives, for each spot check γ a set of vehicle identifiers V_γ observed by that spot check. Vehicles must submit their records (charges and tokens) within a certain time frame. The BO processes the data of a spot check when the closing time of the spot check plus extended by the time

[6] There are several techniques to do so, without the vehicle noticing. We do not discuss this issue in this extended abstract.

frame lies in the past. For such a spot check γ, all valid tuples (γ, v) are processed, and any observed vehicle v is removed from the set V_γ. Any remaining vehicle identifiers in this set indicates a vehicle that did not submit a location record for that spot check location. This either indicates a system failure, or a possible case of fraud. Adequate action towards the Vehicle Owner can then be taken.

6 Security and Privacy Analysis

Due to space constraints we only mention the main lemmas that prove the correctness, security and privacy properties of our system.

Proposition 6.1. Let trip $\tau = v \cdot r_\tau^{K_{AP}}$ be generated by OBU v (using some random r_τ), and let τ not be closed yet. If the PP accepts a message for leg $\lambda = \{\tau, r_\lambda\}_{K_{AP}}$ (for some random r_λ), then that message was sent by OBU v.

Proof. By non-malleability of the encryption used between OBU and PP, and the fact that λ is only known to the OBU and the PP at least until the leg is closed, and τ is only known to the OBU and the AP at least until the trip is closed.

Proposition 6.2. Let τ be generated by OBU v. Let P the set of all location records $\{p_v(t), t, \lambda, c_\lambda\}_{K_{PP}}$ sent by the OBU v during this trip. If the PP and AP are honest, and no messages are lost, then the invoice $\langle\langle \sum €, \tau \rangle\rangle_{k_{AP}}$, computed by AP corresponds to the total charge due for P.

Proof. By Prop. 6.1, as long as τ is not closed, the charge for a one of its legs λ is only based on data sent by OBU v. No charges for τ are accepted by the AP after τ is closed. By honesty of PP and AP, if no messages are lost, the total charge must correspond to P.

Lemma 6.3 (Pricing Correctness). If the PP and AP are honest, an honest OBU only submits charges for trips it makes.

Proof. Immediately follows from Prop. 6.2.

Lemma 6.4 (Enforcement Correctness). If the SC, PP and AP are honest, an honest OBU cannot be accused of fraud.

Proof. Honest OBU's receive tokens for each spot check they pass.

Lemma 6.5 (Fraud resistance). If the SC and PP are honest, an OBU that submits incorrect, lower, invoices for trips it makes (or submits no such charges at all) will eventually be detected.

Proof. By Prop. 6 to submit an incorrect, lower, invoice the OBU must not submit location records for all locations actually visited. Eventually, one such location happens to be spot checked. Alternatively, if the OBU fails to submit a charge record to the BO, it cannot submit the corresponding tokens either.

Lemma 6.6 (Vehicle Privacy). The location of a vehicle at a certain time is only known to the OBU, unless that location was being spot checked at the time.

Proof. For non-spot checked locations, locations in location records are only bound to leg identifiers. These can be related to trip identifiers by the AP, but no party except the OBU can relate them to vehicle identifiers.

Lemma 6.7 (Trip Privacy). Except for the OBU, no other entity can reconstruct the full trip of a vehicle (unless that trip consisted of a single leg).

Proof. As discussed in section 4, if the number of vehicles in a boundary cell of a region is z, then the possible combinations of legs that make up a trip that corresponds to some vehicle is multiplied by z with every region change.

7 Conclusions and Further Research

In this paper we propose an architecture for a road pricing system that is privacy friendly as well as fraud resistant. In order to obtain fraud resistance we do not rely on trusted elements (for example a smart card or on-board-unit in the vehicle) but use a novel way of enforcement based on spot checking together with proof-of-honesty tokens given to vehicles that faithfully submit location data for spot-checked locations.

Privacy is guaranteed by splitting up trips in short legs that cannot be linked to each other, except by the aggregation provider. By the time the aggregation provider processes a leg, the privacy sensitive location data associated with a leg is already stripped. Hence, the aggregation provider does not get to see the actual locations corresponding to a particular leg. Legs and trips cannot be linked to a particular vehicle, except by the vehicle itself.

We note that our proposed architecture is open to extension of services. That is, the generated road usage data may not only be input for the application of road pricing itself, but can also be input for other road pricing services satisfying other apparent information needs that drivers, car owners, etc, may have. Moreover our solution can easily be applied to other contexts such as smart metering and e-ticketing in public transport where privacy and fraud-resistance seem to be conflicting issues.

Further work could address improvements in the privacy level of the enforcement protocol. In the current system, spot checks record the vehicle identifier of all vehicles passing. It may be possible to encrypt this identifier so that the spot checks themselves do not have access to the identifier, while the back-office can only decrypt the identifier if the corresponding proof-of-honesty token has *not* been received.

We thank the members, in particular Han Vogel, of the TNO project LERP for fruitful discussions on this topic.

References

1. Aurenhammer, F., Klein, R.: Voronoi Diagrams. In: Sack, J.-R., Urrutia, J. (eds.) Handbook of Computational Geometry, pp. 201–290. North-Holland, Amsterdam (2000)
2. Balasch, J., Rial, A., Troncoso, C., Geuens, C., Preneel, B., Verbauwhede, I.: PrETP: Privacy-Preserving Electronic Toll Pricing. Technical Report, COSIC, KU Leuven (2010)
3. Blumberg, A., Keeler, L., Shelar, A.: Automated traffic enforcement which respects driver privacy. In: 7th Int. IEEE Conf. on Intelligent Transportation Systems, ITSC (2004)

4. Chaum, D.: Blind Signatures for Untraceable Payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) Advances in Cryptology: Proceedings of CRYPTO 1982, pp. 199–203. Plemum, New York (1982)
5. Dolev, D., Dwork, C., Naor, M.: Nonmalleable Cryptography. SIAM J. Comput. 30(2), 391–437 (2000)
6. Eisses, S., de Jonge, W., Habers, V.: Privacy and distance-based charging for all vehicles on all roads. In: Proceedings of the 13th ITS World Congress (2006)
7. Gruteser, M., Liu, X.: Protecting Privacy in Continuous Location-Tracking Applications. IEEE Security & Privacy 2(2), 28–34 (2004)
8. Hubaux, J.P., Capkun, S., Luo, J.: The Security and Privacy of Smart Vehicles. IEEE Security & Privacy 2(3), 49–55 (2004)
9. de Jonge, W., Jacobs, B.: Privacy-Friendly Electronic Traffic Pricing via Commits. In: Degano, P., Guttman, J., Martinelli, F. (eds.) FAST 2008. LNCS, vol. 5491, pp. 143–161. Springer, Heidelberg (2009)
10. Jonsson, J., Kaliski, B.: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447 (2003)
11. Pieper, R.: MobiMiles: Bewust op weg. (report produced for the Ministry of Transport, Public Works and Water Management) (2001)
12. Popa, R.A., Balakrishnan, H., Blumberg, A.J.: VPriv: Protecting Privacy in Location-Based Vehicular Services. In: Proc. 18th USENIX Security Symposium, San Jose, CA, USA, pp. 335–150 (2009)
13. Rass, S., Fuchs, S., Schaffer, M., Kyamakya, K.: How to protect privacy in floating car data systems. In: Sadekar, V.K., Santi, P., Hu, Y.C., Mauve, M. (eds.) Proceedings of the Fifth International Workshop on Vehicular Ad Hoc Networks, VANET 2008, San Francisco, California, USA, September 15, pp. 17–22. ACM, New York (2008)
14. Rivest, R.L., Shamir, A., Adleman, L.M.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. ACM Commun. 21(2), 120–126 (1978)
15. Troncoso, C., Danezis, G., Kosta, E., Preneel, B.: PriPAYD: privacy friendly pay-as-you-drive insurance. In: WPES, pp. 99–107 (2007)

Privacy in Distributed Commercial Applications*

Nicolai Kuntze and Carsten Rudolph

Fraunhofer Institute for Secure Information Technology SIT,
Rheinstrasse 75, 64295 Darmstadt, Germany
nicolai.kuntze@sit.fraunhofer.de,
carsten.rudolph@sit.fraunhofer.de

Abstract. Devices installed in end-user's homes but controlled by network operators can be the basis for advanced distributed commercial applications. Virtual machines on these devices can be used to efficiently deploy and manage such applications provided by various competing entities. This paper discusses some security and privacy requirements of such distributed commercial applications and proposes two different approaches to root security and privacy in hardware-based attestation of nodes and virtual machines.

Keywords: Virtualisation, Privacy, Trusted Computing, Attestation.

1 Introduction

A major part of commercial applications on the Internet are currently client-server based with browser software representing the application on the client side. Individual users are identified via user name and password with additional security measures in critical applications such as electronic banking. Privacy requirements are often violated through the use of cookies, reading of browsing history, or linking of data between different services or providers. We currently see a diversity of alternative approaches to commercial applications appearing on the market. Some of these approaches involve third-party applications being installed on the client side, i.e. on the computer of the end-user. One prominent example is the App Store for iPhone applications [2] where applications are installed on the device. These applications can enable additional services. Also, devices installed by network operators can pave the way for new approaches to distributed commercial applications, in particular for the distribution of multi-media content.

An architecture for distributed commercial applications is being developed in the EU funded Nanodatacenters Project (NaDa). Autonomous devices are established in the households of the end users. These devices belong to a network operator (NO) and remain under his administrative control. Content providers (CP) can pay for resources on the devices in order to run applications to distribute their actual content according to their needs in terms of security and distribution strategies. P2P protocols are used

* This work was partly accomplished within the project Nanodatacenters under the grant number 223850 financed by the EC.

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 214–224, 2010.

to distribute the content in the network operated by the NO allowing for an efficient utilization of the network and its bandwidth.

In such a scenario it is not sufficient to protect privacy on the level of bi-lateral relations such as those between client and server. Privacy concerns arise if one identity is used in different applications, or different stake-holders and applications share the same devices and networks. Collecting and relating data or linking activities of a particular entity become possible. Aggregated knowledge may bring NO or CP in a position where they could predict an end-user's behavior, impersonate the user, or learn other confidential information. Such privacy issues are also relevant for the distribution system developed in NaDa.

This paper discusses the different and possibly conflicting security and privacy requirements of the stakeholders in distributed commercial applications. Pseudonymous or anonymous attestation of the state of a device protected by a hardware security anchor as part of Trusted Computing technology can be one building block towards privacy-preserving secure distributed commercial applications. Using the example of the NaDa nodes and P2P network, two approaches to pseudonymous and anonymous attestation are discussed. This attestation must include the state of the node itself as well as the CP application running in a virtual machine. The first approach uses a generic method of deep attestation through a virtual machine to the hardware TPM. The second proposal is tailored for the NaDa P2P network and relies on the mutual attestation of nodes in the network. Finally, this paper briefly discusses the two different approaches of attestation to different stakeholders in respect of their particular privacy and security requirements.

2 NanoDatacenters Architecture

The Nanodatacenters project aims at the virtualization of content distribution and access infrastructure. Inexpensive nodes form a P2P overlay network. On each node the network operator NO offers content providers CP virtual machines for rent, so-called slices. A CP can use such a slice to install operating system and application software. The underlying node uses hypervisor architecture to control slices and to provide interfaces to the slices and to the end-user. All communications and other external interfaces are only available through the hypervisor and thus controlled by the NO. One main idea of the NaDa architecture is to provide a network of nodes that can be used by the CP applications to efficiently manage a large number of client applications. The focus is on the domain of multi-media distribution. In this use-case slices can use resources on the node to store and cache multi-media data so that requested data might be provided directly through peers in the network. This approach can minimize the required bandwidth for a central server. Functional prototypes for such a P2P network are being developed in the NaDa project.

In this paper we assume that the operating system on the node, as well as the hypervisor and the operating system and application software on the slice, is properly implemented and free of failures as long as there are no malicious changes to software or configuration. Note that in order to increase assurance in the node's software the NO may require validation and certification on all software and applications running on the nodes.

Security requirements of the stakeholders user, NO and different CPs, are discussed in the next section.

3 Security Requirements Analysis

The different stakeholders, namely user, NO and CPs have possibly conflicting security and privacy requirements in the scenario described above. The presented application area bears similarities to concepts for outsourcing resources for services; for example, in cloud computing scenarios. Different parties move their computational, storage and communication load to an operator who then provides the resources and returns the results to the customer or directly to the end-user via clearly specified user interfaces. Advanced examples are operated e.g. by Amazon where customers can also run publicly available web servers on distributed leased resources. However, in contrast to these applications the P2P character of the underlying network and of possible applications results in unclear boundaries. Furthermore, locating all nodes at the homes of the end-user means that the NO has no physical control over the nodes. The following paragraphs discuss the different security requirements for user, NO and CP.

3.1 User Requirements

The end user represents a special case in this analysis due to his interaction with the node by receiving content and paying for it through the node. Privacy relevant information for the user includes data on content usage but also usage of the Internet through other services not located on the node. Content usage includes the content provided by a particular CP but also from the other CPs on his device. Also, end user specific data like payment information may be stored on the node associated with the user and the physical location of the particular box identifying the address of the user's household. All this information could support the building of a personal profile on the user, thus violating the user's privacy. Therefore, it is a very strong requirement to provide isolation mechanisms preventing unpermitted profiling through single or co-operating content providers.

3.2 CP Requirements

In all such scenarios the isolation of all different stakeholders running their systems on a shared platform is required in terms of resources and information governance. Resource protection has to be established, preventing customers from influencing the operation of other customers sharing the same resources. Information governance states that one party should not be able to access the information stored or processed by other parties. As the NO is the owner of the platform, and therefore has full control over it, all other parties need to lay trust in him. Although some privacy properties can also be enforced towards the NO, this needs access to data required in performing its processing tasks.

In the P2P network regarded here, nodes are operated in the households of end users and are therefore not under the direct physical control of the NO. Thus, nodes can potentially be manipulated. Establishing trust relations between the nodes involved requires that each node is able to provide proof on its state. This state shall represent

the operational state as defined by the NO. As the NO is assumed to have full control over the node, it is in principle able to modify each node and with it also the applications running on it on behalf of the NO's customers. Thus, customers also need to be able to verify the state of their respective application. This proof has to include evidence on the state of their particular slices on the node as well as the state of the underlying node system.

Furthermore, content providers should not have access to information on the status of other competitors running their applications on the same node. This property must also be satisfied if content providers operate their own monitoring software as part of their application. This requirement is to prevent leakage of business relevant information protecting the revenue model of each content provider (i.e. of the customers of the NO).

3.3 NO Requirements

The proof of the state of the node is also relevant for the NO who wants to ensure that only authorized and non-manipulated nodes can access the P2P network. This also requires that the node has got some kind of identity used to sign attestation data. This identity can also identify a node towards the CP's applications in order to provide evidence that data exchanged in the network stems from proper nodes actually belonging to the NO network. However, these identities also allow the CP to identify each individual node, and therefore privacy relevant information can be directly contained in them or be related and linked. Parameters like location, configuration, amount of data, bandwidth, accounting information and utilization allow the CPs to analyze the market penetration of a particular NO. Therefore the NO requires that information on the state of the nodes given to the content providers shall be restricted, and in particular, not allow the analysis of the overall network.

In the NaDa project a security architecture is built on Trusted Computing technology. One central challenge of the architecture is the realization of attestation for node and slices on the node in regard of the different security and privacy requirements described above. The contribution of this paper is to propose two ways to achieve this attestation. The following section gives a brief overview of the underlying concepts of Trusted Computing.

4 Trusted Computing

As discussed in section 3, privacy of the node's identity and secure reporting of the system state are important security requirements. In many approaches these requirements can be contradictory. Trusted Computing TC [17] offers a hardware root of trust that provides certain functionalities designed to approach the combination of requirements (see also [6, 8]). In this section these functionalities are introduced.

TC as defined by the Trusted Computing Group (TCG), are computer systems extended by additional components that shall bring trust to the computing environment. Trust means that components of the system always work as implemented. To achieve this goal, the TCG has published and is still working on specifications describing architectures affecting system components at any level from hardware to the operating system.

Most important hereby is the Trusted Platform Module (TPM). This module is mostly realized as a hardware chip hard-wired to the computer platform. It implements basic cryptographic functionality like SHA-1, message digest creation, random number generation, creation of 2048 bit RSA key pairs, and a RSA engine for encryption and signing purposes. Realized as an independent hardware module it provides protected capabilities for secure storage. The TCG defines three different roots of trust on which the trust to the whole system is built.

First, the Core Root of Trust for Measurement (CRTM) [9] performs initial measurements (e.g. hash values of the respective firmware) of system components involved in the booting process. Measured (and individually trusted) components can then perform measurements of other components involved in the next stage of booting. Through this principle of transitive trust, trust in the correctness of the measurement values can be passed on to the operating system, hypervisor and into virtual machines. Through this architecture it shall be guaranteed that a computer system always starts in an authenticated state that can be verified by an external entity and used for establishment of trust. This reporting process is called Remote Attestation (RA). Second, the Root of Trust for Reporting (RTR) is used in the RA process. Remote entities need to be able to validate that measurement results are genuine and come from a valid TPM and platform. For this purpose every TPM contains a unique 2048 bit RSA key pair, the Endorsement Key (EK), which is generated before shipping. The EK, together with an EK Credential, represents the identity of the platform. However, the EK is never directly used for signing attestation data. Instead, Trusted Computing provides two different techniques to conceal the identity of the platform embodied in the EK during the attestation of the platform:

4.1 Pseudonymous Attestation Based on a Privacy CA

The first proposed concept to protect the privacy of the customer introduced by TCG relies on a trusted third party issuing pseudonyms for the individual TPM platforms, the so-called privacy certification authority (Privacy CA). When a TPM needs to authenticate to a verifier, it generates an RSA key pair called the Attestation Identity Key (AIK) and sends the AIK public key together with public EK and EK certificate to the Privacy CA. There the AIK is authenticated using the EK; the Privacy CA then issues (based on certain rules) a certificate on the TPM's AIK. The TPM then uses this certificate (and the corresponding AIK) to sign measurement values. Note that in this approach verifiers cannot link different actions from the same platform as long as different AIKs are used. However, the Privacy CA can link all AIKs to the unique EK and therefore could reveal the identity of the platform.

4.2 Direct Anonymous Attestation

Direct Anonymous Attestation (DAA) as explained in [1] is a practical and efficient scheme for authenticated pseudonymous attestation with strong privacy properties. In the scheme four parties are involved as shown in Figure 1. A certification authority CA certifies long term public keys (1). The role of the CA corresponds to the role of CAs in usual public key infrastructures. The so-called DAA-issuer creates blindly signed credentials in the DAA join phase (2) that is later used in the DAA attestation

(3). The main idea is that the certificate is not actually shown to the verifier. Instead, a zero-knowledge proof is used to prove that the platform owns a certificate issued by the DAA issuer. Thus, even the DAA issuer in principle cannot link different AIKs to the EK of the platform. It is to be noted that DAA allows for different operation modes with different levels of anonymity. Rudolph presents in [11] an attack showing the limitations of this scheme. This attack is also discussed in [7].

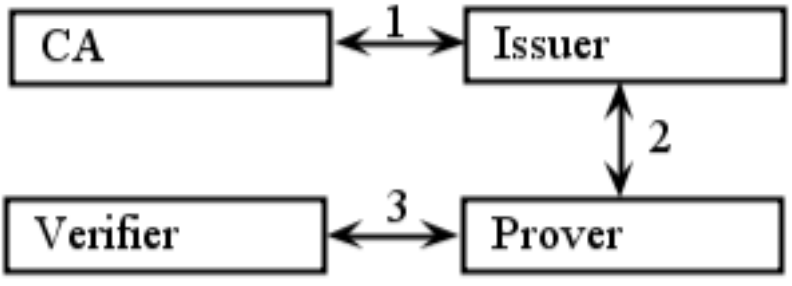


Fig. 1. Overview on DAA interactions

5 Attestation of Virtualized Environments

Satisfaction of the security and privacy requirements identified in Section 3 depends on the state and configuration of the node, in particular of the hypervisor controlling the slices and providing the desired isolation between the slices. The design of the node operating system that is attested to the communication partners is not within the focus of this paper. Different approaches exist for the communication within distributed environments, e.g. building IP over P2P [4] communication allowing for a Virtual Private Network for each customer. There is also work on the design of virtual machine sand-boxes in overlay networks [20, 18]. For this paper we assume the existence of a secure and hardened system with known reference measurement values.

However, the existence of a secure node software is not sufficient. Different stakeholders cannot blindly trust the nodes to be properly implemented and configured. They need assurance that nodes are not changed or compromised. As described in the previous section, TC can be used for attesting the state of a node to a remote party. Nevertheless, deploying remote attestation is not straightforward in a multi-stakeholder environment with multiple virtual machines installed in the slices of each node. Virtual machines only have limited knowledge about the state of the node they are running on. Furthermore, a single hardware TPM with a single identity has to be used for the attestation of several virtual machines. As the virtualized system has no direct access to the TPM of the underlying platform, it has to use its own (intermediate) root for security, a so-called virtualized TPM (vTPM). This concept is also introduced and discussed from different perspectives in [12, 14, 19]. The correct functionality of a TPM depends on its implementation located in the underlying virtualization system. In order to fulfill the requirements of providing proof of the state of the system, this proof also has to include proof on the underlying system.

In the NaDa architecture attestation needs to consider the individual requirements of NO, CP and end-user. The end-user has to trust the NO with respect to the correctness and security of the software installed on the node and of the configuration. Therefore, in this approach we assume that the end-user also delegates the checking of the integrity to the P2P network controlled by the NO.

The NO is mainly interested in the integrity of the node itself. The software installed within the slices is not relevant for the NO as the slices are controlled by the hypervisor. Consequently, the standard TC protocols for remote attestation can be used to check the integrity of the node each time it joins the P2P network for a new session. This attestation needs to be properly integrated into the establishment of new session keys with the peer nodes. For increased assurance, bi-lateral attestation can be repeated during a running session. Failure would result in termination of the session.

In contrast to the NO, CPs are interested in the integrity of their own slices and also that the underlying node and environment is in accordance with the SLA. Information on other slices belonging to different CPs shall not be available to a CP. Furthermore, as described in Section 3 the CP should not get all possible status information because some of the information can be considered part of the confidential business information of the NO. It might also be required that different CPs shall not be able to link status information from their different slices to platform identities.

The following subsections present two different approaches for attesting node and virtual machines in the slices. The nodes in the NaDa project only allow one layer of virtualization. Thus, the more complex case of several virtualization layers is not discussed here. Considering different concurrent attestation requests on one node can result in a performance bottleneck. Fuchs et al. analyzed in [15] possible strategies to approach this problem.

In addition to the attestation it is necessary to protect the communication channels between nodes as well as between slices. These channels need to be bound to the hardware security anchors such that it is assured that the attested state is indeed the state of the end-point of the communication channel. Goldman et al. first proposed a protocol that binds the secure channel established by SSL/TLS to the remotely attested platform [5]. Other work in this area also shows the importance of this ability e.g. [3, 10, 13].

5.1 Pseudonymous Node Using Deep Attestation

In this approach the status of one slice as well as the status of the underlying platform are attested in a single step towards another slice. This other slice is usually located on a different platform, but the slices can also share one platform. The signature generated by the TPM as result of the TPM_Quote command is included in the quote produced by the vTPM.

During the deployment process of a new slice on the node two individual attestation identity keys are created that have to be assumed as being unique for this slice. The first AIK is located in the TPM of the node, while the second key (called vAIK) is an attestation identity key of the vTPM of this particular slice. The usage of the vAIK is restricted by the TPM_Bind operation controlled by the TPM to a specific state of the node and can be bound through the vTPM to a particular state of the individual slice. A certificate for the AIK is issued by the NO or a representative stating

that the node is a node of a certain type and that its usage is restricted to a particular role in the P2P network. The certificate for the vAIK needs to include the AIK of the node to bind the vAIK and the vTPM to the physical TPM.

The slice to be attested has to provide proof that the system running within the slice is compliant to its desired state according to the implementation deployed, and that the node hosting the slice is also not altered. Integrity of the node is in particular needed to show that the vTPM is operating according to its definition and to ensure the isolation of slices on the node.

By using a unique AIK for each slice on a node it is ensured that the identity of the node cannot be linked to other attestation messages for other slices on the same node. The node guarantees that the AIK usage is limited to the attestation of one particular slice.

The attestation process is denoted with deep attestation because it goes through the slice and the vTPM to the hardware TPM of the node. Thus, in one step, it provides two encapsulated remote attestation protocols of the type. During an attestation process a verifier sends to the slice a remote attestation challenge that results in a vTPM_Quote command to the vTPM. The challenge contains a nonce generated by the challenger and used to prevent replay attacks. Implementing deep attestation uses this nonce to also challenge the TPM of the hosting system using TPM_Quote and to return in the result of the vTPM also the attestation result from the TPM.

In order to gain better scalability, the PCA required to sign the AIKs for each slice could be implemented as an internal service of the node operating as a representative of the NO. The required credentials to sign the AIKs are shared between all nodes or a certain subset of nodes. Thus, credential information cannot be used to track back a certain AIK signature to a specific node. To ensure that the node is not issuing fake certificates, and to prevent extraction of the credentials, certain means are required. First, the credentials have to be bound to a certain state of the node preventing malicious software on the node to make use of them. Also, the lifetime of these credentials needs to be limited to a certain (relatively short) time. After this time a replacement mechanism in the P2P network has to renew these credentials and new certificates for the AIKs should be issued.

Clearly, a so-called privacy certification authority (PCA) with high availability is required to issue new AIK certificates for each slice quite often. There are strong security requirements for this PCA, as it is able to reveal the public EK of the TPM for each AIK. Thus, the PCA is able to link different AIKs of the same platform. High availability and security are often seen as contradictory (or at least expensive) requirements. Furthermore, the PCA needs to be separated from the stakeholders of the system. Therefore, it is not clear that a PCA could run with a reasonable business model in such a system. Using DAA could overcome this problem and also provide better privacy.

The deep attestation approach provides attestation of one slice and the underlying node in a single step. The next proposal distinguishes between node attestation and slice attestation. It is tailored for the use in the NaDa P2P scenario.

5.2 Two Step Attestation

The vTPM, in order to implement the deep attestation, needs to differ from a standard TPM as it has to include a TPM_Quote result from the hardware TPM in its own quote. Further, the hardware TPM needs to provide a unique AIK for each slice. Splitting the process in two steps leads to a scheme that does not require modifications to the TPM and also requires only one identity per node and one identity per slice.

Figure 2 depicts the high level steps required. Step one is performed between the hosting environments of the nodes in the P2P network. This process establishes the fundamental trust and also allows that all services offered by the host to the slices are trustworthy as soon as the slice is part of the network. This can be done initially for each session and includes a key exchange to build a session as it is e.g. proposed in [16]. It should be notes that each CP will control at least one node of the peer-to-peer network in order to be able to introduce data into the network. For the CP this node is the root for establishing trust in the other nodes of the network. This trust is achieved by mutual attestation between nodes in the network together with trust in the node software and configuration. The only way to communicate for the slices is through this (now trusted) overlay network. Thus, communication with another slice implies that the underlying host platform is part of this P2P network.

In step two the CP checks the integrity of the slices by performing a remote attestation using vTPM on the slice. These vTPM can operate according to the defined TPM standard.

The host can restrict the interaction of slices according to interaction policies, allowing only for communication between slices from the same owner. This forms another logical overlay network. Interaction between slices is isolated between different CPs. Thus, privacy breaches on the level of information flows between slices are prevented.

In comparison with deep attestation several advantages and disadvantages can be identified. First, it can be seen as a disadvantage that the content providers must trust the NO to enforce the attestation-based control for nodes joining the P2P network. However, the NO will also provide reference values for node states to be used in deep attestation. Therefore, if CPs can actively check the state of the nodes in the case of deep attestation they still have to trust the NO in providing secure configurations.

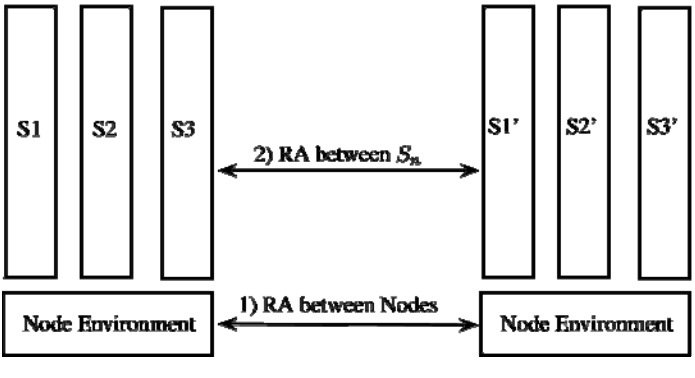


Fig. 2. Two step remote attestation

The option of having private logical overlay networks can be used to isolate traffic and increase the privacy of the CPs. Furthermore, it is not necessary to make the actual identity of nodes visible to the CP. For many applications it is sufficient to know that the slice is running on a node in the P2P network.

This second solution integrates the attestation of the nodes into the establishment of the P2P network. Optional subsequent slice attestation is in the control of the CP and independent from the underlying node controlled by the NO. Furthermore, only one AIK is needed for each node. Thus, organizational processes are more efficient. This solution was chosen for integrating it into the NaDa architecture.

6 Conclusion

The different types of attestation for virtual machines show that Trusted Computing mechanisms can be adapted to different scenarios and requirements without changes to the underlying trusted platform architecture. Different privacy requirements can be satisfied on the basis of this technology without losing security properties required by network operators and service providers. It is this combination of privacy and security that makes trusted computing based solutions suitable for various electronic commerce applications. The use of TPMs in home boxes such as those used in the NaDa project can increase the security of these boxes, and also be the basis for reliable devices to be used in advanced distributed electronic commerce applications.

Prototypical implementations of the privacy and security mechanisms, including independent remote attestation of nodes and slices, have been completed within the Nanodatacenters project. Future work will include the integration of these mechanisms into distributed electronic commerce architectures in order to evaluate the overall privacy and security properties, and the efficiency and usability, of the architecture.

References

1. Brickell, E., Camenisch, J., Chen, L.: Direct anonymous attestation. In: Proceedings of the 11th ACM Conference on Computer and Communications Security, pp. 132–145. ACM, New York (2004)
2. Chen, G., Rahman, F.: Analyzing Privacy Designs of Mobile Social Networking Applications. In: Proceedings of the 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, vol. 2, pp. 83–88. IEEE Computer Society, Los Alamitos (2008)
3. Dietrich, K.: A Secure and Reliable Platform Configuration Change Reporting Mechanism for Trusted Computing Enhanced Secure Channels. In: ICYCS 2008 – The 9th International Conference for Young Computer Scientists, pp. 2137–2142 (2008)
4. Ganguly, A., Agrawal, A., Boykin, P., Figueiredo, R.: IP over P2P: Enabling Self-configuring Virtual IP Networks for Grid Computing. In: Proc. International Parallel and Distributed Processing Symposium (2006)
5. Goldman, K., Perez, R., Sailer, R.: Linking remote attestation to secure tunnel endpoints. In: Proceedings of the first ACM Workshop on Scalable Trusted Computing, pp. 21–24. ACM, New York (2006)

6. Kuntze, N., Schmidt, A.U.: Trusted ticket systems and applications. In: New Approaches for Security, Privacy, and Trust in Complex Systems. Proceedings of the IFIP sec2007, Sandton, South Africa, May 14-16. Springer, Heidelberg (2007)
7. Leung, A., Chen, L., Mitchell, C.: On a Possible Privacy Flaw in Direct Anonymous Attestation (DAA). Technical Report, Tech. Report RHUL-MA-2007-10, Mathematics Department, Royal Holloway. University of London (December 2007)
8. Mitchell, C., et al.: Trusted Computing, vol. 1. IEEE Press, London (2005)
9. Pearson, S.: Trusted Computing Platforms, the Next Security Solution. HP Laboratories, Bristol (2002)
10. Pollock, W., Pitcher, C. Chicago, I.: Identifying Trustworthy Hosts Using Remote Attestation, `http://facweb.cti.depaul.edu/ctiphd/ctirs04/submissions/camera-ready/Pollock.doc` (accessed on May 31, 2010)
11. Rudolph, C.: Covert Identity Information in Direct Anonymous Attestation (DAA). IFIP Security, 232–443 (2007)
12. Scarlata, V., Rozas, C., Wiseman, M., Grawrock, D., Vishik, C.: TPM Virtualization: Building a General Framework. Trusted Computing: Ein Weg zu neuen It-sicherheitsarchitekturen (2007)
13. Schechter, S., Greenstadt, R., Smith, M.: Trusted computing, peer-to-peer distribution, and the economics of pirated entertainment. In: Proceedings of The Second Annual Workshop on Economics and Information Security, pp. 29–30. Springer, Heidelberg (2003)
14. Schmidt, A., Kuntze, N., Kasper, M.: On the deployment of Mobile Trusted Modules. In: Proceedings of the 9th IEEE Conference on Wireless Communications and Networking (WCNC 2008), pp. 3169–3174 (2008)
15. Stumpf, F., Fuchs, A., Katzenbeisser, A., Eckert, C.: Improving the scalability of platform attestation. In: Proceedings of the 3rd ACM Workshop on Scalable Trusted Computing, pp. 1–10. ACM, New York (2008)
16. Stumpf, F., Tafreschi, O., Roder, P., Eckert, C.: A Robust Integrity Reporting Protocol for Remote Attestation. In: Proceedings of the Workshop on Advances in Trusted Computing, WATC (2006)
17. Trusted Computing Group. TPM Specification Version 1.2 Revision 103. Trusted Computing Group (2009)
18. Tsugawa, M., Fortes, J.: A Virtual Network (ViNe) Architecture for Grid Computing. In: Proc. of the IEEE Intl. Parallel and Distributed Processing Symp (IPDPS), Rhodes, Greece (June 2006)
19. Winter, J.: Trusted computing building blocks for embedded linux-based arm trustzone platforms. In: STC 2008: Proceedings of the 3rd ACM Workshop on Scalable Trusted Computing, pp. 21–30. ACM, New York (2008)
20. Wolinsky, D., Agrawal, A., Boykin, P., Davis, J., Ganguly, A., Paramygin, V., Sheng, Y., Figueiredo, R.: On the Design of Virtual Machine Sandboxes for Distributed Computing in Wide-area Overlays of Virtual Workstations. In: Virtualization Technology in Distributed Computing, VTDC, p. 8 (2006)

Section 4

ICT and Sustainable Development

ICT and Sustainable Development

Lorenz M. Hilty[1,2] and Magda David Hercheui[3,4]

[1] University of Zurich, Department of Informatics, Binzmuehlestr. 14,
CH-8050 Zurich, Switzerland
[2] Empa, Swiss Federal Laboratories for Materials Science and Technology, Lerchenfeldstr. 5
CH-9014 St.Gallen, Switzerland
[3] Westminster Business School, 35 Marylebone Road, London, United Kingdom, NW1 5LS
[4] London School of Economics, Houghton Street, London, United Kingdom, WC2A 2AE
lorenz.hilty@empa.ch, m.hercheui@lse.ac.uk

Abstract. We discuss various views and conceptual frameworks put forward in the discussion of ICT and sustainable development: An optimistic and a pessimistic view of ICT with regard to sustainability, the three-pillar approach to sustainable development, the three-level approach to ICT impacts, the claim of human, social and ecological compatibility of ICT and the plain use of ICT for development. We show that each of these approaches has its problems and limitations and conclude with formulating the challenges of finding an analytical approach which will effectively support decision-makers in using ICT in the service of sustainable development.

Keywords: Sustainable Development, Ethics, Technological Determinism, Life Cycle Assessment, Green ICT, Rebound Effect, ICT for Development.

1 The Ethics of Sustainable Development and the Role of ICT

The most-cited definition of "Sustainable Development" was given by the World Commission on Environment and Development: In order to be considered sustainable, a pattern of development has to ensure "that it meets the needs of the present without compromising the ability of future generations to meet their own needs" [1]. This definition, also known as the "Brundtland definition", combines two ethical claims:

- *intra*generational justice (meeting the needs of the present) and
- *inter*generational justice (not compromising the ability of future generations to meet their own needs).

Given the physical and biological limits of our planet [2], this double claim is in fact an ethical dilemma because extending the present consumption patterns of the industrialized countries to all parts of the world would put a great burden on future generations. Escaping this dilemma requires a structural change of the economy that will deeply affect today's industrial patterns of production and consumption.

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 227–235, 2010.

Regarding the role of ICT in the sustainability dilemma [3], there are two opposite positions:

- the optimistic view based on the belief that this structural change is already under way due to the development and world-wide diffusion of ICT;
- the pessimistic view in which ICT adds to resource consumption and pollution and reinforces unsustainable structures and behaviour.

Research in "ICT and Sustainable Development" or "Informatics and Sustainability" has the obligation to strive for a realistic view and provide decision-makers with scientifically sound answers. The growing body of research in this field has clearly shown that ICT is part of the solution and part of the problem at the same time (for a survey see [4] and [5]). It is therefore crucial to find models of ICT governance that exploit the potential of ICT for sustainable solutions while inhibiting the negative potential. This requires, in the first place, a conceptual framework of the interaction between the development of ICT and its applications and other societal developments. The following sections will provide a brief survey of the core ideas and approaches discussed in literature.

2 The Limits of Technical Solutions to Sustainable Development

Both views mentioned above – the optimistic and the pessimistic – suffer from the same problem: they are based on technological determinism insofar as they implicitly assume that ICT development cannot be controlled and the resulting impacts on society are a logical consequence of some "autonomous" technological development.

Technological determinism denies that the development and application of technologies are the result of human choice. In the context of ICT and "the information society" this basic assumption is particularly debilitating. As Holvast et al. [6] put it: "Such determinism reduces humankind to powerless pawns who can only accept their fate and wait to see what other people will do to help them. It is our belief that more can be done by human beings themselves than is often admitted."

The relationship between technological artifacts and the society that creates and interprets them is a complex one: Technologies interact with our perception of the world, which again influences how we use and develop technologies. In this process both symbolic and structuring aspects of technologies play a role, as Zuccato and Fischer-Hübner [7] describe: "…technology not only has a socio-cultural semantic effect (influence on social life) but also an effect on the subject's world experience (it influences the perception of the world and what the individual understands this to be)." Consequently, using technologies influences needs, values, beliefs and other social realities that provide the context for the further development and application of technologies.

From this view of technologies as being embedded in societal development, it follows that solutions to the sustainability dilemma will not be technical solutions alone. As far as technology is involved – and ICT might play a crucial role there – it can only be instrumental as part of a more comprehensive approach, being embedded in organizational or institutional frameworks or in structures of governance.

Conceptual frameworks to structure and analyze the relationship between ICT and sustainable development like those described in the next section are always in danger of falling back into technological determinism by implicitly assuming a unidirectional view of "effects" or "impacts" of a "given" technology on society. It is sometimes necessary to reduce complexity by clipping one of two interacting things and then looking at the other. This is the typical approach underlying the various types of impact assessment, which has many advantages but should be embedded in a model of organizational learning, policy learning or governance [8].

3 Conceptual Frameworks for ICT and Sustainable Development

A conceptual framework for an analytical approach to the relationship between ICT and sustainable development first has to decompose the normative concept of sustainable development.

A very common idea is the so-called three-pillar or three-dimensional approach to sustainable development, decomposing the concept into an ecological, a social and an economic dimension. The role of ICT can then be analyzed along the following questions:

- Ecological dimension: What is the role of ICT in ecological (environmental) issues? How can we use ICT to increase our understanding of ecosystems and to reduce environmental burden (Environmental Informatics)? How can the environmental impact of production, use and disposal of ICT be reduced (Green ICT)?
- Social dimension: What is the role of ICT in social development? How can we use ICT to support (virtual) communities working towards the aim of sustainable development? How can social justice on a global scale be supported by ICT? How can we increase the contribution of ICT to long-term thinking and avoid short-sighted, technologically determined developments?
- Economic dimension: What is the role of ICT in the structural change of the economy from an industrial to a post-industrial mode? How can ICT contribute to a decoupling of economic growth from growth in resource consumption, to substitute virtual forms of production and consumption for energy-intensive processes, to dematerialize relevant parts of the economic system? And how can ICT help emerging economies to leapfrog into this mode without copying the unsustainable patterns of the industrial mode first?

Although this three-dimensional approach may serve as a starting point for brainstorming, it does not provide a sound basis for analysis. Firstly, we also need to decompose the role of ICT in this context, since digital ICT is an almost universal technology and application categories are more relevant than the technology as such. Secondly, multidimensional concepts of sustainable development have been criticized for being inconsistent (the "dimensions" are not at the same conceptual level, i.e. they wrongly suggest orthogonality) and for watering down the concept of sustainable development by suggesting that a depletion of ecological or social capital may be accepted in exchange for economic capital ("weak sustainability" [3]).

Conceptual frameworks for "ICT and sustainable development" that go beyond this approach are briefly discussed in the following sub-sections. None of these

frameworks claims to provide a comprehensive solution. Rather, they may be viewed as ingredients in a more comprehensive approach that still has to be formulated.

3.1 Three Levels of ICT Effects

This approach focuses on applications of ICT and first asks in which way they influence the environment. The three levels cover environmental impacts ranging from the most direct effects (physical effects of using the hardware) to the most indirect effects such as the influence of ICT on economic structures and lifestyles [9]:

- "First-order effects: Includes all environmental impacts resulting from ICT hardware during the product lifecycle, covering production, use, and disposal."
- "Second-order effects: The use of ICT causes effects to other processes such as traffic or industrial production and influences *their* environmental impacts indirectly."
- "Third-order effects: Owing to the assumed widespread use of ICT in everyday life, economic structures and lifestyles can change, indirectly affecting the expression of first- and second-order effects."

The three-level approach is very common in research on environmental impacts of ICT, although it could in principle be generalized to effects on social systems, including the economic system. In fact, the concept of second-order effects presupposes some organizational context in which ICT is used, while third-order effects can only be assessed or explained in a societal context, including, for example, market dynamics.

During the last decade, a few methodologies have been explored to quantify ICT effects at each level.

At the first level, existing Life-Cycle Assessment (LCA) methodology has been applied to computers [10] and to communications infrastructure as well [12]. Life Cycle Inventory (LCI) databases (such as the ecoinvent database [11]) have been extended to include ICT hardware. Some of the work on first-order effects has also focused on end-of-life issues due to the environmental and health problems caused by informal recycling in developing countries [13] and the dissipative use of increasingly miniaturized devices [14, 15]. With the "Green IT" or "Green ICT" hype starting in 2008, the energy consumed by ICT terminal devices and network infrastructures (in particular the Internet) has gained public attention. This view sometimes includes aspects of the second level, in particular when the idea of "Green Software" is introduced. Dick et al. [16] provide an excellent update on this topic in this volume.

At the second level, the methodologies used for quantification are more diverse and difficult to compare. How can we measure the implications of – for instance – mobile work, knowing that mobile ICT is only one of many factors changing the mobility behaviour of people? Erdmann and Hilty [5] provide a review of studies which tried to quantify second-order effects of ICT applications in terms of energy saving potential (or CO_2 reduction potential) at the macro-economic level, including rare cases in which first- and third-order effects were included. Three papers in this volume contribute to this body of knowledge. Houghton [17] gives significant examples of ICT applications which can mitigate climate change and other environmental pressures. Bunse and Vodicka [18] open the perspective for organizational aspects which are essential for using ICT to manage energy efficiency in manufacturing

processes. Santana et al. [19] show how information systems with a Service-Oriented Architecture (SOA) can be used to support sustainable design.

The third level of ICT effects is the most difficult one to be treated quantitatively. Erdmann and Hilty [5] discuss how rebound effects can be dealt with in a scenario-based model. However, rebound-effects (based on efficiency-induced changes of demand) are not the only type of third-order effects: ICT deeply changes the way we communicate. This profound change can affect social systems at all levels, from an organization such as a company to the global society. This is the point where it is essential to abandon technological determinism and adopt a broader view, such as the theory of communicative action by the German philosopher Jürgen Habermas. This is the perspective advocated by Möller and Rolf ([20], in this volume) with their approach to IT support for sustainable development in organisations.

3.2 Human, Social and Ecological Compatibility of ICT

The German Informatics Society set up a working group named "Sustainable Information Society" to clarify the opportunities and risks of ICT for sustainable development one decade ago. The group produced a detailed memorandum that was published as a Fraunhofer IRB book in German with an English abstract [21] and summarized in international publications [22, 23].

The approach taken by the working group has two essential features. Firstly, it builds upon the tree-level approach described in the previous section by redefining the levels as follows:

1. "effects of supply": effects of the effort necessary to provide people with information and communications services, including the production of ICT hardware and software, supplying the energy and other resources to use ICT, and the end-of-life treatment of the hardware.
2. "effects of usage": effects of services provided by ICT viewed in the restricted context of the application, such as substitution or optimization effects.
3. "systemic effects": long-term effects that have to be taken into account, mainly because positive effects of usage may backfire in the economic system (rebound effects).

The working group emphasized that steps toward a sustainable information society cannot be based on technological measures alone [9]: "This is partially due to the so-called rebound effect, according to which a transition to more efficient technologies causes an expansion of activities given constant financial and time budgets. Because of this effect, technological measures alone do not cause a reduction in the use of natural resources by production and consumption."

The second feature of this approach is that it explicitly replaces the "three-pillar thinking" of weak sustainability (as discussed in the beginning of section 3) with the concept of three nested subjects of protection: the *human individual* as part of *society,* which is embedded in *nature*.

From these subjects of protection the working group derived three claims of compatibility: human, social and ecological compatibility. Combining this idea with the three levels of ICT effects yields nine fields of research and societal discourse that should be considered if ICT is to support sustainable development (see Figure 1).

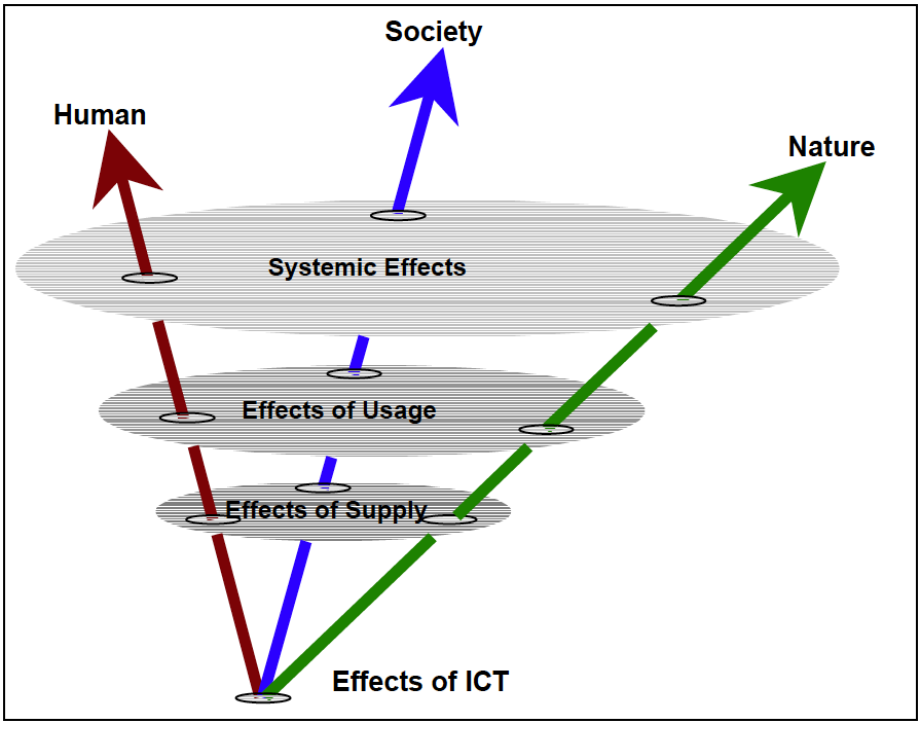


Fig. 1. The conceptual framework created by the working group "Sustainable Information Society" of the German Informatics Society in 2004 [22]

3.3 ICT for Development

This prominent approach differs from the two presented above by its simplicity. It ignores the sustainability dilemma we briefly introduced in Section 1 by putting the emphasis on *intra*generationational justice: ICT is seen as a vehicle to empower the poor and enable development in underdeveloped regions of the world. The overuse of natural resources is implicitly expected to be reduced, rather than, increased by economic growth in poor countries.

This approach has at least some arguments working in its favour, the first of them being the statistical fact that population growth is negatively correlated with the education of young women. If it is true that ICT can successfully be applied in educating the poor, ICT would then indeed contribute to sustainable development. Secondly, there are some impressive examples of leapfrogging into the information society, most of them centered around the role of the mobile phone, which is an essential infrastructure that can be built up without waiting for other industrial infrastructures, even without centralized and stable power grids.

The issue of supplying schools in developing countries with affordable computers is treated by Streicher-Porte et al. [24], and Dobson et al. [25], showing another excellent example of ICT for development in this volume.

4 Conclusion: Challenges in ICT and Sustainable Development

We have shown that analysing the relationship between ICT and sustainable development poses a number of challenges:

- finding a meaningful decomposition of the concept of sustainable development to start with,
- finding a meaningful classification of ICT interactions with aspects of sustainable development,
- finding methods to quantify effects of the ICT life cycle, of ICT applications and the way ICT changes societal structures (including the economic system), and finally,
- embedding these analyses in an organizational or political context of decision-making and in a societal discourse.

We hope that Track 4 "ICT and sustainable development" of the 9th Conference on Human Choice and Computers (HCC9), embedded in the 2010 IFIP World Computer Congress in Brisbane, Australia, will be a milestone in meeting these challenges.

Acknowledgments. As track programme chairs, we thank all the programme committee members for their efforts in supporting the organisation of this track. In this respect, we would especially like to acknowledge the following for their intellectual and organisational inputs: Gunilla Bradley, Katharina Bunse, Vlad Coroama, Lorenz Erdmann, Wolfgang Hofkirchner, John Houghton, Shirin Madon, Scott Matthews, Bill McIver, Therese Meier, Andreas Möller, Bernd Page, Thomas Ruddy, and Eric Williams.

References

1. World Commission on Environment and Development: Our Common Future. Oxford University Press, London (1987)
2. United Nations Millennium Ecosystem Assessment (MEA): Ecosystems and Human Well-Being: Synthesis. Island Press, Washington (2005)
3. Hilty, L.M., Ruddy, T.F.: Sustainable Development and ICT Interpreted in a Natural Science Context: the Resulting Research Questions for the Social Sciences. Information, Communication & Society 13(1), 7–22 (2010), http://dx.doi.org/10.1080/13691180903322805
4. Hilty, L.M.: Information Technology and Sustainability. In: Essays on the Relationship between ICT and Sustainability. Books on Demand, Norderstedt (2008), http://www.amazon.de/gp/product/3837019705/
5. Erdmann, L., Hilty, L.M.: Scenario Analysis: Exploring the Macroeconomic Impacts of Information and Communication Technologies on Greenhouse Gas Emissions. Accepted for Publication in the Journal of Industrial Ecology
6. Holvast, J., Duquenoy, P., Whitehouse, D.: The Information Society and its Consequences: Lessons from the Past. In: Berleur, J., Avgerou, C. (eds.) Perspectives and Policies on ICT in Society – An IFIP TC9 (Computers and Society) Handbook, pp. 135–152. Springer, New York (2005)

7. Zuccato, A., Fischer-Hübner, S.: Symbolic and Structuring Effects of the Internet on Privacy. In: Berleur, J., Avgerou, C. (eds.) Perspectives and Policies on ICT in Society – An IFIP TC9 (Computers and Society) Handbook, pp. 219–237. Springer, New York (2005)
8. Ruddy, T.F., Hilty, L.M.: Impact Assessment and Policy Learning in the European Commission. Environmental Impact Assessment Review 2-3(28), 90–115 (2008), http://dx.doi.org/10.1016/j.eiar.2007.05.001
9. Köhler, A., Erdmann, L.: Expected Environmental Impacts of Pervasive Computing. Human and Ecological Risk Assessment 10, 831–852 (2004)
10. Williams, E.: Energy intensity of computer manufacturing: hybrid assessment combining process and economic input-output methods. Environmental Science and Technology 38(22), 6166–6174 (2004)
11. Frischknecht, R., Jungbluth, N., Althaus, H.J., et al.: The Ecoinvent Database: Overview and Methodological Framework. International Journal of Life Cycle Assessment 10, 3–9 (2005)
12. Scharnhorst, W., Hilty, L.M., Jolliet, O.: Life Cycle Assessment of Second Generation (2G) and Third Generation (3G) Mobile Phone Networks. Environment International 32, 656–675 (2006)
13. Widmer, R., Oswald-Krapf, H., Sinha-Khetriwal, D., et al.: Global Perspectives on e-Waste. Environmental Impact Assessment Review 25, 436–458 (2005)
14. Hilty, L.M.: Electronic waste – an emerging risk? Environmental Impact Assessment Review 25(5), 431–435 (2005)
15. Kräuchi, P., Wäger, P., Eugster, M., Grossmann, G., Hilty, L.M.: End-of-life impacts of pervasive computing. IEEE Technology and Society Magazine 24(1), 45–53 (2005)
16. Dick, M., Naumann, S., Kuhn, N.: A Model and Selected Instances of Green and Sustainable Software. In: Berleur, J., Hercheui, M., Hilty, L.M. (eds.) HCC9/CIP 2010. IFIP AICT, vol. 328, pp. 248–259. Springer, Heidelberg (2010)
17. Houghton, J.W.: ICT and the Environment in Developing Countries: A Review of Opportunities and Developments. In: Berleur, J., Hercheui, M., Hilty, L.M. (eds.) HCC9/CIP 2010. IFIP AICT, vol. 328, pp. 236–247. Springer, Heidelberg (2010)
18. Bunse, K., Vodicka, M.: Managing Energy Efficiency in Manufacturing Processes – Implementing Energy Performance in Production Information Technology Systems. In: Berleur, J., Hercheui, M., Hilty, L.M. (eds.) HCC9/CIP 2010. IFIP AICT, vol. 328, pp. 260–268. Springer, Heidelberg (2010)
19. Santana, F.S., Barberato, C., Saraiva, A.M.: A Reference Process to Design Information Systems for Sustainable Design based on LCA, PSS, Social and Economic Aspects. In: Berleur, J., Hercheui, M., Hilty, L.M. (eds.) HCC9/CIP 2010. IFIP AICT, vol. 328, pp. 269–280. Springer, Heidelberg (2010)
20. Möller, A., Rolf, A.: IT Support for Sustainable Development in Organizations. In: Berleur, J., Hercheui, M., Hilty, L.M. (eds.) HCC9/CIP 2010. IFIP AICT, vol. 328, pp. 281–291. Springer, Heidelberg (2010)
21. Dompke, M., von Geibler, J., Göhring, W., Herget, M., Hilty, L.M., Isenmann, R., Kuhndt, M., Naumann, S., Quack, D., Seifert, E.K.: Memorandum Nachhaltige Informationsgesellschaft. Fraunhofer IRB, Stuttgart (2004)
22. Göhring, W.: The Memorandum Sustainable Information Society. In: Proceedings 18th International Conference Informatics for Environmental Protection, EnviroInfo 2004, Geneva (2004), http://www.wolf-goehring.de/OverMemoSIS.pdf

23. Isenmann, R.: Sustainable Information Society. In: Quingley, M. (ed.) Encyclopedia of Information Ethics, pp. 622–630. IGI Global, Hershey (2008)
24. Streicher-Porte, M., Marthaler, C., Böni, H., Schluep, M., Camacho, A., Hilty, L.M.: One laptop per child, local refurbishment or overseas donations? Sustainability assessment of computer supply scenarios for schools in Colombia. Journal of Environmental Management 90(11), 3498–3511 (2009)
25. Dobson, J., Duncombe, R., Nicholson, B.: Utilising the Internet to improve peasant artisan incomes: Evidence from Mexico. In: Berleur, J., Hercheui, M., Hilty, L.M. (eds.) HCC9/CIP 2010. IFIP AICT, vol. 328, pp. 292–309. Springer, Heidelberg (2010)

ICT and the Environment in Developing Countries: A Review of Opportunities and Developments

John W. Houghton

Centre for Strategic Economic Studies
Victoria University, Melbourne, Australia
john.houghton@vu.edu.au

Abstract. Both developed and developing countries face many environmental challenges, including climate change, improving energy efficiency and waste management, addressing air pollution, water quality and scarcity, and loss of natural habitats and biodiversity. Drawing on the existing literature, this paper explores how the Internet and ICT can help tackle environmental challenges in developing countries through more environmentally sustainable models of economic development and environmentally friendly technologies and applications. This review focuses on the role of ICTs in climate change mitigation, mitigating other environmental pressures and climate change adaptation, providing an overview and pointing to examples of current activities and opportunities in each of these areas.

Keywords: Information and Communication Technology (ICT), The Environment, Climate Change, Mitigation, Adaptation, Developing Countries, Sustainable Development.

1 ICT and the Knowledge Economy

A major feature of the knowledge economy is the impact that ICTs have had on industrial structure, with a rapid growth of services and a relative decline of manufacturing. Services are typically less energy intensive and less polluting, so among those countries with a high and increasing share of services, we often see a declining energy intensity of production – with the emergence of the Knowledge Economy ending the old linear relationship between output and energy use and partially de-coupling growth and energy use.

Traditional development models have focussed on a shift from agriculture to manufacturing, the development of free markets, encouraging exports and industrialisation in labour-intensive consumer goods – a model borne out in The East Asian Miracle [1] and the emergence of China as the World's largest exporter of ICT and related consumer equipment. Sheehan suggests a re-think, based on the evidence from the emergence of India [2]. Looking at long-term trends in employment and sectoral GDP shares and growth rates, he suggests that India provides an example of a 'big-push' development driven by services. India's services sector now accounts for some 60% of GDP and has been twice as large as the industrial sector for more than 50

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 236–247, 2010.

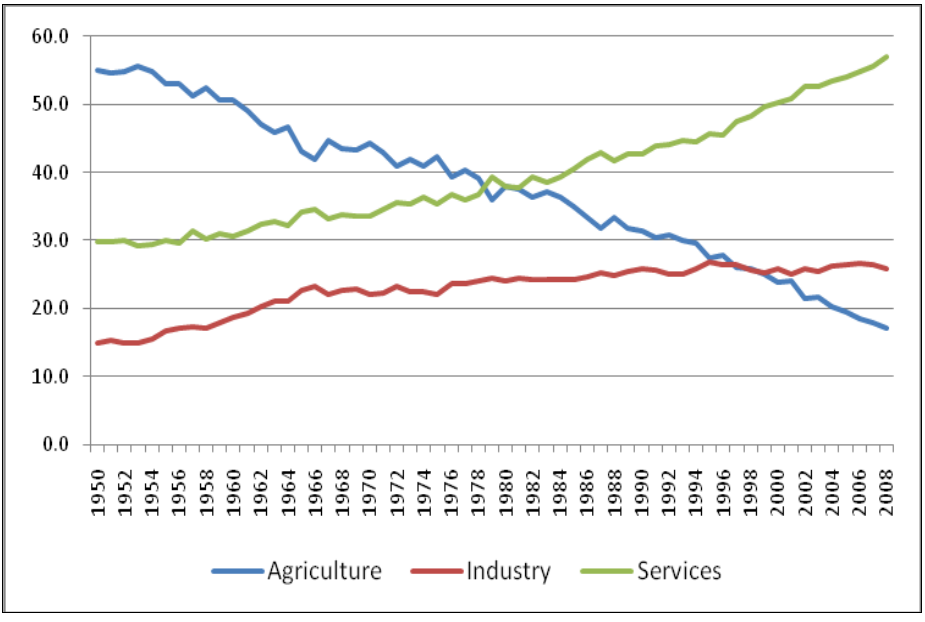


Fig. 1. Value added shares by sector, India 1950–51 to 2007–08 [4]

years. India's CO_2 intensity per unit of GDP is substantially lower than is typical of developing countries, comparable to that of Japan and lower than Germany's [3].

ICTs have played a key role in making services tradeable and the globalisation of IT and IT-enabled services. Looking at the intensity of IT and IT enabled services exports, Houghton and Welsh note that in only three countries did computer and information services account for more than 25% of total services exports during 2006 – India, where they accounted for almost 40% (down from 50% in 2004), Ireland 31% (down from 39% in 2004), and Israel 27% [5]. Their analysis suggests that IT and IT-enabled services exports can play an important role in a wide range of developed, emerging and developing economies, and may in the latter provide the basis for a more environmentally sustainable development path than has characterised industrialisation in the past.

Assessing the possibility of alternative development pathways, Berkhout *et al*. argue that the convergence of economic structures and growth rates, which plays such a central role in growth theories, does not imply that the emergence of socio-technical systems underpinning growth must also be convergent in terms of their technological composition and environmental quality, and they call for greater attention to the resource and environmental quality of development as the basis of more sustainable development pathways [6, 7].

2 ICT and the Environment

The relationship between ICTs and the environment is complex, as ICTs can play both positive and negative roles. Positive impacts can come from dematerialization

and online delivery, transport and travel substitution, a host of monitoring and management applications, greater energy efficiency in production and use, and product stewardship and recycling. Negative impacts can come from energy consumption and the materials used in the production and distribution of ICT equipment, energy consumption in use directly and for cooling, short product life cycles and e-waste, and exploitative applications (*e.g.* remote sensing for unsustainable fishing [8]).

The impacts of ICT on the environment can be direct (*i.e.* the impacts of ICTs themselves, such as energy consumption and e-waste), indirect (*i.e.* the impacts of ICT applications, such as intelligent transport systems, buildings and smart grids), or third-order and rebound (*i.e.* the impacts enabled by the direct or indirect use of ICTs, such as greater use of more energy efficient transport). Exactly what the impacts of ICT are, and to what extent there may be rebound effects, are widely discussed topics. However, it is clear that attempts to measure the impacts of ICT on the environment should take account of the potential rebound effects and the entire life cycle, rather than just the direct impacts of the product or application itself [9, 10, 11].

Estimates of the direct impacts of the ICT industries vary with the definition of the industry and coverage of ICT-related energy uses, but the production and use of ICT equipment is estimated to be equivalent to 1% to 3% of global CO_2 emissions (including embedded energy) and a higher and growing share of electricity use. In 2006, it was estimated that ICT equipment (excluding broadcasting) contributed around 2% to 2.5% of worldwide Greenhouse Gas (GHG) emissions – 40% of this was reported to be due to the energy requirements of PCs and monitors, 23% to data centres, 24% to fixed and mobile telecommunications, and 6% to printers [12]. More recent life cycle assessments produce broadly similar results [13]. Data centres are a particular focus, and Koomey estimated that worldwide electricity use for servers doubled between 2000 and 2005, and he suggested that consumption would increase by a further 40% by 2010 [14].

Nevertheless, the indirect enabling impacts of ICTs are greater, and a number of studies have identified potentially significant net positive impacts from ICTs. For example, The Climate Group identified key areas of enabling impacts potentially leading to global emissions reductions by 2020 that were five times the ICT sector's direct footprint [15]. This paper explores some examples of the role ICTs play in climate change mitigation, mitigating other environmental pressures, and climate change adaptation.

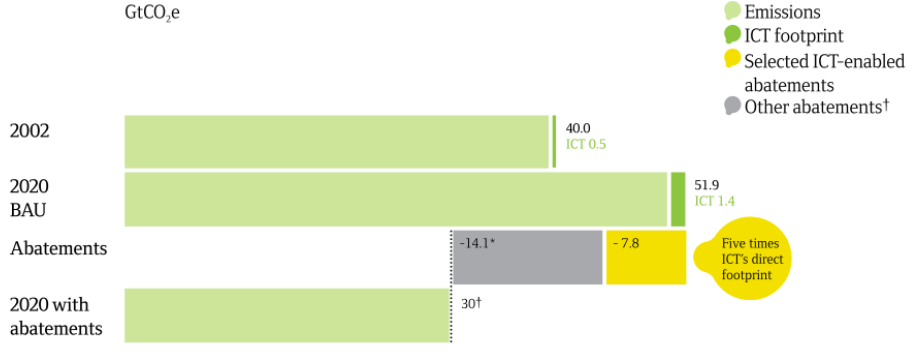


Fig. 2. ICT Impact: The global footprint and the enabling effect [16]

2.1 Mitigation: Avoiding the Unmanageable

Mitigation activities are directed at reducing the adverse impacts of climate change on the environment and are crucial to meeting emissions targets. Such activities can be focused on mitigating climate change directly or at a range of other environmental effects (*e.g.* water availability and salinity, desertification and deforestation).

2.1.1 Climate Change Mitigation

There are many studies and reports identifying areas in which ICTs can have a major impact on the environment, with a number identifying the energy efficiency in buildings and transport rationalization and substitution through dematerialisation, tele- and video-conferencing and tele-work as the major areas of impact based on sectoral energy use shares and trends, as well as application opportunities [17].

Developing and emerging economies face many challenges in the provision of infrastructures as economic growth progresses, with rapidly increasing demand for reliable electricity supply, transport infrastructures and commercial buildings. The very difficulties faced in meeting rapidly growing demands can, and are, driving investments towards more energy efficient solutions. The Climate Group cited a number of examples [18].

***Energy infrastructure*:** Smart Grids entail the modernisation of electricity distribution networks through the introduction of ICT and sensing network technologies. Smart grids enable improved monitoring and control of the energy network as a supply chain, which means reductions in energy losses, greater network operational efficiency, better quality and reliability of energy supply, greater customer control of their energy use, better management of highly distributed sources of energy generation (*e.g.* greater solar and wind generation), and reductions in greenhouse gas emissions. Smart meters add the possibility of two-way communication and supply between providers and users [19] and play a vital role in making energy and environmental issues visible to the household consumer, thereby informing and empowering consumers and enabling behavioural change.

Electricity generation capacity limitations and grid transmission and distribution losses are driving 'smart grid' developments in India and China which are both improving energy use efficiency and reducing the rate of expansion of what are largely coal-fired electricity generation systems. Electricity generation accounts for 57% of India's total emissions and with rapidly increasing demand those emissions are forecast to increase by 4% per annum, twice the global average. But, it is estimated that as much as 32% of generated power is lost along the grid [20].

With infrastructure investments for the next 20-30 years now taking place, there is an opportunity to 'leapfrog' to smart grid systems, to reduce power losses and outages and realise greater energy efficiency, and Indian distributors are looking to smart grid investments (*e.g.* North Delhi Power). However, rebound effects are likely to be greater in developing countries where demand is far from saturated [21], so market and price signals will be particularly important.

***Motor systems*:** Motor systems convert electricity into mechanical power, and while invisible to most of us they are crucial to the manufacturing sector's energy use.

Motors can be inefficient if they operate at full capacity, regardless of load. A motor is 'smart' when it can be controlled to adjust its power usage to a required output through a variable speed drive and intelligent motor controller. It is estimated that the motor systems in operation in China use 70% of total industry electricity consumption and are 20% less energy efficient than those in Western countries. By 2020, industrial motor systems in China will be responsible for an estimated 34% of power consumption and 10% of carbon emissions, or 1-2% of global emissions. Industrial energy use in China could be reduced by 10% by improving the efficiency of motor systems, as motor system optimisation alone could reduce China's emissions by 200 $MtCO_2e$ by 2020 – comparable to total 2006 emissions from the Netherlands [22]. Recognising the potential, China's government has implemented the *China Motor Systems Energy Conservation Program* to help reach its energy efficiency targets. It is unlikely that the necessary investments would be made without such initiatives.

***Buildings*:** Energy consumption in buildings is driven by two factors – energy intensity and surface area. ICT-based monitoring, feedback and optimisation tools can be used to reduce both at every stage of a building's life cycle, from design and construction to use and demolition. Energy modelling software can help architects determine how design influences energy use. Builders can use software to compare energy models with actual construction. Once the building is complete, ICT can measure and benchmark its performance and compare actual to predicted energy efficiency. Occupants can install a building management system (BMS) to automate building functions such as lighting, heating and cooling and if a building undergoes a change of use, ICT can be used to redesign its energy model and measure the impacts of this change. It has been estimated that such tools could reduce the emissions from buildings by 15% by 2020 [23]. Building standards and regulation are crucial elements in achieving such savings.

***Transport*:** Globalisation has led to increasingly complex international supply chains and brings with it challenges for transport, storage and logistics operations. ICT can improve the efficiency of logistics operations in a number of ways. These include software to improve the design of transport networks, allow the running of centralised distribution networks and management systems that can facilitate flexible home delivery services. Specific levers include inter-modal shift, route optimisation and inventory reduction. The transport sector is a large and growing emitter of GHGs, responsible for 14% of global emissions, and it is estimated that optimising logistics using ICT could result in a 16% reduction in transport emissions and a 27% reduction in storage emissions globally [24]. Many policy and regulatory issues influence transport and logistics, from airline route regulation, to building planning and regulation, and noise and pollution regulations relating to transport [25], presenting a major challenge for policy coherence.

2.1.2 Mitigating Other Environmental Pressures

Emerging and developing economies are often dependent on agriculture and fishing for both cash crops and subsistence, and water can be a more pressing issue in emerging and developing economies than is energy use. Deforestation can also be a major concern in some regions. Hence, mapping, monitoring and managing lands, forests

and waterways are crucial to the efficiency and sustainability of key sectors. Geographic Information Systems (GIS) provide major opportunities in land and waterway monitoring and management in Egypt [26], Africa and across South East Asia and the Himalayan region [27]. As elsewhere, information is the key to enabling people to make more sustainable choices and realise benefits from their actions, as well as for education, awareness and support.

Observational data are increasingly available to users around the world through a range of portals and systems, allowing for environmental observation and prediction. Examples include the Earth Observation Portal [28] and Climate Change Prediction Net [29], while conservation is the focus of the Society for Conservation's portal [30]. There is an increasing tendency to make geo-spatial environmental information more readily available through the use of common interfaces, such as Google Earth and Microsoft's Virtual Earth. This enables information holders to make geo-specific information available to users through a standard web interface at very low cost. Examples include: The Tropical Ecology Assessment and Monitoring Network [31], Atlas of Our Changing Environment [32], Climate Change in Our World [33], and others [34].

On the ground in emerging and developing countries there are a number of examples of how cellular mobile phones and wireless networks can provide a leapfrogging opportunity where fixed line networks are rudimentary or simply do not exist. Noting that agriculture is the mainstay of the Kenyan economy, Mungai provided a number of examples relating to mitigation, such as the SokoniSMS service, which enables farmers to receive market prices in various market centres through their mobile phones [35, 36] Equipped with this information, the farmers are able to determine the most profitable market to transport products to, circumventing middlemen who usually offer to buy the products at much lower prices and reducing the tendency to transport goods from market to market in search of buyers. Other initiatives include the use of geographical information systems in the Lake Victoria basin [37] and along the Nile basin [38] to support natural resource management and local development. These systems can be supplemented by location or eco-system specific information kits, such as The Mekong and Nile River Awareness Kits [39]. Integrated eco-system monitoring, sensing and modelling is also increasingly common (*e.g.* The Pearl River Delta [40]).

Noting the vulnerabilities of rural communities in South East Asia and the Himalayan regions, their dependence of eco-systems and pressures from unsustainable use and over use, Tyler and Fajber noted the importance of access to information and a number of innovative projects [41]. For example:

- In Indonesia, Bogor Agricultural University is working with farmers to use climate forecasts through climate field schools, and when seasonal forecasts suggested a drier than normal crop season in 2006-07, farmers stored a larger proportion of their first rice crop in anticipation of higher prices due to dry conditions for the second crop.
- In the Philippines, the Manila Observatory (MO) has partnered with SMART, one of the country's mobile phone service providers, for a pilot project providing telemetric rain gauges and phones in disaster-prone areas. Local farmers read the rain gauges and phone the information to the Observatory, while the Observatory can also use the phones to issue early

warning of storms to the farmers. In addition, the farmers can use the phones to access market information.

There are also many examples of supporting information networks (see below).

2.2 Adaptation: Managing the Unavoidable

Adaptation refers to actions designed to reduce the negative impacts of climate change that are already occurring. Unfortunately, the most vulnerable are at most risk, and for the developing world it is the role that ICTs can play in climate change monitoring and adaptation that is likely to be most important [42]. Examples of adaptation include preparing risk assessments, protecting ecosystems, improving agricultural methods, managing water resources, instituting better building designs and building settlements in safe zones, developing early warning systems, improving insurance coverage and developing social safety nets [43, 44].

2.2.1 Climate Change Adaptation

Monitoring and providing early warning of climate change induced events, such as storm and tsunami, drought and flood, famine and disease, play a vital role. Examples at the international level include:

- The *Famine Early Warning Systems Network (FEWS NET),* a USAID-funded network that brings together international, regional and national partners to provide early warning and vulnerability information on emerging and evolving food security issues. FEWS NET professionals in Africa, Central America, Haiti, Afghanistan and the United States monitor and analyse climate information for potential impacts on livelihoods and markets to identify potential threats to food security. Once identified, FEWS NET uses a suite of communications and decision support technologies to help decision makers act to mitigate food insecurity. These include monthly food security updates for 25 countries, regular food security outlooks and alerts, as well as briefings and support to contingency and response planning efforts [45].
- *Distant Early Warning System for Tsunami (DEWS)* is a tsunami warning system for the Indian Ocean, which aims to create a new generation of interoperable tsunami early warning systems based on an open sensor platform, which integrates sensor systems for the rapid detection of earthquakes, for the monitoring of sea level, ocean floor events, and ground displacements. Tsunami warnings can be sent via SMS to mobile cellular phones, by facsimile or as a television overlay [46].
- *PreventionWeb* serves the information needs of the disaster risk reduction (DRR) community, including the development of information exchange tools to facilitate collaboration, providing a common platform for the disaster risk reduction community to find and share DRR information, exchange experience, connect and collaborate [47].

Another area in which the use of ICTs supports adaptation is that of climate and impact models, which can be used to inform practitioners and decision makers in

planning as well as predicting the impacts of climate change on agriculture (*e.g.* combined with crop models). SEI cite a number of examples [48] including:

- A South African study undertaken by the University of Pretoria that focused at the provincial level and found a significant correlation between higher historical temperatures and reduced dryland staple production, and forecast a fall in net crop revenues by as much as 90% by 2100.
- A Nigerian study that applied the EPIC crop model to give projections of crop yield during the 21st century. The study modelled worst case climate change scenarios for maize, sorghum, rice, millet and cassava, and found that there will be increases in crop yield across all low land ecological zones as the climate changes during the early parts of the 21st century, but towards the end of the century the rate of increase will tend to slow down.
- An Egyptian study that compared crop production under current climate conditions with those projected for 2050, and forecast a decrease in national production of many crops, ranging from -11% for rice to -28% for soybeans.
- A study that mapped climate vulnerability with a focus on the livestock sector and identified arid and semi-arid rangeland and the drier mixed agro-ecological zones across the African continent, particularly in Southern Africa and the Sahel, and coastal systems in East Africa as being particularly prone to climate change [49].

Similarly, ICRISAT's integrated climate risk assessment and management system uses remote sensing and GIS techniques to study rainfall patterns and prepare advisories for farmers in drylands of Asia and sub-Saharan Africa [50].

Having identified areas of vulnerability, ICTs enable a range of responses, with information networks playing a crucial role. There are many examples:

- *The Arid Lands Information Network (ALIN)* states that its strategy is informed by the belief that knowledge is a source of competitiveness, where value lies in new ideas, practices, information on opportunities and new technologies as drivers of this process; that knowledge improves lives, reduces poverty and empowers people; that access to knowledge is fundamental to development and progress; and that ICTs are key for enabling access to knowledge. ALIN provides an information sharing forum that helps people to adjust to climate change [51].
- *RANET* uses radio and the Internet for the communication of hydrometeorological information for rural development, and includes the use of SMS emergency altering systems and community-based weather observation [52].
- *The Open Knowledge Network (OKN)* and *openeNRICH* also provide regular information relating to climate change adaptations, such as the recent exchange "Climate change increases food insecurity in Kyuso, Kenya" (09-07-2009) [53].
- Focusing on mountain regions the *Mountain Forum* and its regional partners provide information to enable residents of mountain regions to adapt to climate change (*e.g.* Climate Change and the Himalayas [54]) [55].

Periodicals, such as I4D [56], telecentre magazine [57], newsfordev [58], World-changing [59] provide many examples, and a number of international ICT4D agencies operate environment related programs (*e.g.* IICD [60]). Links and overviews can be seen through such sites as scidevnet [61] km4dev [62] and t4cd [63].

3 Summary and Conclusions

ICTs are all but ubiquitous and the potential uses and impacts of ICTs on the environment in emerging and developing economies are many and varied. No short paper can cover all aspects, and this paper does no more than provide examples. However, it is possible to note some of the key areas of impact and potential in more general terms, highlighting some of the major policy issues arising for both developed and developing countries.

Specific applications with particular relevance to emerging and developing economies include: detection and early warning (*e.g.* storm, flood, earthquake and tsunami warning); energy efficiency applications (*e.g.* intelligent building systems, intelligent transport systems, smart grids and home automation); and information, education and capability building (*e.g.* technology awareness and transfer, public education and support).

Key issues for emerging and developing economies include: access to infrastructure and ways to enable investments in smarter greener energy, transport and building infrastructures, as well as access to the broadband networks and ICT equipment and services necessary to enable their operation; access to data and how the masses of data collected can be brought together to provide a holistic picture of an eco-system or environment (*i.e.* who owns the data, who can use it and what can it be used for?); affordability and how emerging and new technologies can be implemented in contexts of severe budgetary constraint; and capability and how the necessary skills can be brought to bear on environmental issues in developing and emerging economies.

Areas for concern for developing and emerging economies include: understanding life cycle impacts in the many different contexts and circumstances that exist in developing and emerging economies, while operating within the constraints of available data (*e.g.* insufficient national statistical collections to support input-output analysis and life cycle assessments); managing possible rebound effects, which are likely to be greater in rapidly growing markets where there is unmet demand for energy and resources [64], and the related difficulties of establishing an equitable international price for carbon and regulating for appropriate price signals; and ensuring that there is sufficient technology transfer and enabling funding flows to emerging and developing countries.

Fundamentally, ICTs are about information and communication, and it is these roles that are vital. Data must be collected, analysed and interpreted, transformed into information that enables individuals to make smarter greener choices, and communicated to individuals in such a way as to inform and educate, influence and change behaviours. It is not simply a matter of price signals shaping behaviour, even if it were possible to get those signals right, but also about informing, monitoring performance and providing non-price feedback in such a way as to motivate and reward individuals and communities for creating sustainable livelihoods.

References

1. World Bank: The East Asian Miracle: Economic growth and public policy. The World Bank, Washington DC (1993), http://www.worldbank.org/
2. Sheehan, P.J.: Beyond Industrialization: New Approaches to Development Strategy Based on the Services Sector. UNU-WIDER Research Paper 2008/60: Helsinki (2008), http://www.wider.unu.edu/publications/working-papers/research-papers/2008/en_GB/rp2008-60/
3. Ghosh, P.: The climate change debate: The story from India. In: A Taxing Debate: Climate Policy Beyond Copenhagen, CEDA, Melbourne (2009), http://www.ceda.com.au/public/publications/growth/growth_61.html
4. Sheehan, P.J.: Beyond Industrialization: New Approaches to Development Strategy Based on the Services Sector, UNU-WIDER Research Paper 2008/60: Helsinki (2008)
5. Houghton, J.W., Welsh, A.: Australian ICT Trade Update 2009. Australian Computer Society, Sydney (2009), http://www.cfses.com
6. Berkhout, F., Angel, D., Wieczorek, A.J.: Asian development pathways and sustainable socio-technical regimes. Technological Forecasting and Social Change 76, 218–228 (2009)
7. Berkhout, F., Angel, D., Wieczorek, A.J.: Sustainability transitions in developing Asia: Are alternative development pathways likely? Technological Forecasting and Social Change 76, 215–217 (2009)
8. Daly, J.: ICT and Ensuring Environmental Sustainability, Development Gateway (dgCommunities) (2003), http://topics.developmentgateway.org
9. Plepys, A.: The grey side of ICT. Environmental Impact Assessment Review 22, 509–523 (2002)
10. Yi, L., Thomas, H.R.: A review of research on the environmental impact of e-business and ICT. Environment International 33, 841–849 (2007)
11. Hilty, L.M.: Information Technology and Sustainability: Essays on the relationship between information technology and sustainable development. Books on Demand, Norderstedt (2008)
12. Kumar, R., Mieritz, L.: Conceptualizing Green IT and data center power and cooling issues, Gartner Research Paper (2007), http://www.gartner.com/DisplayDocument?id=519717
13. Malmodin, J.: Life cycle assessments of ICT. In: OECD Conference on ICTs, the environment and climate change, Helsingor (2009), http://itst.media.netamia.net/ict2009/video.php?tab=demand
14. Koomey, J.: Estimating total power consumption by servers in the U.S. and the world. Analytics Press, Oakland (2007), http://enterprise.amd.com/Downloads/svrpwrusecompletefinal.pdf
15. The Climate Group: SMART 2020: Enabling the low carbon economy in the information age, London (2008), http://www.smart2020.org/
16. The Climate Group: SMART 2020: Enabling the low carbon economy in the information age, London (2008), http://www.smart2020.org/
17. Climate Risk. Towards a High-Bandwidth, Low-Carbon Future: Telecommunications-based opportunities to reduce greenhouse gas emissions, Climate Risk, Sydney (2008), http://www.climaterisk.com.au
18. The Climate Group: SMART 2020: Enabling the low carbon economy in the information age, London (2008), http://www.smart2020.org/

19. Access Economics. The economic benefits of intelligent technologies, Access Economics, Canberra (2009), http://www.accesseconomics.com.au/
20. The Climate Group: SMART 2020: Enabling the low carbon economy in the information age, London (2008), http://www.smart2020.org/
21. Sorrell, S.: The Rebound Effect: An Assessment of the Evidence for Economy-wide Energy Savings from Improved Energy Efficiency, UKERC (2007)
22. The Climate Group: SMART 2020: Enabling the low carbon economy in the information age, London (2008), http://www.smart2020.org/
23. The Climate Group: SMART 2020: Enabling the low carbon economy in the information age, London (2008), http://www.smart2020.org/
24. The Climate Group: SMART 2020: Enabling the low carbon economy in the information age, London (2008), http://www.smart2020.org/
25. Houghton, J.W.: Digital Delivery in Distribution and Logistics. OECD, Paris (2005)
26. IISD: A Developing Connection: Bridging the Policy Gap Between the Information Society and Sustainable Development, IISD, Winnipeg (2005), http://www.iisd.org/publications/pub.aspx?pno=740
27. IISD: Land and Water Resource Management in Asia: Challenges for climate adaptation, IISD, Winnipeg (2009), http://www.iisd.org/climate/
28. http://www.eoportal.org/
29. http://www.climateprediction.net/
30. http://www.scgis.org/
31. http://www.teamnetwork.org
32. http://na.unep.net/digital_atlas2/google.php
33. http://earth.google.co.uk/outreach/kml_entry.html#tClimate%20Change%20In%20Our%20World
34. http://earth.google.co.uk/outreach/kml_listing.html#cenvironment%20science#s1#e20
35. Mungai, W.: Using ICTs for Poverty Reduction and Environmental Protection in Kenya. In: IISD A Developing Connection: Bridging the Policy Gap Between the Information Society and Sustainable Development. IISD, Winnipeg (2005), http://www.iisd.org/publications/pub.aspx?pno=740
36. http://www.gkpnet.org/projects/public/ict4dinitiatives/view.do?gkpprojectid=32600
37. Mungai, W.: Using ICTs for Poverty Reduction and Environmental Protection in Kenya. In: IISD A Developing Connection: Bridging the Policy Gap Between the Information Society and Sustainable Development. IISD, Winnipeg (2005), http://www.iisd.org/publications/pub.aspx?pno=740
38. Sobeih, M.: Geographic Information Systems (GIS) in Egypt. In: IISD A Developing Connection: Bridging the Policy Gap Between the Information Society and Sustainable Development. IISD, Winnipeg (2005), http://www.iisd.org/publications/pub.aspx?pno=740
39. http://www.mrcmekong.org/, http://www.nileteap.org/nrak/
40. Chan, E.: Dealing with the environmental problems of The Pearl River Delta Region with ICTS. In: OECD Conference on ICTs, the Environment and Climate Change, Helsingor (2009), http://itst.media.netamia.net/ict2009/video.php?tab=demand
41. Tyler, S., Fajber, L.: Land and Water Resource Management in Asia: Challenges for climate adaptation, IISD, Winnipeg (2009), http://www.iisd.org/climate/
42. InfoDev: ICTs and Climate Change. infoDev (2009), http://www.infodev.org/

43. ISDR: Climate Change and Disaster Risk Reduction. UN/ISDR, Geneva (2008), http://www.unisdr.org/
44. ITU: ICTs for e-Environment: Guidelines for developing countries, with a focus on climate change. ITU, Geneva (2008), http://www.itu.int/themes/climate/
45. http://www.fews.net
46. http://www.dews-online.org
47. http://www.preventionweb.net/
48. SEI: Climate Change and Adaptation in African Agriculture. SEI, Stockholm (2008), http://www.sei.se
49. Thornton, P.K., Jones, P.G., Owiyo, T., Kruska, R.L., Herrero, M., Kristjanson, P., Notenbaert, A., Bekele, N., Omolo, A.: with contributions from Orindi V., Otiende B., Ochieng A., Bhadwal S., Anantram K., Nair S., Kumar V., Kulkar U.: Mapping climate vulnerability and poverty in Africa, Report to the Department for International Development. ILRI, Nairobi, Kenya (2006)
50. http://www.icrisat.org/
51. http://www.alin.or.ke/
52. http://www.ranetproject.net/
53. http://196.201.231.147/eNRICH/viewContentItem.do?View=viewItem&itemid=137921&ptltid=302
54. http://www.icimod.org/home//pub/publications.content.php?puid=126
55. http://www.mtnforum.org/index.cfm, http://www.mtnforum.org/rn/index.cfm
56. http://www.i4donline.net/articles/current-article.asp?articleid=1910&typ=Features
57. http://www.telecentremagazine.net/
58. http://www.newsfordev.org/index.html
59. http://www.worldchanging.com/
60. http://www.iicd.org/sectors/environment
61. http://www.scidev.net/en/climate-change-and-energy/
62. http://www.km4dev.org/
63. http://www.t4cd.org/
64. Sorrell, S.: The Rebound Effect: An Assessment of the Evidence for Economy-wide Energy Savings from Improved Energy Efficiency. UKERC (2007)

A Model and Selected Instances of Green and Sustainable Software

Markus Dick, Stefan Naumann, and Norbert Kuhn

Trier University of Applied Sciences, Umwelt-Campus Birkenfeld, Campusallee,
D-55768 Hoppstädten-Weiersbach, Germany
m.dick@umwelt-campus.de, s.naumann@umwelt-campus.de,
n.kuhn@umwelt-campus.de

Abstract. The power consumption of ICT is still increasing. To date it is not clear if the energy savings through ICT overbalance the energy consumption by ICT or not. Where manifold efforts of Green IT address the environmental aspects of sustainability considering computer hardware, there is a lack of models, descriptions, or realizations in the area of computer software. In this paper we present some results that form the basis towards a definition of the term "Sustainable Software", an outline of a process and lifecycle model for "Green and Sustainable Software Engineering", and six concrete instances of this model for practitioners.

Keywords: Sustainable Software, Green Software Engineering, Green IT, Sustainable Development.

1 Introduction

It is well known that global warming, greenhouse gas (GHG) effects, climate change and sustainable development (SD) are key challenges of the 21st century [1]. Information and Communication Technology (ICT) takes an important role within these challenges. On the one hand, ICT can optimize material flows and therefore reduces energy consumption [2]. But ICT itself is consuming more and more energy: the energy consumption of IT especially that of the Web is still increasing [3]. E.g. the estimated power consumption of data centres in the U.S. was increasing from 28 billion kWh in 2000 to 61 billion kWh in the year 2006 [4] and in the world from 58 billion kWh in 2000 to 123 billion kWh in 2005 [5].

Up to now, several publications have examined the relationship between the field of sustainability and ICT. They discuss the impact of ICT on the environment [6] or consider the balance between energy savings and energy consumptions by ICT [7]. Especially, to date it is not clear if energy consumption by ICT is greater or smaller than energy savings by ICT, e.g. via more efficient processes or simulation of scenarios.

In our paper we present an approach for a model of green and sustainable software that tries to handle both challenges: Reducing the energy consumption of ICT itself and using ICT to contribute to other goals of "Sustainable Development". From a

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 248–259, 2010.

theoretical point of view, our approach can be classified into a new research field called "Sustainability Informatics" [8].

2 What Is Sustainable Software?

As a first step on our way to a general definition of the term “Sustainable Software”, we interviewed five lecturers and practitioners of computer science and asked them about their understanding of Sustainable Software. Of course, this sample size is too small for a substantial analysis, however it gives some good indications of what Sustainable Software might be. The answers lead to the following categories that sharpen the picture towards a definition: software design and programming, need-based development, project management, special features, possible applications, and resource saving.

The category “software design and programming” subsumes software quality aspects that comply with software quality needs according to ISO/IEC 25000 [9], like e.g. portability, reusability, extensibility, adaptability, modularization, documentation, or readable source code which makes future extensions of software products easier and less error-prone, but also an expected long physical life time. Modularization depends directly on the need to deliver only those functions that are necessary for a user. Another point is the possibility of making software products comparable with respect to sustainability e.g. power consumption or resource efficiency during runtime. This may be accomplished through an eco-label similar to the EU energy label [10].

The category “need-based development” subsumes efficiency criteria like processing time, memory requirements and network load which are also quality needs as already mentioned above. Some interviewees addressed the function-richness of modern standard software like e.g. text processors. Standard users rarely tap the full potential of such applications. Thus, sustainable software should only be delivered with functions that are used by a specific user.

The category “project management” addresses distributed software development, supporting paperless offices with document management systems or pursuing company visions that touch sustainability.

The category “special features” contains items like smart techniques and drivers, ergonomic user adjustments or even health promoting interventions. Smart techniques and drivers should anticipate intelligent (and therefore sustainable) user behaviour. Examples are device drivers that do not switch devices on prior to their usage, or printer drivers that ask if two pages should be printed on one sheet of paper when printing in concept or economy mode. An example for a health promoting intervention may be a program that invites users to perform gymnastic exercises when they worked nonstop for some time.

The category “possible applications” addresses the visualization of energy and resource consumption, the reduction of data redundancy, or software that supports the reduction of power and resource consumption indirectly.

Resources can be saved directly and indirectly. The corresponding answers are subsumed under the category “resource saving”. Direct effects mentioned are: alternative data mediums, lower transport and retail packaging efforts or low hardware requirements, so that the software runs even on hardware that is out of date. This means, that new software products should not lead to the need to replace existing

hardware with newer hardware, because of the overall recycling (old hardware) and production (new hardware) expenditure. Indirect effects mentioned are: socially acceptable working conditions, more efficient route planning systems, and more efficient warehouse management systems. More efficient route planning systems can result in lower transport rates and distances and therefore save fossil energy in form of e.g. fuel. Efficient warehouse management systems can lead to smaller warehouses and thus result in fewer sealed surfaces.

These results show that sustainable software focuses not only on a reduction of the consumption of natural resources and energy in the sense of the environmental dimension of sustainability, but also on the social and economic dimensions. This leads to a definition of Sustainable Software as follows:

Definition 1: Sustainable Software is software whose direct and indirect negative impacts on economy, society, human beings, and the environment resulting from development, deployment, and usage of the software is minimal and/or has a positive effect on sustainable development.

This definition and some aspects of the interviews are taken into consideration in order to initially form a model for Green Software Engineering as one part of a model for Sustainable Software Engineering.

3 A Model for Green and Sustainable Software Engineering

The model for Green and Sustainable Software Engineering comprises two general components: the process and lifecycle model, and guidelines and checklists. The model (for an overview see Fig. 1) delimits Green and Sustainable Software Engineering from other software engineering methodologies and includes guidelines and checklists. The process model identifies tasks or activities during a software product's lifecycle, which are relevant for the sustainability valuation of the product. The guidelines and checklists support actors with different professional levels in applying green or sustainable techniques in general when developing, administrating or using software products.

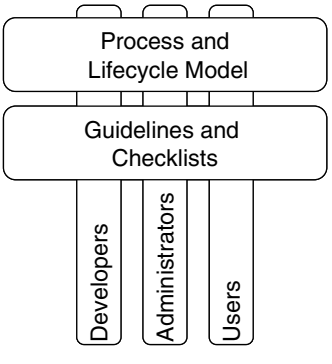


Fig. 1. A model for Green and Sustainable Software Engineering

3.1 Process and Lifecycle Model

The proposed process and lifecycle model is based upon ISO 12207 ("Software life cycle processes") [11] and ISO 14040 ("Life cycle assessment") [12]. Its objective is to provide starting-points for activities that allow an assessment of the sustainability relevant consequences resulting from the usage of the software product during its whole lifecycle (see Fig. 2). These activities are intended to lead to more sustainable software products. The early draft of the model presented below, focuses mainly on the environmental aspects of sustainability. Extensions to the other pillars of sustainability are planned for the future.

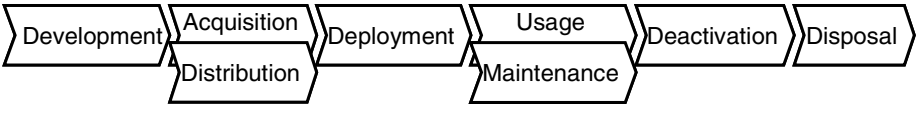


Fig. 2. Process and lifecycle model

The software development processes applied during the *development* lifecycle phase are extended with continuous reflection meetings and assessment activities. These are targeted at assessing direct and indirect environmental impacts, which result from the software development process itself and are expected to arise from the future use of the software product under development. The outcomes of the assessments and reflection meetings should be used to take action towards more sustainable software products e.g. by increasing resource efficiency (which leads possibly to a reduction of the power consumption during program execution), reducing hardware requirements of the software product, avoiding business trips for meeting the development team, or involving prospective users tightly in the development process.

In the next process phase a distinction is drawn between *acquisition* and *distribution*. Here, acquisition means that one evaluates different standard software products, chooses one that fits the needs best and purchases it from a software retailer. A sustainable software selection process should consider selection criteria that take account of direct and indirect impacts on the environment resulting from use of the software product. The acquisition process part can generally be omitted when developing custom software products, because the sustainability aspects that are corresponding to selection criteria can there be considered as software requirements. The distribution process part is relevant for both standard and custom software. Here, it is necessary to consider whether the software product should be delivered as a download or on a physical data medium. If the software is delivered on a data medium, it is also necessary to decide which transport and sales packaging is necessary and justifiable against the background of ecological sustainability. In making the decision, one has to consider the impacts of the corresponding production chains and also the anticipated impacts of the necessary recycling processes. Even though the impacts of recycling/disposal are already considered in the decisions in this phase, the recycling costs themselves, like resource consumption, are assigned to the disposal phase.

The *deployment* lifecycle phase considers aspects that are relevant for administrators during deployment of software products. This includes: data centre virtualization, configuration of the runtime environment necessary to run the software product and

appropriate initial configuration of the software product. These activities do not take effect until the usage phase.

The *usage* and *maintenance* phase considers direct and indirect sustainability effects that evolve from the utilization of the software product. The impact on sustainability that results from this phase, is already considered during the development phase by actors such as the software programmers. In this model, the term "maintenance" does not include the programming activities that are necessary to correct faults after the software product has been delivered. On the contrary, in this context it refers to the support and maintenance offered by administrators to end users, e.g. in organizations which run a data centre. In order to reduce the power consumption of computer systems, users can configure programs, or the energy management of the operating system properly, so that the overall power consumption is minimized. This also includes configuring large caches in web browsers, so that the necessary data transfer, and thus power consumption, is minimized. Another example is the visualization of the energy consumption of working groups, which also has an educational formation effect that is considered to be relevant in developing an awareness of sustainability and ecologically relevant questions. In organizations, where computer users act with low or even no administrational rights on their computer systems, the responsibility to configure the computer systems in an energy conserving way is taken over by the administrators. In organizations that implement service desks according to the IT Infrastructure Library as single points of contact to end users, the mission of the service desks is also to advise the end users proactively [13]. This means that service desks could also advise users proactively on software configurations regarding energy conservation and sustainability issues.

The *deactivation* phase considers aspects that become relevant if software products are taken out of service. An example would be backups of files that have proprietary file formats and can therefore possibly not be processed with newer or competing software products. In this example, one must decide if the old files have to be converted to new data formats, e.g. if copies must be kept due to legal issues, or if the files are obsolete and can therefore be deleted. The deletion of these files releases backup resources, which can be used for other backup purposes and thus save energy and natural resources, because there is possibly no need to buy new backup storages.

The *disposal* phase takes impacts on sustainability into account that result from the disposal of the data medium and packaging. This includes energy and resource consumption that is necessary for recycling. In this phase, no further actions or considerations take place, because the relevant actions and considerations are already taken in the distribution phase. Hence, only the impacts of disposal and recycling are assigned to this phase.

3.2 Guidelines and Checklists

Guidelines and checklists represent the implementable parts of the model and are therefore a constitutive component of it. At large, they are forming an open knowledge base, which enables the consideration of future developments, trends, and

evolving technical expertise. The guidelines and checklists provide tips and helpful hints on how to develop, use, provide, and maintain software products in a sustainable way. Therefore, the guidelines and checklists are aligned to the activities and product scenarios of the lifecycle model described in the preceding section. The knowledgebase should regard the different technical levels of its users according to roles shown in the reference model (see Fig. 1). Appropriate basic roles are: developer, administrator, and user. In order to find the best guidelines and checklists for an actor it is necessary to create specialized roles like: web developer, web author, requirements engineer, software architect etc. as sub roles of the developer role [14].

4 Selected Instances of Guidelines and Software Tools

In the following sections we present six representative instances of our model, realized as software tools or guidelines.

4.1 For Developers

The first two examples are addressing the development lifecycle phase of our model and are thus relevant to developers. Although these examples are applied during the development lifecycle phase, they do not take effect until the usage phase.

Optimization Guideline for Graphical Design Elements in Websites. Today, 54% of an average website is made up of graphics [15]. Hence, optimizing graphical save power because of less network load. Graphical design elements are, unlike photographs or charts, images which are used to design borders, tabs, buttons, or as a logo identifying a company or an organization. In comparison to photographs or charts, graphical design elements are smaller in size and generally have a limited number of colours. This means that reducing the number of colours within an image from RGB living colour to a colour-palette with a limited number of colours reduces the filesize significantly (see Table 1). These images should be saved in the Portable Network Graphics (PNG) format, which, in contrast to the JPEG format, supports indexed palettes. Compared to the GIF format, the PNG format has a better compression algorithm, which results in a smaller filesize [15]. Furthermore it is possible to remove text from a logo. The logo without text is then put as a background image behind the text implemented directly with HTML. In the special example given in table 1, the savings that can be achieved by switching from JPEG to PNG with an indexed palette are for b design elements is a promising way to minimize the transferred data volume and thus oth cases (with text and without text) approx. 84%. Furthermore, the removal of the text results in savings of approx. 50% to 60% in cases of PNG and JPEG. The total saving, when converting from JPEG (with text) to PNG (without text) is approx. 92%. So it is recommended to optimize graphical design elements like those described above, in order to reduce the network load and thus power consumption of a website.

Table 1. Filesizes of a graphical design element (see Fig. 3) in different optimization levels (JPEG files at 85% quality level; all values in bytes)

	File format	RGB living colour	12 colour palette	7 colour palette
Filesize with text	JPEG 85%	8,152	n/a	n/a
	GIF	n/a	2,345	2,248
	PNG	9,036	1,320	1,290
Filesize without text	JPEG 85%	3,895	n/a	n/a
	GIF	n/a	1,528	1,431
	PNG	3,425	666	639

Fig. 3. Left: Logo with RGB living colour; Right: Logo with 7 colour palette without text

Website Optimization Suggestions Integrated in Development Tools. Optimizing the text based source files that make up a website is a promising way to reduce the network load generated by it. One possibility is to minimize CSS files. An exemplary tool that supports minimization is CSSTidy (http://csstidy.sourceforge.net/). It removes unnecessary characters (e.g. whitespaces and line breaks), unnecessary values and attributes (e.g. default values), combines separate single properties to shorthand notations (e.g. margin, border, font), and uses abbreviations. There are many other possibilities to minimize CSS [14].

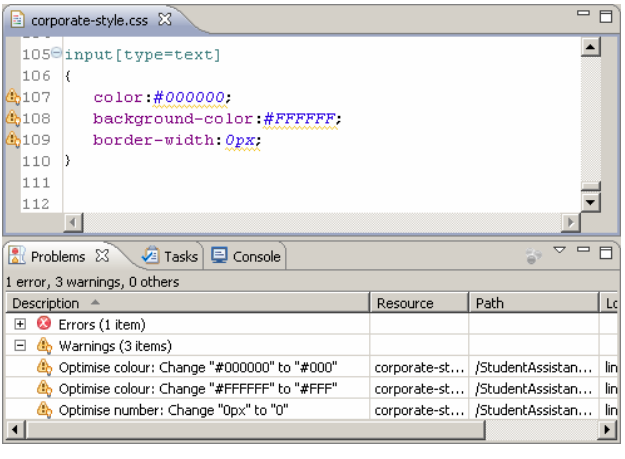


Fig. 4. Integration of network load reducing optimization suggestions for CSS in Eclipse

For web developers, it is not easy to follow all these different suggestions during development. Hence, appropriate situational assistance tools integrated in development environments are essential to simplify matters. Figure 4 depicts our prototypical integration of the above mentioned tool CSSTidy in the well known integrated development environment Eclipse (http://www.eclipse.org). After saving the CSS file under work, the developer gets optimization feedback as warning hints next to the affected code lines. These hints are additionally listed in the problems view, beneath the editor view. In contrast to the original CSSTidy tool that reformats the code of the processed files, our Eclipse Plug-in prototype uses only the processing log output of CSSTidy to generate its hints. Thus developers are free to decide whether or not they want to follow these hints and hence retain full control of the source code.

4.2 For Administrators

The next two examples address the deployment lifecycle phase of our model and therefore are relevant to administrators. Although, the examples are applied during the deployment phase they take effect to ecological sustainability mainly not until the usage and maintenance phase.

Caching and Compression. Today, approx. 80% of the web users have their browsers configured for caching [16]. Therefore supporting the caching strategies of web browsers is ecologically worthwhile, because this will significantly decrease the amount of transferred data and thus power consumption. Since the configuration of the user's web browser cannot be affected by administrators, they have to focus on the server-side configuration aspects of caching. Caching in HTTP/1.1 is designed to reduce the need to send requests to servers (expiration mechanism) and the need to send full responses back to clients (validation mechanism). The latter does not reduce the amount of HTTP requests but it reduces the payload of the HTTP responses that are sent back to the client and thus addresses network bandwidth reduction [17].

In addition to caching, modern web browsers usually support some kind of data compression. This reduces response sizes and transfer times, which results in lower power consumption. A web server may compress the content using one of the compression methods that a browser claims to support [17]. On the contrary, compressing content on the fly, depending on the capabilities of the user's web browser, results in higher processor load, which in turn leads to higher power consumption. Hence, compressible files should be stored in a compressed and an uncompressed version.

In order to reduce the total amount of HTTP requests and HTTP payload sizes we suggest that administrators of web servers configure the cache support and the compression support properly, so that power consumption is reduced effectively.

Energy-Saving Software for Hardware and Data Centres. So far, several data centre providers exist that operate their processing services with renewable energy. Additionally, administrators can apply the newest techniques regarding Green IT like virtualization strategies. According to [18] it seems to be possible to save 4.1 megatons of carbon dioxide emissions by virtualization and by optimizing heating, ventilating and air conditioning in German data centres.

Unfortunately, introducing virtualization strategies in data centres carries the risk that persons responsible tend to deploy server based applications like e.g. web services or web based content management systems to distinct virtual machines. One advantage is that these services do not interfere with each other anymore when applying software patches or updates, because they run on separate systems, which makes them at a first glance easier to maintain. But from a certain point in time this possibly leads to an additional workload for administrators, because they may have to maintain even more machines than before virtualization was introduced.

On the contrary, virtualization software consumes processing time to manage the different virtual machines, and this leads to some overhead. Virtualization of peripheral devices is much more resource intensive than CPU virtualization. It was shown that the throughput of virtualized network devices is only 75% down to 50% compared to non-virtualized devices, depending on applied virtualization strategies [19].

This shows, that introducing virtualization strategies in data centres can easily lead to rebound effects because it is so easy to run a new server for a service or software instead of deploying them on existing ones. Hence, it is suggested for administrators to use virtualization techniques, because it reduces power-consuming servers that are hardly working to capacity, but administrators should resist starting new virtual servers for every new service or software, because that may lead to rebound effects resulting from processing overheads caused by virtualization.

4.3 For Users

Our proposed model includes concepts for different user types. Beyond the possibilities for developers and administrators, end users also influence a sustainable software approach. In this section, we describe two different examples implementing the usage lifecycle phase of our model, which is also relevant for end users.

Generating User-specific Interactive Documents (GUIDO). In looking at Sustainable Development, not only questions regarding the environment are relevant, the social and economical dimensions have to be considered. Regarding the accessibility of information systems and governmental processes it is necessary, also for handicapped people to have access to information and to be able to participate in formal workflows. The GUIDO-System [20] depicted in Figure 5 helps users by simplifying access to official forms. By generating a generic structure of forms like official applications or notifications, the GUIDO-System provides a presentation on the user side, which takes special handicaps like visual impairment into account. By means of special profiles – the user profile and the device profile – GUIDO is able to convert arbitrary forms and documents into a user-specific presentation. Thus the GUIDO-System contributes to the social dimension of sustainability as it enables impaired people to participate in official decision and management processes within modern information societies without the need of assistance from other people.

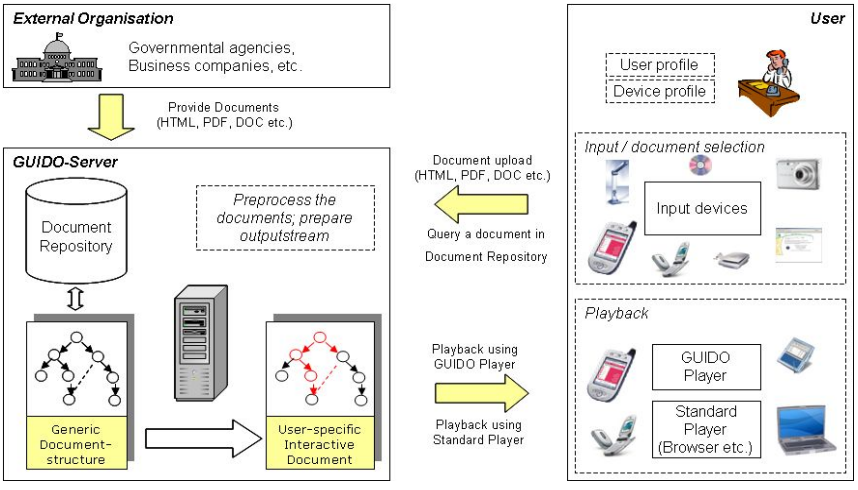


Fig. 5. System Architecture and Workflow of the GUIDO-System [20]

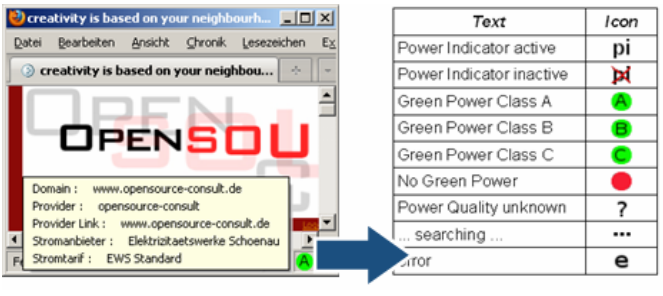


Fig. 6. Screenshot of the Power Indicator application [21]

Visualizing Power Quality of Websites. As mentioned, in order to achieve a "greener" Internet, one first step is to visualize for web users whether a website is hosted with renewable energies or not. Our Firefox add-on "Power Indicator" visualizes the green power state of a website via a small icon (see Fig. 6). The application is based on a database which contains web providers and their power supply companies.

5 Conclusion and Outlook

Today, the three pillars of sustainability: economy, society, and environment are far from being balanced [1]. The environmental pillar especially, is still underrepresented. Additionally, to date it is not clear whether energy consumption by ICT is greater or smaller than energy savings by ICT. Where manifold efforts of Green IT address the environmental pillar considering computer hardware, hardly any models, descriptions or realizations exist in the area of computer software so far. In order to

fill this gap, it seems to be necessary to foster corresponding sustainability efforts in the field of software engineering. This can be achieved with appropriate models, descriptions and tools. Therefore, we presented in our paper the results of a few expert interviews that form the basis for a definition of the term "Sustainable Software", a process and lifecycle model for "Green and Sustainable Software Engineering", and six concrete instances of this model for practitioners.

The model comprises the process and lifecycle model component and the guidelines and checklists component. The process and lifecycle model is based on common software lifecycle process standards and common lifecycle assessment standards. It is intended to provide starting points for activities that lead to software products that are developed, provisioned and used with respect to sustainability issues. Guidelines and checklists are applicable representations of the model regarding various process steps. The presented instances of the model consider different phases and actors during the lifecycle.

Our next steps are to detail and broaden our model. More details can help in the finding of solutions for more special problems regarding energy efficiency. Broadening comprises such as barrier-free techniques as the idea of sustainable development also contains aspects of sociability and free access to common goods.

Acknowledgments. This paper evolved from the research and development project "Green Software Engineering" (GREENSOFT) sponsored by the German Federal Ministry of Education and Research under reference number 17N1209.

References

1. World Commission on Environment and Development (ed.): Our Common Future, 13th edn. Oxford University Press, Oxford (1991)
2. Fichter, K.: Sustainable Business Strategies in the Internet Economy. In: Hilty, L.M., Gilgen, P.W. (eds.) Sustainability in the Information Society, Proceedings of the 15th International Symposium Informatics for Environment Protection, Zurich. Metropolis Verlag, Marburg (2001)
3. Erdmann, L., Hilty, L.M., Goodman, J., Arnfalk, P.: The Future Impact of ICTs on Environmental Sustainability. Technical Report Series EUR 21384 EN. IPTS, Brussels (2004), http://ftp.jrc.es/EURdoc/eur21384en.pdf
4. U.S. EPA (U.S. Environmental Protection Agency): Report to Congress on Server and Data Center Energy Efficiency, Public Law, pp. 109-431, August 2 (2007)
5. Koomey, J.G.: Estimating total Power Consumption by Servers in the U.S. and the World. Final report, February 15. Analytics Press, Oakland (2007), http://enterprise.amd.com/Downloads/svrpwrusecompletefinal.pdf
6. Göhring, W.: The Memorandum "Sustainable Information Society". In: Proceedings 18th International Conference Informatics for Environmental Protection, EnviroInfo, Geneva (2004), http://www.wolf-goehring.de/OverMemoSIS.pdf
7. Coroama, V., Hilty, L.M.: Energy Consumed vs. Energy Saved by ICT – A Closer Look. In: Wohlgemuth, V., Page, B., Voigt, C. (eds.) Environmental Informatics and Industrial Environmental Protection: Concepts, Methods and Tools. 23rd International Conference on Informatics for Environmental Protection, vol. 2, pp. 353–361. Shaker Verlag, Aachen (2009)

8. Naumann, S.: Sustainability Informatics – A new Subfield of Applied Informatics? In: Möller, A., Page, B., Schreiber, M. (eds.) EnviroInfo 2008. Environmental Informatics and Industrial Ecology, 22nd International Conference on Environmental Informatics, pp. 384–389. Shaker Verlag, Aachen (2008)
9. International Organization for Standardization (ed.): ISO/IEC 25000:2005 Software Engineering—Software Product Quality Requirements and Evaluation (SQuaRE)—Guide to SQuaRE. International Organization for Standardization, Geneva (2005)
10. The EU Energy Label, http://www.energy.eu/focus/energy-label.php
11. International Organization for Standardization (ed.): ISO/IEC 12207:2008 Systems and software engineering - Software life cycle processes. International Organization for Standardization, Geneva (2008)
12. International Organization for Standardization (ed.): ISO 14040:2006 Environmental management - Life cycle assessment - Principles and framework. International Organization for Standardization, Geneva (2006)
13. Office of Government Commerce (ed.): Service Support: ITIL; [the key to] managing IT services. TSO (The Stationery Office), London (2005)
14. Dick, M., Naumann, S., Held, A.: Green Web Engineering. A Set of Principles to Support the Development and Operation of "Green" Websites and their Utilization during a Website's Life Cycle. In: Filipe, J., Cordeiro, J. (eds.) WEBIST 2010: Proceedings of the 6th International Conference on Web Information Systems and Technologies, Valencia, Spain, April 7-10, vol. 1, pp. 48–55. INSTICC Press, Setúbal (2010)
15. King, A.: Website Optimization. O'Reilly Media, Sebastopol (2008)
16. Theurer, T.: Performance Research, Part 2: Browser Cache Usage - Exposed! http://www.yuiblog.com/blog/2007/01/04/performance-research-part-2/
17. Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., Berners-Lee, T.: Hypertext Transfer Protocol - HTTP/1.1. Request for Comments 2616. The Internet Society (1999), http://tools.ietf.org/html/rfc2616
18. The Boston Consulting Group: SMART 2020 Addendum Deutschland: Die IKT-Industrie als treibende Kraft auf dem Weg zu nachhaltigem Klimaschutz (2009), http://www.gesi.org/Media/GeSINewsFullStory/tabid/85/smid/503/ArticleID/43/reftab/37/t/The%20Need%20For%20a%20SMART%20Alliance/Default.aspx
19. Menon, A., Santos, J.R., Turner, Y., Janakiraman, G., Zwaenepoel, W.: Diagnosing Performance Overheads in the Xen Virtual Machine Environment. In: VEE 2005: Proceedings of the 1st ACM/USENIX International Conference on Virtual Execution Environments, Chicago, USA, June 11-12, pp. 13–23. ACM, New York (2007)
20. Richter, S., Kuhn, N., Naumann, S., Schmidt, M.: Enhancing Accessibility to E-Government Processes. International Journal of Information Communication Technologies and Human Development, Special Issue: ICT and E-Governance 1(2), 28–47 (2009)
21. Naumann, S., Gresk, S., Schäfer, K.: How Green is the Web? Visualizing the Power Quality of Web-sites. In: Möller, A., Page, B., Schreiber, M. (eds.) EnviroInfo 2008. Environmental Informatics and Industrial Ecology, 22nd International Conference on Environmental Informatics, pp. 62–65. Shaker Verlag, Aachen (2008)

Managing Energy Efficiency in Manufacturing Processes – Implementing Energy Performance in Production Information Technology Systems

Katharina Bunse and Matthias Vodicka

ETH Zurich, BWI Center for Enterprise Sciences, 8092 Zurich, Switzerland
kbunse@ethz.ch, mvodicka@ethz.ch

Abstract. Climate change and unsecured energy supply are topics that become increasingly important in today's society. Although renewable energy technologies may be a long-term solution, more efficient energy use potentially makes a high and economic contribution to the given challenges in the short term. New CO_2 regulations, rising energy prices and environmentally aware customers make energy efficient manufacturing a priority topic on the agenda of industrial companies. This paper focuses on drives for industrial companies to become more energy efficient in their manufacturing processes by integrating energy efficiency performance information and communication technology (ICT) in production management systems. Based on an EU roadmapping project, the paper analyzes which management tools and concepts support manufacturing companies to successfully implement energy efficiency improvement measures. By integrating energy efficiency performance criteria in ICT systems, decision-makers in industrial companies will be supplied with real-time and accurate information enabling them to make more effective business decisions.

Keywords: Energy Efficient Manufacturing, Information and Communication Technology, Production Management.

1 Introduction

Climate change and unsecured energy supply are topics that are becoming increasingly important in today's society and economy. Using the available energy more efficiently is one approach in meeting rising energy needs [1]. Furthermore, energy efficiency helps in preventing fossil fuel depletion, enhancing a nation's energy security, and preventing further deterioration of environmental quality [2]. With its share of 33% of final energy consumption, the manufacturing industry is one of the main energy consumers and the largest emitter of CO_2 emissions [3]. Not only from a policy and society perspective does energy efficiency hold great benefits, there are also numerous advantages from an industrial perspective in becoming more energy efficient in manufacturing processes. There are three main reasons for companies to implement energy efficiency improvements: rising energy prices, new environmental regulations with their associated cost for emissions, and customers

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 260–268, 2010.

changing their purchasing behavior with regard to environmentally benign products and services. In the energy-intensive manufacturing industries (e.g., steel, cement, pulp and paper, chemicals), energy costs can represent up to 60% of operating costs [4].

Moreover, energy efficiency is an important pillar of sustainable business strategies. The move towards sustainability comes with many benefits for industrial companies. Willard [5] suggests seven major benefits from adopting a sustainability business strategy for industrial companies: (a) easier hiring of the best talent, (b) higher retention of top talent, (c) increasing employee productivity, (d) reduced expenses in manufacturing, (e) reduced expenses at commercial sites, (f) increased revenue/market share, and (g) reduced risk and easier financing. Examples in literature and practice show that although the manufacturing sector has made continuous improvements in energy efficiency over the last years, "the economic energy efficiency potential in the industrial sector is far from being exhausted" [6]. Moreover, some researchers in the field of energy efficiency suggest that there are productivity benefits that can be associated with energy efficiency improvement measures [7, 8, 9]. These non-energy benefits could be, for example, lower maintenance costs, increased production yield, safer working conditions and many others. Worell et al. [10] argue that additional productivity benefits should be included in an economic assessment of the potential of energy efficiency improvements.

This paper focuses on the integration of energy efficiency performance criteria into production management systems as an enabler for companies to become more energy efficient in their manufacturing process. As IT infrastructure is increasing drastically since the 80's [11] appropriate ICT systems in manufacturing are significant drivers for successful businesses. Based on a EU funded roadmapping project this paper analyses which ICT related management approaches and concepts need to be adapted by companies in order to successfully implement energy efficiency improvement measures. In this paper we want to highlight the most important and promising research areas for utilizing ICT for energy efficient manufacturing.

1.1 Initial Background and Problem Definition

As mentioned before, there are several reasons and incentives for industrial companies to implement energy efficiency improvements in their manufacturing process. Nevertheless, several studies show that even profitable investments in energy efficiency are sometimes not undertaken by companies, and that there exists a gap between potential and actual energy saving measures (e.g., [6, 12, 13, 14.). The "energy efficiency gap" debate focuses on the reasons why profitable investments to reduce energy consumption are not realized in companies. One reason may be that in many companies, particularly small and medium-sized companies, investments - except for buildings and infrastructure - are decided on according to payback periods instead of internal interest rate calculations [15]. Unrealistic high implicit discount rates in standard investment models are one of the reasons that profitable energy efficiency technologies are not implemented ([12, 15]). Moreover, energy investment costs include "difficult-to-measure components, such as transaction costs, monitoring costs, administrative costs, and adjustment costs" [16]. The most important barriers

for investments in energy-saving technologies may be “other more attractive investment opportunities, incomplete depreciation of the existing capital stock” [13], and not important enough energy costs.

Some studies have also identified the low status of energy management as a barrier to energy efficiency [17]. The most important paradoxes and problems associated with the development and implementation of Total Quality Environmental Management (TQEM) systems are, among others: a strong bias in favor of ignorance at the highest management levels of the firms, a real concern as to whether customers are willing to pay the added costs associated with having something that is environmentally friendly, fear of negative returns, lack of appropriate measures and tools for capturing the environmental impact (see [18]).

In this paper we argue that ICT holds a high potential for companies to overcome some of the barriers responsible for the energy efficiency gap. By making information available and energy saving and financial savings from energy efficiency investments transparent, by reducing complexity, or by automatically controlling the production process with regard to energy efficiency, ICT is a major enabler for energy efficient manufacturing.

1.2 Objectives of the Paper

This paper demonstrates that integration of energy efficiency performance criteria in ICT systems is a highly relevant topic for manufacturing companies nowadays. The IT infrastructure of industrial companies consists of many different systems. Enterprise Resource Planning (ERP) Systems, Manufacturing Execution Systems (MES), Supply Chain Management systems (SCM), Customer Relationship Management (CRM), and Product Lifecycle Management (PLM) are important ICT tools and have a high impact on business processes [19]. Moreover, measurement and control systems are an integral part of the manufacturing system.

This paper highlights the need for future research in the area of ICT enabling energy efficiency in manufacturing processes. First, it demonstrates that this research area is highly relevant. Second, the paper gives more details on the concepts and tools necessary for integrating energy efficiency Key Performance Indicators (KPIs) into production management systems. It concludes with a discussion and outlook on future collaborative research activities.

2 Methodology

This research is based on the results of the EU funded project IMS2020, which has the objective of supporting future manufacturing environments by building a roadmap and highlighting the main milestones for future research activities needed to achieve a desired vision for manufacturing systems. IMS2020 is embedded in the global activities of the Intelligent Manufacturing Systems (IMS) initiative. IMS is a platform for global collaborative research and experience exchange. At the time of writing this paper Japan, Korea, Europe (EU incl. Norway, and Switzerland), and the United States are participating in the IMS initiative. IMS2020 focuses on five research areas, the so-called Key Area Topics (KAT), namely Sustainable Manufacturing, Energy

Efficient Manufacturing, Key Technologies, Standards and Education. The paper at hand is based on the results of this project in the area of Energy Efficient Manufacturing (EEM). In order to identify the needs and challenges of industrial companies a thorough state-of-the-art analysis was conducted. In parallel, 106 interviews, an online survey with 261 participants, and several workshops were conducted in order to gather experience in the field of EEM and to gain up-to-date information about trends in this area. The identified topics were consolidated to 62 research topics and sent again to industrial and academic experts to evaluate their relevance in a second online survey with 356 participants. The development of the roadmaps has been supported by collaborative tools shared with all the Roadmapping Support Group, a growing community that, at the moment, counts 254 participants from 108 mainly industrial organizations.

3 Integrating Energy Efficiency Performance Criteria into ICT of Production Management Systems

In the area of EEM, 11 research topics were identified. They were clustered into four research areas called: "Energy Sources for Factories", "Efficient Production Processes", "Energy Utilization in Collaborative Frameworks" and "Management and Control of Energy Consumption" [20]. The second most important research topic within the Key Area Topic EEM with a mean relevance of 3.03 (where 1 means "very low relevance" and 4 means "very high relevance") was the research topic "Integrating Energy Efficiency Performance Criteria into ICT production management systems". Moreover, around 80% of the participants stated that they are interested in collaborative research regarding this topic, now or in the future.

In the interviews with industry representatives it became evident that most of the present production planning and control systems do not integrate energy efficiency as a relevant performance criterion. ICT plays an enabling role for energy efficiency improvements – either as a tool to help companies track their energy consumption and identify areas where savings can be made, or as the basis for more efficient production concepts and techniques. An enhanced framework for managing and optimizing energy efficiency in manufacturing processes needs to be developed and implemented in enterprise production information systems, as depicted in table 1, which shows some examples of industrial needs mentioned in the interviews.

Research should aim at extending the scope of MES, ERP, and SCM software to achieve energy efficiency goals. MES deliver information that enables the optimization of production processes from order receipt until outgoing goods [21]. As MES enable production managers and the process owner to understand how resources are used in the production process, they hold a significant potential for enhancing energy efficiency in production. Thus, a framework should be developed with the aim of showing how MES can be enhanced towards energy efficiency performance and how it can be implemented software-wise. A study from Rockwell Automation states: "As control systems and MESs increase the amount of information available to manufacturers, data management will become a more important part of ensuring that sustainability goals are met" [21]. Based on proper performance indicators and guiding management principles, MES are an important tool. For enhancing MES

towards energy efficiency there are three important key technology areas: 1. Sensor technology for monitoring and transmitting production asset performance, 2. Software for the evaluation of performance data, 3. Management concepts to derive appropriate improvement strategies.

Table 1. Examples for research areas where ICT acts as enabler of EEM in order to coordinate actions and increase the benefits of energy efficiency improvement activities (based on interviews with representatives of manufacturing companies)

Examples for research areas where ICT acts as enabler of EEM (based on interviews)
Plant-wide solutions for energy efficiency and process integration.
Full and dynamic integration of information from the shop-floor to top-floor (e.g. integration with MES).
Open Information Systems for small and medium sized companies (SMEs), enhancing functionalities of ERP/SCM/CRM software for an effective and efficient integration into whole Supply Chain.
Development of ubiquitous information platform which visualize manufacturing processes holistically.
Making key business processes more transparent and visible throughout the company's environment and include technologies as voice recognition, RFID tagging.
PLM systems to manage dynamically and in real-time all necessary information in order to make better and quicker management decisions
Standardization of data down broken to the shop-floor may result in a new generation of inter-organizational platforms for the exchange of data between ERP-Systems.

MES typically have interfaces to the automation and control systems and to ERP systems [21]. Modern ERP systems incorporate the resource planning and business processes of the entire company. Improving the shop floor scheduling and planning of the EPR system contributes to increased energy efficiency. ERP systems often have an interface to SCM modules for providing data for network optimization. The optimization that is performed by these software tools should also take into consideration the implications in terms of energy efficiency. Fig. 1 highlights important elements to be considered, when enhancing ICT production management systems towards energy efficiency.

By setting up production information systems towards EEM, decision makers will be provided with relevant information about impacts on energy performances due to production planning and business decisions. Hence more energy-aware and effective decisions can be taken, improving the enterprise performances in terms of energy efficiency. Individual IT-solutions can play a central role for increasing energy efficiency in many sectors [23]. Virtualization tools and digital manufacturing engineering require further improvement in order to assist organizations in reducing their expenditures for energy and emissions ([24, 25]). Information technology has the

potential to help manage and control the energy consumption in the industrial and public sector. A study by McKinsey reveals that the global market potential for energy management-IT-solutions will be around 15 billion EUR in the year 2020. This correlates with an annual growth of 14% from the year 2008 [23]. The European Commission also highlighted the relevance of ICT for energy efficiency in manufacturing, especially focusing on the potentials of intelligent controls, sensor and actuator networks, smart components and systems, asset monitoring systems, and advanced scheduling algorithms [26].

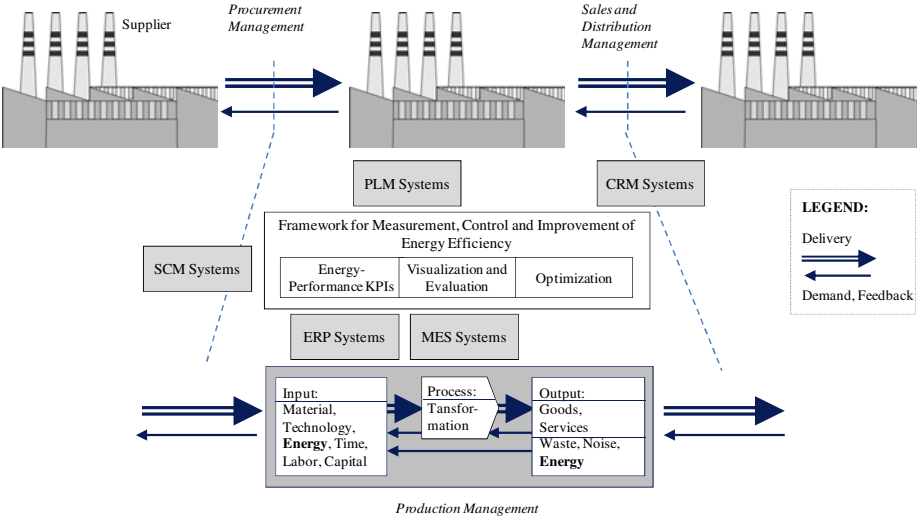


Fig. 1. Important elements for ICT enabling energy efficient manufacturing (adapted from [22])

A report by the climate group on behalf of the Global eSustainability Initiative (GeSI) states that the ICT sector can be expected to be responsible for 1.43 $GtCO_2$ emissions in the year 2020 (about 3% of global CO_2 emissions in a business-as-usual scenario), while ICT as an enabler can also lead to CO2 emission reduction of about 7.8 $GtCO_2$ emissions by 2020 [27]. For achieving this reduction in energy consumption and CO_2 emissions ICT driven manufacturing systems and optimization in logistics networks will be critical factors. The development of EEM oriented IT solutions requires the integration of various production levels - from shop floor to management level. Moreover, the definition of suitable performance indicators is a basic requirement for an ICT enabled management of energy efficiency. In [28] a selection of energy efficiency KPIs can be found, which are implemented in manufacturing companies, especially in the energy-intensive industries. Two typical indicators are the energy intensity (EI) and the specific energy consumption (SEC). EI is called an economic indicator as it is derived from economic terms. In contrast, the SEC relates to physical units per tonne of product and is thus called a physical indicator.

When integrating energy performance in ICT systems for production management, a special attention has to be given to the interface between the different systems. MES

and ERP systems, for example, should be linked in order to integrate the financial perspective and the dynamics of the shop floor (e.g., machine utilization and downtime). Lee suggests that this link "is hindered by the lack of integrated information coming from and flowing to control systems on the plant floor" [19]. There are also limitations of ERP systems to be utilized for SCM planning and optimization. Current ERP are not sufficient in their modularity, openness and flexibility for supporting SCM across multiple enterprises [29]. Besides the software and tool development, education and training of employees and an enterprise culture with the flexibility of local dynamic decision-making are critical factors for the successful implementation of new production management ICT solutions and tools [19].

In the discussion about enhancing ICT systems towards supporting EEM special attention has to be given to the fact, that ICT systems are not only enablers for energy efficiency but are also main consumers of energy. ICT systems are responsible for the same amount of CO_2 emissions as global air travel due to the increase in power required for rising data rates and growing market penetration of ICT solutions [30]. Moreover, due to the rebound effect - that refers to an effective increase of energy consumption as a consequence of increasing energy efficiency and the associated decrease in energy price – the overall effect of increasing energy efficiency through enhanced ICT systems is very difficult to assess [31]. Hilty et al. [32] identified positive and negative environmental impacts from ICT on different levels (first, second and third order effects). Yi and Thomas [33] reviewed existing literature and research projects on the environmental impact of ICT and concluded "that traditional assessment approaches are insufficient to accommodate the digital technology revolution and cannot accommodate the challenge of measuring the impacts of ICT on environmental sustainability" [33].

4 Discussion and Conclusion

Adapted ICT systems for energy efficiency may enhance a company's IT infrastructure to support strategies striving for sustainable business activities. By making relevant production and process data transparent and available to decision-makers in real time, energy efficiency improvements would be supported in various ways: On the one hand, benefits and financial savings from energy efficiency improvements may gain visibility, mitigating barriers to energy efficiency improvements. On the other hand, ERP and MES systems allow for more energy efficient production processes by specifically controlling the processes with regard to energy efficiency. However, to accomplish latter suitable energy efficiency, KPIs have to be defined and integrated into these systems. In this area also standardization activities are required to allow for benchmarks. Further, new interfaces for solutions from different providers need to be established. Concluding, we suggest, that future research should aim at enablers, such as concepts and tools, supporting the integration of energy efficiency performance criteria into ICT systems for production management.

In order to develop new energy management systems, the sensors and control devices require attention as well as the KPIs and the techno-human interfaces. With

this, energy efficiency can become an integral part of the manufacturing systems and can be represented in the ICT systems. In future research projects, enhanced frameworks for managing and optimizing energy efficiency need to be developed and implemented in enterprise planning and control information systems. Furthermore, investigation on the overall effect of enhancing ICT with regard to energy efficiency performance indicators, especially taking into consideration the rebound effect, may be undertaken.

References

1. International Energy Agency (IEA): Assessing measures of energy efficiency performance and their application in industry, http://www.iea.org
2. Mukherjee, K.: Energy use efficiency in U.S. manufacturing: A nonparametric analysis. Energy Economics 30, 76–96 (2008)
3. International Energy Agency (IEA): Worldwide Trends in Energy Use and Efficiency, Key Insights from IEA Indicator Analysis, http://www.iea.org
4. International Energy Agency (IEA): Feedstock Substitutes, Energy Efficient Technology and CO2 Reduction for Petrochemical Products. In: Workshop Proceedings, http://www.iea.org
5. Willard, B.: The sustainability advantage: Seven business case benefits of a triple bottom line. New Society Publ., Gabriola Island, B.C. (2002)
6. Eichhammer, W.: Industrial Energy Efficiency. In: Cleveland, C.J. (ed.) Encyclopedia of Energy, pp. 383–393. Elsevier, New York (2004)
7. Elliott, R.N., Latiner, S., Pye, M.: Considerations in the estimation of cost and benefits of industrial energy efficiency projects. In: Cairns, E.J. (ed.) Proceedings of the Thirty-Second Intersociety Energy Conversion Engineering Conference. American Institute of Chemical Engineers, New York (1997)
8. Porter, M.E., van der Linde, C.: Green and Competitive: Ending the Stalemate. In: Harvard Business Review, pp. 120–134 (September-October 1995)
9. Boyd, G.A., Pang, J.X.: Estimating the linkage between energy efficiency and productivity. Energy Policy 28, 289–296 (2000)
10. Worrell, E., Laitner, J.A., Ruth, M., Finman, H.: Productivity benefits of industrial energy efficiency measures. Energy 28, 1081–1098 (2003)
11. Krcmar, H.: Informationsmanagement. Springer, Berlin (1997)
12. DeCanio, S.J.: The efficiency paradox: bureaucratic and organizational barriers to profitable energy-saving investments. Energy Policy 26, 441–454 (1998)
13. De Groot, H.L.F., Verhoef, E.T., Nijkamp, P.: Energy saving by firms: decision-making, barriers and policies. Energy Economics 23, 717–740 (2001)
14. Paton, B.: Efficiency gains within firms under voluntary environmental initiatives. Journal of Cleaner Production 9, 167–178 (2001)
15. Anderson, S.T., Newell, R.G.: Information programs for technology adoption: the case of energy-efficiency audits. Resource and Energy Economics 26, 27–50 (2004)
16. DeCanio, S.J., Watkins, W.E.: Investment in Energy Efficiency: Do the Characteristics of Firms Matter? The Review of Economics and Statistics 80, 95–107 (1998)
17. SPRU (Science and Technology Policy Research): Reducing barriers to energy efficiency in public and private organizations Brighton, UK (2000)

18. Curkovic, S., Sroufe, R.: Total Quality Environmental Management and Total Cost Assessment: An exploratory study. Scheduling in batch-processing industries and supply chains. International Journal of Production Economics 105, 560–579 (2007)
19. Lee, J.: E-manufacturing - fundamental, tools, and transformation. Leadership of the Future in Manufacturing. Robotics and Computer-Integrated Manufacturing 19, 501–507 (2003)
20. IMS2020. Action Roadmap on Key Areas 1, 2 and 3, http://data.fir.de/projektseiten/ims2020/files/Action_Roadmap.pdf
21. Rockwell Automation: Manufacturing Execution Systems for Sustainability. Extending the Scope of MES to Achieve Energy Efficiency and Sustainability Goals, http://literature.rockwellautomation.com
22. Schönsleben, P.: Integral logistics management. Operations and Supply Chain Management in Comprehensive Value-Ndded Networks. Auerbach Publ., Boca Raton (2007)
23. McKinsey Deutschland: Wettbewerbsfaktor Energie. Neue Chancen für die deutsche Wirtschaft, http://www.mckinsey.de
24. European Commission (EC): The Future of Manufacturing in Europe 2015-2020 - The Challenge for Sustainability – Scenarios, http://simula.cesga.es/document/docs/TheFuturemanufacturing.pdf
25. European Commission (EC): Manufuture – Strategic Research Agenda - Report of High Level Group, http://manufuture.org
26. European Commission (EC): ICT and energy efficiency - the case for manufacturing. Recommendations of the Consultation Group, http://ec.europa.eu
27. The Climate Group: SMART 2020: Enabling the low carbon economy in the information age, http://www.smart2020.org
28. Bunse, K., Sachs, J., Vodicka, M.: Evaluating Energy Efficiency Improvements in Manufacturing Processes. In: Proceedings of the International Conference on Advances in Production Management Systems Conference, Bordeaux, France (2009)
29. Akkermans, H.A., Bogerd, P., Yücesan, E., van Wassenhove, L.N.: The impact of ERP on supply chain management: Exploratory findings from a European Delphi study. European Journal of Operational Research 146, 284–301 (2003)
30. Fettweis, G., Zimmermann, E.: ICT Energy Consumption - Trends and Challenges. In: The 11th International Symposium on Wireless Personal Multimedia Communications (2008)
31. Plepys, A.: The grey side of ICT. Sustainability in the Information Society. Environmental Impact Assessment Review 22, 509–523 (2002)
32. Hilty, L.M., Arnfalk, P., Erdmann, L., Goodman, J., Lehmann, M., Wäger, P.A.: The relevance of information and communication technologies for environmental sustainability - A prospective simulation study. Environmental Informatics. Environmental Modelling and Software 21, 1618–1629 (2006)
33. Yi, L., Thomas, H.R.: A review of research on the environmental impact of e-business and ICT. Environment International 33, 841–849 (2007)

A Reference Process to Design Information Systems for Sustainable Design Based on LCA, PSS, Social and Economic Aspects

Fabiana Soares Santana[1], Claudio Barberato[2], and Antonio Mauro Saraiva[3]

[1] Universidade Federal do ABC, Brazil
[2] Centro Universitário da FEI, Brazil
[3] Universidade de São Paulo, Brazil
fabiana.santana@gmail.com, claudio.barberato@gmail.com, saraiva@usp.br

Abstract. The purpose of Sustainable Design, SD, is to satisfy customer needs while reducing environmental impacts. The main challenge is to integrate Life Cycle Assessment, Product Service Systems, social and economic aspects while considering the tensions and trade-offs of each activity in depth. SD requires data from many sources in addition to many software tools to perform each analysis. In order to provide information systems for SD, the adoption of a Service-Oriented Architecture, SOA, is appropriate because of its integration requirements. SOA best practices recommend the design of a reference process prior to architectural definitions, so as to identify the complexities and provide a comprehensive solution to the problem. A reference process is presented here as the first step for building information systems for SD. In addition, the reference process presents a list of activities to be performed during the design stage and is very helpful as a guide for SD beginners.

Keywords: SOA, Reference Process, Sustainable Design, Information Systems, Information Systems to Support Sustainable Design.

1 Introduction

Sustainable Development is "the development that meets the needs of the present without compromising the ability of future generations to meet their own needs" [3]. Eco-Efficiency addresses the delivery of products and services, raising the quality of life, reducing ecological impacts to acceptable levels and providing competitive prices [10]. Cleaner Production [http://www.uneptie.org/pc/cp/home.htm] is the continuous application of environmental strategies so as to increase Eco-Efficiency [6]. One of the main purposes of Cleaner Production is reducing the environmental impacts that, despite all concerns about the subject, continue to grow [6, 23].

Climate change and ecological disasters attributed to global warming, are leading to the establishment of legal and trade restrictions related to the development of products and services so as to increase their sustainability [26, 29]. This is known as *Sustainable Design,* SD, or *Design for Sustainability*. *Product Service System* [29],

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 269–280, 2010.

PSS, is a system proposed to create new products and services focused on meeting the client's needs, eventually replacing products for services or vice versa, or modifying the existing productive processes. Life Cycle Assessment, or LCA, is a standard technique [20, 21] used to evaluate the impact of a product on the environment.

SD is a highly complex activity with many tensions and trade-offs, and one of its main challenges is to design products integrating PSS concepts and LCA techniques to the social and economic aspects of the production process. The purpose is to offer a complete and realistic evaluation of the environmental burden caused by a product or a service. This complexity can be reduced with the development of appropriate information systems for SD. Software tools to assist in the design activity and for performing analysis and evaluations of quantitative aspects of SD would be very helpful to the designer.

Information systems for SD will demand resources for integration and interoperability with other systems and data, obtained from many potential different providers, since it requires information about raw material, the productive process, the product disposal and many others. Hence, a solution based on Service-Oriented Computing, SOC, is recommended [2, 31].

The development of a SOC-based solution may start with the design of a Service-Oriented Architecture, SOA. A SOA-based solution may start with the definition of a reference process to present a clear elicitation of the tasks to be performed and to include the experts' knowledge in a single process view [8].

A reference process is thus presented here to address the requirements of an information system for SD. This is the first step for defining a SOC-based software solution for this problem. As additional benefits, the reference process can show improvements in the design activity and can be very useful for beginners, as a guide to SD.

2 Evaluating the Environmental Burden

This section presents basic concepts related to the evaluation of the environmental burden of products and services, and strategies to try and reduce it.

2.1 Processes, Products, Services and the Environment

A process is a collection of steps, arranged in a sequence and following a particular set of rules. The decomposition of a domain is recommended as a starting point to identify the problems to be solved in a SOA-based system [19]. This can be achieved by designing a process in which the steps required are described with the respective inputs and outputs.

A reference process in SOA maps the detailed information contained in an existing standard or model [1, 32]. It summarizes and organizes the knowledge about a subject. Besides documenting and formalizing current practices, a reference process may be a guide to define each specific step of the process and can also be applied to identify gaps, extra work, failures and improvements. It represents an important tool for a software architect because it condenses all the knowledge about the problem in a single diagram.

SD must consider the conservation of raw materials, energy and water, the reduction of emissions and wastes and the elimination of toxic components during the production process. Reduction of environmental burden through the complete product life cycle must be considered in SD, in addition to the well-established concerns about safety and health. Environmental impacts must also be considered in the design, delivery and disposal of each product. Therefore, the main purpose of SD must be to integrate efforts in designing clean processes, products and services in order to achieve a global result that is more effective in preventing environmental damage than isolated solutions. The design stage is the adequate moment to approach environmental impact minimization [6].

Eco-Design is an adequate strategy for approaching the problem, since the entire life cycle of the product or service system must be discussed [4, 10, 24]. If the economic, social and legal aspects are also considered then the sustainability of the productive system can be completely evaluated, because of the interconnected views [6]. For example, the reduction of raw material usage may reduce both the environmental burden and the cost of the product; thus, sustainability and economy aspects are related. Legal aspects are also relevant in a global economy, since many countries have restrictions on import products whose production process does not follow certain conditions and, in the future, perhaps, compliance with SD will be mandatory. Actually, there is already a market share for "green products", so this concern may not be disregarded.

Ecological product design must consider [6]: 1) Optimal function and ecology efficiency; 2) Durability; 3) Minimization of the energy and non-renewable resources use during the product life cycle; 4) Minimization of the use of non-biodegradable substances; and 5) Recycling and waste management.

2.2 PSS – Product Service System

PSS integrates products and services in order to design a system able to meet the clients' demands. The main idea is to sell client satisfaction instead of selling products only [29]. This stems from a new concept of mutually dependent products and services focusing on the compliance of a client demand instead of the physical result of an industrial production process [28].

PSS potentialities include the synergy among the environmental benefits and other product issues such as profit and competitiveness [13, 29, 30]. However, PSS may not result in a sustainable solution because of the rebound effects. They are the result of changes in consumer behaviour or profile due to the introduction of a new PSS, even when it is designed to reduce the environmental burden. The classical example is related with the use of computers and Internet for text editing and exchanging. It could avoid the waste of paper but, at least in the beginning, computers and the Internet only increased our capacity to produce content and a large deal of this content was printed, causing an overall waste of paper many times greater than previously thought [29].

A PSS may be sustainable or not and the following aspects must be analyzed along the life cycle of products and services in PSS [29]: 1) Greenhouse effect analysis to evaluate gas emissions; 2) Use of renewable resources, e.g. raw materials; and 3) Overall environmental and social impacts. A sustainable PSS designer may require

ability to undertake the business, understanding the social context and applying patterns from a different point of view. The result may be a new product, a new service, or a new system including both a new product and a new service, so as to satisfy the client demands.

Sustainability may rely on providing added value to the entire PSS life cycle by establishing infrastructure to enable its implementation and rules for ownership and usage, resulting in benefits to the consumer. It means, for instance, that a client may operate the product with decision power for a while but, when the contract is over or the product or system is no longer useful, the producer may take it back, deciding new sales opportunities or disposal treatment. This simplifies the control of the PSS life cycle and allows the establishment of more effective rules for reducing the environmental burden.

2.3 LCA – Life Cycle Assessment

Life Cycle Assessment is defined by ISO [20, 21]. [20] establishes the main principles and the framework for the adoption of LCA in a language accessible to a broad target audience, and [21] presents the formal requirements for a more specialized audience, and is hence the core reference document for LCA practitioners [11]. [20] and [21] are currently the only valid references for LCA, replacing the older versions.

LCA is defined as the "compilation and evaluation of the inputs, outputs and potential environmental impacts of a product throughout its life cycle" [20] and it includes [18]: 1) Analysis of the problem origins for each product; 2) Comparisons among the variations of the same product; 3) Adequate design of new products; and 4) Product choice, considering a variety of analogous offers. In LCA, the term product includes goods and services at the operational and strategic levels, and all types of impacts of a product on the environment must be considered [18].

LCA must be as quantitative as possible, so as to allow comparisons among different products that accomplish the same function. For comparative analysis, the function provided by the acquisition or rental of a product must be considered, as well as both the present and future environmental burdens.

The guiding principles of LCA are transparency, credibility, comprehensiveness and consistency [11]. Transparency interferes with the LCA planning and execution, and establishes that the scientific approach or international conventions must be the base for decisions [20]. For credibility, a comparative assertion considering unambiguousness, clarity and accuracy, and the intention to disclose it to the public, is fundamental. Comprehensiveness refers to the consideration of all aspects of the environment, resources and human health, using a cross-media perspective so as to identify potential trade-offs. Consistency refers to the harmony among all parts of the process.

LCA must consider the entire life cycle of the productive process [20, 21], including: 1) Material choice – extraction and acquisition of the raw material; 2) Manufacturing – energy required for the production and distribution processes; 3) Product use – consumption aspects; and 4) Product disposal – treatment and final disposal of the product at the end of its life cycle.

The broad scope of the analysis usually results in the simplification of some aspects of a product, so LCA has limitations [18]. For instance, LCA does not address

local impacts and dynamic approaches, and does not consider the rebound effects from the introduction of a new product onto the market, since the analysis is linear. Data availability for the analysis may also represent an important constraint in some cases. Social and economic impacts are outside the scope of LCA. There are intrinsic limitations when conclusions and recommendations about a product are being prepared, so the consistency of the technique is dependent on the methodological approach [20]. A critical review or third party reports are strongly recommended [11].

LCA allows environmental management and environmental performance evaluation, identifies relevant aspects of products within a specific context, incorporates environmental concerns into product design and development, and quantifies and certifies greenhouse gas emissions.

However, LCA may be dependent on the size, culture, product, internal system and strategy of each organization. Hence, in the SD context, LCA adoption is even more complex, requiring many techniques and software packages.

2.4 Sustainable Design

SD is "a strategic activity to conceive and develop sustainable solutions" [27]. The solution must allow people to live with quality of life but consuming less environmental resources. SD must consider social and economic impacts [25, 26].

Social impacts involve [26]: 1) Evaluation of the best alternative between a product or a service for meeting a specific demand; 2) Verification of social aspects related to the raw material, e.g.: extraction and processing, ownership rights and trading arrangements; 3) Employment conditions; 4) Impacts and investments on the local community; and 5) Adverse impacts for local and global communities, considering safety and health aspects.

It is necessary to consider the surrounding world and the recommended economic model is the distributed one; power generation, creative communities and cooperative networks take place [33]. The consumption of natural resources and innovation would be based on local structures, enterprises, initiatives and communities. The main question is how to practice SD in a global economy.

The economic impact includes evaluating the cost-effectiveness of a product or service compared to other available solutions. A balance between ecological and economic issues is necessary, in addition to technological development, specific legislation and changes in social life [9]. Life cycle must be considered to evaluate the nature and quality of PSS, confronting economic and environmental aspects to obtain significant environmental improvements [9]. Social and economic issues depend on the product or service that is being developed, but both aspects must be considered in all steps of SD.

Relevant aspects of SD are [5]: 1) Sustainable consumption is as important as sustainable production so as to avoid the rebound effects; 2) Replacing a product with a service will not necessarily improve its sustainability; 3) Consumer satisfaction is divided into one-off occurrences (e.g.: eating a hamburger) or continuous occurrences (driving a car); 4) Products and services have a different apprehension for the consumers; 5) The time to consumer satisfaction is different from a product or service use, so the consumer must thoroughly understand the substitution of one product for a service.

SD of products and services also must consider functionality, quality, demand, customer requirements, technical feasibility and compliance with legislation and technical specifications, as well as any other standards [26].

3 A Reference Process for Sustainable Design

The reference process considers products, services and other dimensions of the problem, in order to balance economic and social aspects with the environmental approaches provided by PSS and LCA.

The aim is to provide a balance among environmental protection, social equity and economic prosperity, maintaining the traditional product design requirements, such as quality, demand, technical and cost issues [26]. LCA requires the analysis of the product life cycle [20, 21], which will be made in this paper considering the standard viewpoint.

The reference process for SD will extend the concepts of ecodesign, design for disassembly, design for recycling [12], LCA, PSS and social and economic impacts. All concepts are integrated in a single process, considering the basic product life cycle, Fig. 1, according to the standard [11].

The reference process presented in Fig. 2 was defined in order to incorporate all relevant aspects of SD. The steps describe the activities to be performed during the design stage of a product. Some steps or activities must require software tools or experts to evaluate the environmental impacts.

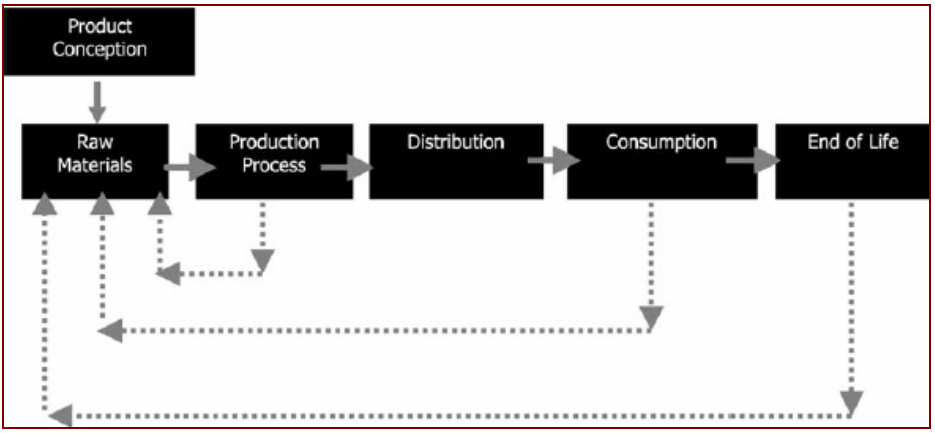


Fig. 1. The basic product life cycle can be summarized as the application of six main steps, from the raw material choice to the product disposal [8]

The six steps of the Reference Process for SD are described in Fig. 2. They are:

Step 1 – Functionality conception: this step defines the functionalities of the item to be designed, analyzes its environmental impacts and the alternatives between products and services.

Step 2 – Raw material acquisition: this step must consider minimizing the

volume of material used, especially non-renewables, and replacing the type of raw materials so as to reduce environmental impact; besides this, it must analyze the trade-offs between extracting and processing the raw materials and the transport conditions.

Step 3 – Manufacturing: the purpose of this step is to optimize the technology for manufacturing a product or delivering a service, by eliminating or reducing emissions to the air, effluents, waste, and energy use.

Step 4 – Trade and delivery: this step defines the requirements for the transport related to the delivery of a product or service, including its volume and nature, and the type of vehicle and fuel to be used; the purpose is eliminating or minimizing emissions to the air, effluents, waste, and energy use.

Step 5 – Use and maintenance: the purpose of this step is eliminating or reducing the waste related to a product or service, including its packaging and consumption.

Step 6 – Reuse, recycling, energy recovery and disposal: the purpose of this step is to extend the life of a product or to facilitate the recovery of its components for reuse, recycling, and treatment/disposal. The design must be modular, so as to maximize the upgradability, or adequate to allow the repair of eventual damages to the product.

The economic aspects are the same for all steps of the process, and the purpose is to verify the cost-effectiveness of products or services in all the previous steps of the process, comparing them to available products, evaluating environmental and non-environmental costs, and analyzing global vs. distributed economy.

Before starting the design stage, data about the raw material, the manufacturing process and the trade and delivery processes are essential. Data availability is a serious limiting factor for SD.

4 A Case Study: The Ethanol Program in Brazil

This section presents a brief overview of the ethanol program in Brazil so as to illustrate the reference process for SD. The purpose is only to comment on each step of the reference process using ethanol as an example. The evaluation of this program, the analysis of the possibilities for its adoption worldwide, and all types of metrics are outside the scope of this section so as to simplify the example and keep the focus on the reference process. The ethanol program in Brazil will be presented according to the steps of the process, even if this process was not available when the product was conceived.

Step 1 – Functionality conception: Brazil was critically affected by the oil crisis of 1973 and, in addition to the increased efforts in prospecting petroleum under the deep waters of the continental shelf, the country started the PROALCOHOL program so as to produce large amounts of sugarcane ethanol [15]. Sugarcane ethanol is a substitute for gasoline. It has the same purpose as gasoline, similar properties, the same health and safety requirements are necessary and the social and economic impacts are related, since the purpose is to reduce the price of the fuel, and the legal aspects are abided by [15].

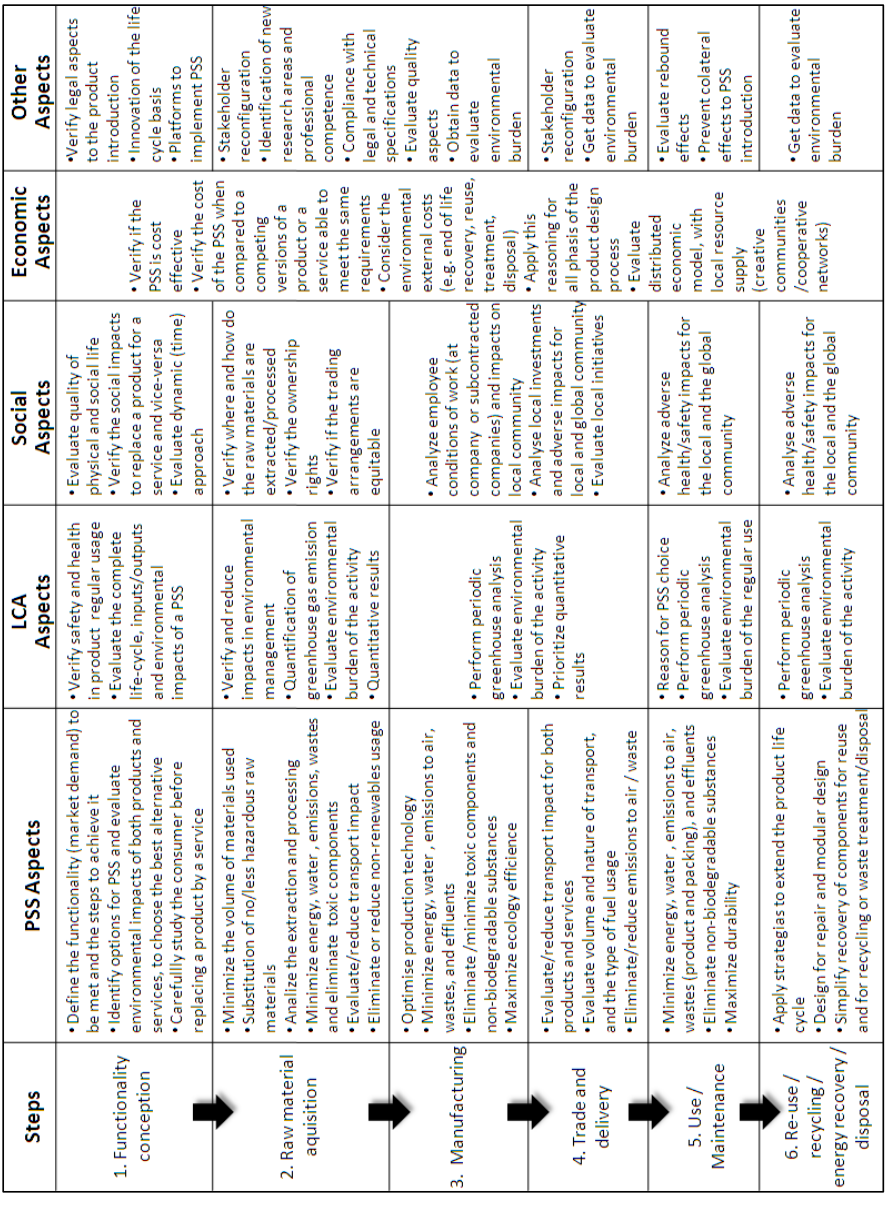


Fig. 2. A Reference Process for Sustainable Design

Steps 2 and 3 – Raw material acquisition and Manufacturing: The raw material for ethanol, in Brazil, is sugarcane. Therefore, raw material acquisition is related to sugarcane production, and sugarcane production is related to ethanol production, both will hence be studied together in this example.

Since the beginning of PROALCOHOL, the legislation has improved and the land use has been severely controlled, avoiding deforestation and preserving natural ecosystems (60% of the sugarcane production is in the state of São Paulo, no sugarcane is produced in Amazonia as the humid climate is unsuitable for sugar production), the adoption of controlled fertirrigation practices is being applied, the harvest burning practices are being phased-out through a strict legal enforcement, and the industrial sugarcane and ethanol plants have their air emissions controlled [5]. From the economic point of view, new investments are private and the cost of the production of sugarcane is decreasing [5]. From the social point of view, at least 700,000 jobs were created with the sugarcane production for ethanol while the competition for land with food production has been shown to be a myth [5]. Energy needs for its production come from the bagasse, which is used to generate power and, since the Brazilian Energy Matrix is mainly based on hydropower, the indirect consumption of fossil fuels is low [17]. The direct consumption of fossil fuels in these steps is related to the use of fertilizers and harvest machines and the main liquid effluents of ethanol are vinasse and wastewaters [17]. There are laws and technical standards to regulate vinasse disposal and techniques to reduce organic pollutants in wastewater [17].

Step 4 – Trade and delivery: One of the main requirements for trading ethanol is to prepare the vehicles for replacing gasoline with ethanol [17]. Since the beginning of the PROALCOHOL, the multinational automobile industries in Brazil agreed to produce automobiles with converted motors and have introduced all the necessary engine and vehicle modifications for ethanol use. Even gasoline vehicles use blends from 20% to 26% of ethanol. Nowadays, many cars in Brazil use a flexible fuel technology, which means the driver can choose between ethanol and gasoline or a mix of both.

Besides the vehicles, the availability of an infrastructure for ethanol pumps in service stations and ethanol distribution is required and this infrastructure started to be developed in Brazil at the beginning of the PROALCOHOL [17]. Transportation trucks, however, still use fossil fuels, but their emissions are included in the studies for evaluating the greenhouse gas emissions of ethanol [22].

Step 5 – Use and maintenance: Nowadays, ethanol is a renewable replacement for gasoline; its GHG emissions are reabsorbed by photosynthesis during the growth of sugarcane in the following season [17]. The only difference from the use of gasoline in Brazil is related to the consumption of fuel. From the economic point of view, it is regulated by the ethanol price, which is usually smaller than that of gasoline or at least in the same proportion. The consumption of ethanol in Brazil tends to drop when this proportion in not respected.

6) Reuse, recycling, energy recovery and disposal: Only the ethanol greenhouse gas emissions must be considered in this step. There is the reuse of bagasse for energy recovery and other aspects related to the ethanol production, but they were analyzed in the previous steps.

In this case, as compared to gasoline, ethanol has additional benefits, the importance of which was reinforced years after the beginning of the PROALCOHOL program. They are: a) The use of ethanol as fuel has smaller impact on the environment because it avoids CO2 emissions as compared to gasoline [17, 22]; and b) Ethanol has a favorable energy balance and is a renewable and sustainable energy source [16].

5 Discussion

The definition of this reference process shows that many aspects must be considered and weighted so as to put SD into practice.

However, the process is mainly a guideline and researchers and companies must define more specific criteria for each step of the reference process. The use of numeric criteria for evaluating products and services is mandatory in order to define comparable criteria on which to base design activity and the consumer rules.

Note that the reference process uses words such as "minimize" or "maximize", and these are not adequate or precise evaluations. However, more restricted criteria do not depend on process modeling but on the research in other areas of knowledge such as Chemistry and Physics that are able to define numerical values for LCA. Besides, as a reference process, this process must be customized for each company or production segment, by detailing each step and defining the metrics and parameters for its adoption as a regular company process.

Some activities identified in the reference process are very difficult to perform. For instance, stakeholder reconfiguration may involve the pressure of the investors or the interference of external partners, such as governments, to achieve good results. Another difficulty is to evaluate rebound effects. Some social impacts may also be hard to evaluate and, in this case, a consulting service may be a good strategy to adopt.

The definition of a reference process is a starting point in providing a more accurate evaluation of SD. It also represents the first step in the software engineering process for designing a SOA-based solution for the development of information systems for SD. The main challenge is building tools for data synthesis and analysis in SD, which must be able to get results faster and allow easy visualization, interpretation, and analysis of environmental information.

The purpose of the reference process is also to integrate the activities so as to obtain a global maximum result instead of only local results, directing the production towards client satisfaction and improvements in quality of life. This may produce unexpected synergies to improve many aspects of a consumer's satisfaction, including profit, competitiveness and environmental benefits.

6 Conclusion

The reference process to design information systems for SD based on LCA, PSS, social and economic aspects captures the main steps and activities involved in SD. The process stratifies the design activity and performs a careful analysis of each step so as to identify the problems and, within the context of a SOA-based solution, to capture the software requirements.

Since the designers must work with sustainability concepts, the reference process presents a list of activities to be performed and is also a guide to beginners. Considering the complexity of SD, the clear definition of each step for each company is mandatory.

Acknowledgments. The authors thank FINEP – Financiadora de Estudos e Projetos (Research and Projects Financing) – from the Ministry of Science and Technology – MCT/Brazil for supporting the PROSENSAP project (01.08.0566.00).

References

1. Bass, L., Clements, P., Kazman, R.: Software Architecture in Practice, 2nd edn. Addison Wesley, Boston (2005)
2. Bichler, M., Lin, K.J.: Service-Oriented Computing. Computer 39(3), 99–101 (2006)
3. Brundtland, G.: Our Common Future. Oxford University Press, Oxford (1987)
4. Charter, M., Young, A., Kielkiewics-young, A., Belmane, I.: Integrated Product Policy and Eco-Product Development. In: Charter, M., Tischner, U. (eds.) Sustainable Solutions. Developing Products and Services for the Future, pp. 98–116. Greenleaf Publishing, Sheffield (2001)
5. Coelho, S.T., Goldemberg, J., Lucon, O., Guardabassi, P.: Brazilian sugarcane ethanol: lessons learned. Energy for Sustainable Development, X-2 (June 2006)
6. Dewulf, W., Duflou, J.: Proc. of CIRP Seminar on Life Cycle Engineering, Copenhagen, Denmark (May 2003)
7. Ehrenfeld, J.R.: Industrial Ecology: Coming of Age. Environmental Science & Technology 36(13), 280A–285A (2002)
8. Endrei, M., Ang, J., Arsanjani, A., Chua, S., Comte, P., Krogdahl, P., Luo, M., Newling, T.: Patterns - Service-Oriented Architecture and Web Services. IBM Redbook (2004), http://www.redbooks.ibm.com/redbooks/pdfs/sg246303.pdf
9. Feldmann, K.: Foreword. In: Feldmann, K. (ed.) Recy 1994, Presentations of the 2nd International. Seminar on Life Cycle Engineering, Erlangen, October 10-11. Meisenbach Verlag, Bamburg (1994)
10. Fiksel, J.: Design for Environment: Creating Eco-Efficient Products and Processes. McGraw-Hill, New York (1996)
11. Finkbeiner, M., Inaba, A., Tan, R.B.H., Christiansen, K., Klüppel, H.: The New International Standards for Life Cycle Assessment. International Journal on LCA 11, 80–85 (2006)
12. Gertsakis, J., Lewis, H., Ryan, C.: A guide to EcoReDesign. Centre for Design at RMIT. RMIT University, Melbourne (1997)
13. Goedkoop, M., van Halen, C., te Riele, H., Rommes, P.: Product services systems, ecological and economic basics, Report 1999/36. VROM, The Hague (1999)
14. Goldemberg, J.: The evolution of ethanol costs in Brazil. Energy Policy 24(12), 1127–1128 (1996)
15. Goldemberg, J.: The ethanol program in Brazil. Institute of physics publishing environmental research letters. Environ. Res. Lett. 1, 014008 (5pp) (2006), doi:10.1088/1748-9326/1/1/014008
16. Goldemberg, J.: Ethanol for a Sustainable Energy Future. Science 315, 808 (2007), doi:10.1126/science.1137013
17. Goldemberg, J., Coelho, S.T., Guardabassi, P.: The sustainability of ethanol production from sugarcane. Energy Policy 36, 2086–2097 (2008)
18. Guinée, J.B., Gorée, M., Heijungs, R., Huppes, G., Kleijn, R., de Koning, A., van Oers, L., Wegener Sleeswijk, A., Suh, S., Udo de Haes, H.A., de Bruijn, H., van Duin, R., Huijbregts, M.A.J.: Handbook on Life Cycle Assessment: Operational Guide to the ISO Standards. Institute of Environmental Sciences-Universiteit Leiden. Eco-Efficiency in Industry and Science, vol. 7. Kluwer Academic Publishers, Dordrecht (2002)

19. Huhns, M., Singh, M.P.: Service-Oriented Computing: Key Concepts and Principles. IEEE Internet Computing 9(1), 75–81 (2005)
20. ISO/IEC 14040. LCA – Principles and Frameworks (2006)
21. ISO/IEC 14044. LCA – Requirements and Guidelines (2006)
22. Macedo, I.C., Seabra, J.E.A., Silva, E.A.R.: Green house gases emissions in the production and use of ethanol from sugarcane in Brazil: The 2005/2006 averages and a prediction for 2020. Biomass and Bioenergy 32, 582–595 (2008)
23. Meadows, D., et al.: The Limits to Growth. Universe Books, New York (1972)
24. McAloone, T.: Industrial Application of Environmentally Conscious Design. Engineering Research Series 1, Professional Engineering. McGraw-Hill, London (2000)
25. McAloone, T.C., Andreasen, M.M.: Design for utility, sustainability and societal virtues. In: International Design Conference – Design, May 18-21 (2004)
26. Maxwell, D., van der Vorst, R.: Developing sustainable products and services. Journal of Cleaner Production 11, 883–895 (2003)
27. Manzini, E.: Design research for sustainable social innovation. In: Michel, R. (ed.) Design Research Now, pp. 233–245. Birkhäuser, Basel (2007)
28. Manzini, E., Vezzoli, C.: Product–service systems and sustainability. Opportunities for sustainable solutions. In: United Nations Environment Programme, Division of Technology Industry and Economics, Production and Consumption Branch. CIR.IS Politecnco di Milano, Milan (2002)
29. Manzini, E., Vezzoli, C.: A strategic design approach to develop product service systems: examples taken from the 'environmental friendly innovation' Italian prize. Journal of Cleaner Production 11, 851–857 (2003)
30. Mejcamp, R.: Changing consumer behavior through eco-efficient services. Delft University of Technology, Delf (2000)
31. Papazoglou, M.P., Traverso, P., Dustdar, S., Leymann, F.: Service-oriented computing: state of the art and research challenges. Computer 11, 38–45 (2007)
32. Santana, F.S., Siqueira, M.F., Saraiva, A.M., Correa, P.L.P.: A reference business process for ecological niche modelling. Ecological Informatics Journal 3(1), 75–86 (2008)
33. Vezzoli, C.: Design for sustainability: the new research frontiers. In: 7th Brazilian Conference on Design, P & D, Curitiba, August 9-11 (2006)

IT Support for Sustainable Development in Organizations

Andreas Moeller and Arno Rolf

Leuphana University Lueneburg, Germany
University of Hamburg, Germany
moeller@uni.leuphana.de, rolf@informatik.uni-hamburg.de

Abstract. This contribution is based on Habermas' theory of communicative action and his distinction between lifeworld and social subsystems like the economy, science and public administration. This distinction does not only help in understanding the role of generalized action orientations and symbolic mechanisms in social subsystems, one important conclusion is that evolution and transition of orientations and mechanisms require communication and discourse: communication about problems, about problematic orientations, new ways and mutual insights etc. IT support in this regard (conversation support) plays a completely different role than "normal" information systems that are aimed at the stabilization of established orientations (like in economy profit maximization in combination with Taylor's efficiency thinking). This allows discussion of different IT solutions with respect to their capabilities supporting the transition phase of sustainable development, as well as their contributions to modified or new generalized action orientations: environmental management information systems (EMIS), specialized modeling tools (e.g. life cycle assessment tools) but also all-purpose tools such as Excel, Email and web-based social networks.

Keywords: Communicative Action, Systemic Mechanisms, Communication, Conversation, Generalized Action Orientation, Lifeworld.

1 Introduction

IT support for sustainability has been in discussion for more than fifteen years now. Many new approaches have been presented; prototypes and software tools demonstrated that, in principle, effective support for more sustainability in organizations, in particular in companies, is possible. Good examples in this regard are software tools for life cycle assessment [1, 2]. The implementations of which are used in several companies and associations. They help to perform life cycle assessments as well as material and energy flow based cost accountings [3]. Research projects addressed the question of how to combine the new concepts with standard software systems in companies, in particular enterprise resource planning systems (ERP systems): Interfaces, additional data fields within the ERP system, required reporting components etc. [4, 5, 6, 7].

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 281–291, 2010.

However, the success of all these efforts was limited since life cycle assessment tools are in use in only a very small percentage of companies. Effective and fully integrated support for corporate sustainability in ERP systems is still not available [8, 9]. Companies use the new approaches mainly for the purpose of cost cutting. In this contribution we discuss the reasons for this. To do this we apply Habermas' communication theory [10, 11]. Habermas introduced the concept of lifeworld and social subsystems such as public administration, economics, science etc. We will show that software support is mainly developed to support these social subsystems. This kind of software is called management information system or decision support system [12]. The social subsystems have established their own specific generalized action orientations (like value creation in economics) and systemic mechanisms. With respect to sustainable development, new concepts supporting sustainability can stay in conflict with these generalized action orientations so that they cannot be applied in practice. These theories might allow us to formulate ways to overcome these problems.

2 IT Based Decision Support

As mentioned above, computers should mainly support action in social subsystems. Because of this, researchers and software developers adopt the generalized action orientations of these subsystems. For example, in economics, managers are treated as the most important functional units. They are decision makers and need all relevant information to come to an optimal decision. Accordingly, the software solutions are called decision support systems or management information systems. With regard to environmental protection and sustainability, generalized action orientations of economy are the starting point, too. The corresponding software solutions are called environmental management information systems ((EMIS) [4, 13]. These systems are motivated by the idea that in order for managers to find the optimal solutions including aspects of environmental protection and sustainable development they require certain information which is provided by these information systems.

One of the first approaches for better decision support was the period-oriented input/output eco-balance [3]. This type of eco-balance shows all input and output material and energy flows for one year. The problem with this concept is that it is not compatible with conventional approaches, in particular cost accounting. Cost accounting can be interpreted as a conclusion of Taylor's philosophy of efficiency: The main purpose of scientific management, and therefore of appropriate management information systems, is to increase efficiency. In the introduction of his book Taylor quotes the former US president Roosevelt: "The conservation of our national resources is only preliminary to the larger question of national efficiency" [14].

Efficiency can be defined as a relationship between the positive outcomes of a process and the required effort to generate these outcomes. A typical form of efficiency is a ratio. The enumerator represents the outcomes, e.g. in terms of revenues for sold products, the denominator the effort. The effort can be quantified by costs [15].

However, other quantifications can be applied. Here, life cycle assessment and in particular eco-efficiency approaches, come into play, e.g. contributions to climate change or cumulative energy demand [16, 17]. In other words: Life cycle assessment

is the basic concept used to calculate the denominator of eco-efficiency ratios. Accordingly, ISO 14040 defines LCA as a "compilation and evaluation of the inputs, outputs and potential environmental impacts of a products system throughout its life cycle" [1, 2]. LCA does not comprise all flows of a material and energy flow system, e .g. a company or supply chain; all flows must be related to a product or service [18, 19]. This clarifies the intended application context of life cycle assessment. It is designed as a decision support instrument: "A decision-maker uses LCA for generating information on the environmental implications of products. For this purpose a model is set up covering the material and energy flows attributed to a product and their evaluation in view of their environmental impact" [20].

Although eco-efficiency is compatible with Taylor's philosophy of efficiency on a formal level, eco-efficiency is not a very successful concept in practice. Taylor's interpretation of efficiency is linked to another important (or the most important) action orientation in economics: profit maximization or value creation. We have, thus, two slightly different interpretations (or dimensions) of efficiency: On the one hand efficiency of a sustainable society that tries to avoid inadvertent damages to its natural environment and, on the other hand, an interpretation of efficiency which has its origins in the basic action orientation of the economic system. Efficiency in the second interpretation is a generalized value in modern industrial societies.

It is, after all, not surprising that the new concepts are not applied in practice: They are not compatible with basic action orientations in the social subsystem of economy. One way to make the new concepts more attractive is to include the second dimension of efficiency, i.e. by including cost accounting. In fact, cost accounting components make the software systems more attractive. Many companies apply the new concepts mainly because they incorporate new cost accounting concepts that allow new insights: waste of energy and resources. Material flow cost accounting (MFCA) is such a new concept [21]. However, these information systems cover only so-called win/win-constellations: We increase eco-efficiency only if it has a positive impact on profit maximization.

Another starting-point could be to question the generalized action orientations. Conventional and enhanced management information systems are not designed to support that. At least, these are not the only forms of IT support in organizations. To apply information technology in this regard, the question is how social subsystems and their systemic mechanisms and action orientations emerge in societies and how the action orientations can be modified or enhanced.

3 The Theory of Communicative Action

To answer these questions we applied Habermas' theory of communicative action. Habermas' concept of society [10, 11] distinguishes lifeworld and social subsystems like the society's economy or public administration. "From the internal perspective of lifeworld, society is represented as a network of communicatively mediated cooperation… What binds sociated individuals to one another and secures the integration of society is a web of communicative actions that thrives only in the light of cultural traditions, and not systemic mechanisms that are out of the reach of a member's intuitive knowledge" [22]. Communication is not interpreted as information exchange

between decision makers but as a special form of action: communicative action. This interpretation of the role of communication in a society is based on the speech act theory by Austin [23] and Searle [24].

Habermas' concept of lifeworld does not fit into the understanding of computer support discussed in the previous section. However, computers are not only used for decision support in economic and public administration. Email, chat and many Web 2.0 applications stand for a completely different form of computer use. Habermas' concept of lifeworld helps to better understand these developments.

The lifeworld is not another separated social subsystem besides others. It is rather a different perspective: an internal perspective. Winograd and Flores have applied the internal perspective of communicatively mediated cooperation to the management of organization beyond decision making: "In understanding management as taking care of articulation and activation of a network of commitments, produced primarily through promises and requests, we cover many managerial activities. Nevertheless, we also need to incorporate the most essential responsibilities of managers: to be open, to listen, and to be an authority regarding what activities and commitments the network will deal with. These can be characterized as participation in 'conversation for possibilities' that open new background for the conversation for action" [25].

From an external system's perspective a society can be described as a set of social subsystems. Action in these subsystems is not based on communication and discourse but on de-linguistified rules or systemic mechanisms. This set of rules includes mechanisms for self-organization and self-preservation. Members of these systems become functional units. Their activities are ideally completely rule-based: "Members behave toward formally organized action systems, steered via processes of exchange and power, as towards a block of quasi-natural reality" [26]. If software systems are to support social subsystems, appropriate software engineering is required. In fact, many concepts and modeling tools of modern software engineering meet these demands.

A special kind of functional unit can change structures: decision makers. External observers can identify different phases of decision making abstract from the lifeworld: problem analysis, goal definition information collection, decision. Decision makers optimize the structures with respect to predefined rules. In fact, if decision support systems or the underlying concepts are not compatible with the rules, they cannot be applied by decision makers.

4 Co-evolution of Lifeworld and Social Subsystems

The question is why modern societies need social subsystems? Habermas' answer is: because of complexity. He started with the ritually preserved fund of social solidarity and existing norms and personal identities in traditional societies [26]. In a process of linguistification more and more of the old norms and rules are questioned. Step by step normatively guided actions are replaced by communication-based action. This dramatically increases the complexity. Not every new solution can be consensus-based. The focus of communication is rather on new mutual insights and action orientations. Rules are an effective way of reducing complexity. Finally, this process generates new rules and generalized action orientations. So the

process of linguistification is a process of de-linguistification at the same time. "Action oriented to mutual understanding gains more and more independence from normative contexts. At the same time, even greater demands are made upon this basic medium of everyday language; it gets overloaded in the end and replaced by de-linguistified media" [27]. That's the paradox of communication: It triggers a co-evolutionary process and "modern societies attain a level of system differentiation at which increasingly autonomous organizations are connected with one another via delinguistified media of communication: these systemic mechanisms – for example, money – steer a social intercourse that has been largely disconnected from norms and values, above all in those subsystems of purposive rational economic and administrative action that, on Weber's diagnosis, have become independent of their moral-political foundations" [26]. Based on this theory, economic efficiency, as described by Taylor, cost cutting and value creation are generalized action orientations in the social subsystem of economy. It is the result of a "social evolution as a second-order process of differentiation: system and lifeworld are differentiated in the sense that the complexity of the one and the rationality of the other grow" [26].

However, communication not only allows questioning of the norms and rules of traditional societies; it also allows challenging the systemic mechanisms and action orientations in social subsystems. With regard to corporate sustainability, before developing new information systems, it is required to place emphasis on generalized action orientations in relevant social subsystems: What is the relationship between the action orientations and the concept of sustainable development? If there are contradictory forces then how can we harmonize the orientations? Based on Habermas' theory of communication action, a process of linguistification is required.

5 IT Support – Lifeworld and System

Information technology can support these processes in two different ways. To support the process of linguistification, communication and conversation support systems come into play. If new generalized action orientations emerge, computer-based management information systems for corporate sustainability are required.

Because the process of linguistification is a process of de -linguistification at the same time, this process can be characterized as a transition phase. Computer support for this transition phase should be more than arbitrary conversation support. The action orientations in the subsystems, and of sustainable development, define the background of all communication processes in this phase so that IT support for "effective communication" [28] is required.

In the following, we make use of Habermas' two perspectives: lifeworld and system. In addition, another perspective on the subject will be adopted and examined: We are looking for "transition support systems".

5.1 Lifeworld Support

As mentioned above, research in the field of applied computer science is often focused on specific social subsystems. The basic action orientations and systemic

mechanisms are adopted. The promise is that the IT systems help to optimize the structures. However, other forms of computer use play an important role in our societies: computers as a new medium of communication: Web 2.0, Twitter, chat rooms and forums on the web. Sites like Geocaching and OpenStreetMap have established new collective forms of cooperation. The most important and most dangerous aspect of many software games is that they provide a virtual background of new collective forms of life.

Habermas' definition of lifeworld: "From the internal perspective of lifeworld, society is represented as a network of communicatively mediated cooperation" can be used as well to characterize this form of computer support. Two questions arise: Can computers really support the lifeworld? The main problem in this regard is what Habermas calls the "colonization of the lifeworld" [29]: If we apply concepts and software solutions to parts of the lifeworld, we will transform these parts into parts of social subsystems. But if lifeworld support is possible: What are the images of such an interpretation of computer science?

Winograd and Flores have presented an analysis and a new approach (language-action perspective) for a special part of the lifeworld [28]. This approach is restricted to companies: companies are part of the subsystem economy as well as of the lifeworld of the members. They propose to interpret management as support for "effective communication" instead of decision-making. However, such an approach is closely related to the social subsystem of economy and cannot cover phenomena like Geocaching or Blogging. More general approaches for computer-based lifeworld support are still not available, whereas several components or basic findings of such an approach are already on hand: groupware, human computer interaction, computers as a medium etc.

In the following we discuss software applications with regard to their lifeworld support.

(1) The first example is Geocaching [30]. Geocaching is in a way a modern form of the treasure hunt. However, geocaches does not really contain treasures, the "cache items" are more or less cheap things like pencils, coins from foreign countries or similar. The geocaching website www.geocaching.com describes all available caches including their geographical position. GPS equipment is required to find the caches. If geocachers find a cache they log it on the website. There is a really significant community gathered around geocaching. Geocachers have developed their own language; they have developed special forms of communication and social interaction. These phenomena are remarkable because from a systems perspective geocaching is quite useless.

(2) A second example is instant messaging (IM). Of course, IM is not useless compared to geocaching. IM plays a more and more important role in office organization. IM has the potential to increase the efficiency and effectiveness of business processes. However, this was not an intended purpose of IM; special empirical analyses were required to prove this. Because of its group-oriented functionality (distributed cooperative work, real-time communication, planning social events, socializing) instant messaging supports teams in the workplace. Handel and Herbsleb have analyzed the content of chat and categorized chat content of instant messaging at workplaces. They found that 69% of conversations relate to specific work tasks [31]. Other reasons are negotiating availability (13%), greeting (7%), non-work (3%) and humor (5%).

Although work-related content dominates instant messaging at workplaces, data exchange between decision makers does not play an important role. This was a result of sub classifying 'work'. Handel & Herbsleb write: "We dropped 'walkthrough', 'goal', 'digression' and 'clarification' since we never observed them within the 'work' portion of our protocol" [31]. The most important sub categories were technical work, project management and meeting management. Finally, Handel & Herbsleb point out that "chat was used overwhelmingly for work discussions or for articulation work to coordinate projects and meetings, and to negotiate availability" [32]. After all, empirical analyses show that today communication support systems play a critical role in enhancing effective communication within organizations. Moreover, the fact that empirical analyses are required to understand email and instant messaging in organizations emphasizes the high flexibility of these support systems.

(3) The third example is a bit strange: We have analyzed computer tools regarding their lifeworld support capabilities [33]. Computer tools have a predefined application domain. They are not useless like geocaching. However, computer tools are very flexible and unintended usage of computer tools is quite normal. Computer tools are often described as flexible decision support applications. Excel and LCA tools are good examples. As mentioned above, decision makers should make use of the tools to take rational decisions. An interesting aspect of computer tools with respect to lifeworld support is that they often define new languages and support good arguments, for instance, in the form of special diagrams and flow charts. For example in the field of material and energy flow analysis so-called Sankey diagrams play an important role. Sankey diagrams can be thought of as the language of material and energy flow analysis including life cycle assessment [34, 35]. The results of the analyses should be presented in the form of Sankey diagrams if possible. Here, the argumentation support becomes an important purpose of the tools.

The three examples demonstrate typical characteristics of lifeworld support. The software applications have a barely or ambiguous purpose. If the applications have an impact on social subsystems, special empirical analysis is required and the impact on structures and orientations is not predictable. This results in modified software engineering models: engineering requirements must be redefined. In the use phase, empirical analyses help us to understand the impacts of the applications and to improve future versions of the application: better recognition of new languages in the community.

5.2 System Support

As already mentioned, system support applications adopt their purposes from generalized action orientations in the respective social subsystems. The software should be a step forward. The conclusions are:

(1) Optimal compatibility with systemic mechanisms is required. Therefore, extensive system integration is necessary. For example, so-called stand alone solutions are suboptimal. Highly integrated enterprise resource planning systems should be the backbone of the corporate management information systems [36].

(2) A representation of the system as a computer model helps managers to find optimal structures and procedures [37]. E.g. workflow management components do not only control all important business processes, they are as well an important interface

to the real world: all processes are recorded so that the component provides basic data for cost accounting, financial accounting etc. [38].

(3) Taylor's idea of scientific management and in particular of standards (today we discuss business processes and works flows) should result in optimal and stable structures and operations. The dynamics of the socio-economic environment is an annoying and hopefully marginal phenomenon [36, 39].

From a systems perspective, computer tools are a less than optimal solution. Normally, the use of software tools is less efficient: the efforts of data collection are high, the consistency of data is often in question and system integration is poor. They are used for dealing with the dynamics of the socio-economic environment. The tools become prototypes of future fully integrated information components. LCA tools are again a good example. LCA tools are regarded as special environmental management information systems. However, they are suboptimal because of their insufficient system integration. So, it is self-evident based on experiences with LCA tools that material and energy flow based enterprise resource planning system components should be developed.

5.3 Transition Support

One aspect of lifeworld support can be interpreted as a problem. Its support applications cannot enforce predefined orientations, including sustainable development. It can happen that our societies develop new orientations, which are quite different from current definitions and interpretations of sustainable development. However, based on Habermas' theory of communicative action, modifications and enhancements of generalized action orientations require communication. As stated above, we can interpret this process of linguistification and de-linguistification as a transition phase.

Concepts for transition phase are already well known. They help to overcome problematic structures and mechanisms with respect to basic action orientations like profit maximization. Typical examples are Business Process Re-engineering, Lean Production and Supply Chain Management [40, 41]. Even if the goals of these concepts do not have much to do with lifeworld and communication, successful implementation of the concepts does require communication. Kieser [42] has analyzed the concepts in this regard. He identified different phases and aspects of such a transition: good arguments and examples for the identification of problems, the argumentation that the problems must be solved if the organization wants to have success in the long run, the presentation of several plausible examples of how to solve the problems and the advantage of being a pioneer. Successful concepts include a new language for the communities and a set of typical visualizations. Members of the communities obtain important hints on how to operationalize basic action orientations in their social context. Often the concepts can be combined with specialized consulting concepts and software applications.

With respect to sustainable development, socio-ecological transitions were connected with events like Rio 1992 or the Stern report 2006. Concepts like business process reengineering and lean production have not played a decisively important role. Maybe life cycle assessment has the capabilities.

6 Conclusions

From the perspective of social subsystems, computer science and computer applications are useful in supporting the respective generalized action orientations and optimal systemic mechanisms and structures. This results in a problematic equivalence in applied computer science. Computer science is relevant if - and only if - it is useful in a systems perspective. Our starting point, however, is "useless" computer support: People and communities can use computers in any way they want; there is no predefined purpose. By doing this, very important developments in our societies can be examined. To analyze these phenomena we adopted Habermas' theory of communicative action. This theory allows us to make the right distinctions: lifeworld support and system support.

What is the relationship to sustainable development? Based on the theory of communication action, the challenges of sustainable development are not a problem of insufficient software support. Rather, problematic generalized action orientations in relevant social subsystems prevent substantial steps forward: socio-ecological transitions. One conclusion of Habermas' theory is that societies can modify generalized action orientations and systemic mechanisms through consensus-oriented communication in the lifeworld. It is interesting that computer based lifeworld support is possible and already available; these systems have been in discussion for several years. We interpret several important Web 2.0 applications as lifeworld support systems. Many conventional software applications, in particular computer tools, also support communication processes in the lifeworld (or they provide corresponding components). However, lifeworld support includes that we cannot enforce and plan a sustainable development. So it is not useful to implement a "Sustainability Management System" in order to support the transition phase. Sustainability Management Systems, to support sustainability governance as well as enhanced EMIS, will be the second step.

References

1. International Standardisation Organisation: Environemental Management – Life Cycle Assessment – Principles and Framework – ISO 14040. Paris (1996)
2. Guinée, J.B. (ed.): Handbook on Life Cycle Assessment – Operational Guide to the ISO Standards. Kluwer Academic Publishers, Dordrecht (2002)
3. Möller, A.: Grundlagen stoffstrombasierter betrieblicher Umweltinformationssysteme. Projekt-Verlag, Bochum (2000)
4. Page, B., Rautenstrauch, C.: Environmental Informatics – Methods, Tools and Applications in Environmental Information Processing. In: Rautenstrauch, C., Patig, S. (eds.) Environmental Information Systems in Industry and Public Administration. Idea Group Publishing, Hershey (2001)
5. PAS 1025: Austausch umweltrelevanter Daten zwischen ERP-Systemen und betrieblichen Umweltinformationssystemen. Beuth-Verlag, Berlin (2003)
6. Isenmann, R., Arndt, H.-K., Brosowski, J., Marx-Gómez, J., Schappert, M.: Using Internet Technologies and Services for Sustainability Reporting: Research Initiative, Agenda, Early Results. In: Hryniewicz, O., Studzinski, J., Romaniuk, M. (eds.) EnviroInfo 2007 – Environmental Informatics and Systems Research, Shaker, Aachen, vol. 1 (2007)

7. Wohlgemuth, V., Mäusbacher, M.: Analyse umweltrelevanter Daten in SAP und Implementierung einer Beispielanwendung zum Datenaustausch mit betrieblichen Umweltinformationssystemen (BUIS). In: Hegering, H.-G., Lehmann, A., Ohlbach, H.J., Scheideler, C. (eds.) Informatik 2008, Beherrschbare System – dank Informatik. LNI, vol. 2. Gesellschaft für Informatik, Bonn (2008)
8. Funk, B., Möller, A., Niemeyer, P.: Integration von ERP- und Umweltinformationssystemen – Status quo, Perspektiven und Anwendungsfelder. In: Hegering, H.-G., Lehmann, A., Ohlbach, H.J., Scheideler, C. (eds.) Informatik 2008, Beherrschbare System – dank Informatik. LNI, vol. 2. Gesellschaft für Informatik, Bonn (2008)
9. Funk, B., Möller, A., Niemeyer, P.: Integration of Environmental Management Information Systems and ERP Systems using Integration Platforms. In: Athanasiadis, I.N., Mitkes, P.A., Rizzoli, A.E., Marx Gomez, J. (eds.) Information Technologies in Environmental Engineering. Springer, Heidelberg (2009)
10. Habermas, J.: The Theory of Communicative Action, Reason and the Rationalization of Society, 3rd edn., vol. 1. Beacon Press, Boston (1985)
11. Habermas, J.: The Theory of Communicative Action. In: Lifeworld and System: A Critique of Functionalist Reason, 3rd edn., vol. 2. Beacon Press, Boston (1985)
12. French, S., Turoff, M.: Decision Support Systems. Communications of the ACM 50(3), 39–40 (2007)
13. Rautenstrauch, C.: Betriebliche Umweltinformationssysteme – Grundlagen, Konzepte und Systeme. Springer, Heidelberg (1999)
14. Taylor, F.W.: The Principles of Scientific Management, p. 7. Harper & Brothers Publications, New York (1907)
15. Beattie, B., Taylor, R.: The Economics of Production. John Wiley & Sons, Chichester (1985)
16. Huppes, G., Ishikawa, M.: Why Eco-Efficiency? Journal of Industrial Ecology 9(4), 2–5 (2005)
17. Huppes, G., Ishikawa, M.: A Framework for Quantified Eco-Efficiency Analysis. Journal of Industrial Ecology 9(4), 25–42 (2005)
18. Berlin, D., Uhlin, H.-E.: Opportunity cost principles for life cycle assessment: toward strategic decision making in agriculture. Progress in Industrial Ecology 1, 187–202 (2004)
19. Frankl, P., Rubik, F.: Life Cycle Assessment in Industry and Business – Adoption Patterns, Applications and Implications. Springer, Heidelberg (2000)
20. Werner, F.: Ambiguities in Decision-oriented Life Cycle Inventories, p. 5. Springer, Heidelberg (2005)
21. Möller, A., Prox, M.: From Material Flow Cost Accounting to MFA and LCA. In: Proceedings of the Eight International Conference on EcoBalance 2008 - The Challenge of Creating Social and Technological Innovation Through System-Thinking, Tokyo, Japan (2008)
22. Habermas, J.: The Theory of Communicative Action. In: Lifeworld and System: A Critique of Functionalist Reason, 3rd edn., vol. 2, p. 148. Beacon Press, Boston (1985)
23. Austin, J.: How to Do Things with Words. Harvard University Press, Cambridge (1962)
24. Searle, J.: Speech Acts. Cambridge University Press, Cambridge (1969)
25. Winograd, T., Flores, F.: Understanding Computers and Cognition, p. 151. Addison Wesley, Reading (1986)
26. Habermas, J.: The Theory of Communicative Action. In: Lifeworld and System: A Critique of Functionalist Reason, 3rd edn., vol. 2, pp. 153–154. Beacon Press, Boston (1985)
27. Habermas, J.: The Theory of Communicative Action. In: Lifeworld and System: A Critique of Functionalist Reason, 3rd edn., vol. 2, p. 155. Beacon Press, Boston (1985)

28. Winograd, T., Flores, F.: Understanding Computers and Cognition. Addison Wesley, Reading (1986)
29. Habermas, J.: The Theory of Communicative Action. In: Lifeworld and System: A Critique of Functionalist Reason, 3rd edn., vol. 2, p. 332. Beacon Press, Boston (1985)
30. Geocaching - The Official Global GPS Cache Hunt Site, http://www.geocaching.com/
31. Handel, M., Herbsleb, J.D.: What is chat doing in the workplace? In: Proceedings of the 2002 ACM Conference on Computer Supported Cooperative Work, Louisiana, USA, p. 6 (2002)
32. Handel, M., Herbsleb, J.D.: What is chat doing in the workplace? In: Proceedings of the 2002 ACM Conference on Computer Supported Cooperative Work, Louisiana, USA, p. 8 (2002)
33. Möller, A., Prox, M., Viere, T.: Computer Support for Environmental Management Accounting. In: Schaltegger, S., Bennett, M., Burritt, R. (eds.) Sustainability Accounting and Reporting. Springer, Dordrecht (2006)
34. Schmidt, M.: The Sankey Diagram in Energy and Material Flow Management. Part I: History. Journal of Industrial Ecology 12(1), 82–94 (2008)
35. Möller, A., Michelsen, G.: Voraussetzungen einer IKT-gestützten Nachhaltigkeitskommunikation in Unternehmen. In: Bichler, M., et al. (eds.) Multikonferenz Wirtschaftsinformatik 2008. GITO-Verlag, Berlin (2008)
36. Funk, B., Möller, A., Niemeyer, P.: Integration of Environmental Management Information Systems and ERP Systems using Integration Platforms. In: Athanasiadis, I.N., Mitkes, P.A., Rizzoli, A.E., Marx Gomez, J. (eds.) Information Technologies in Environmental Engineering. Springer, Heidelberg (2009)
37. Rolf, A.: Grundlagen der Organisations- und Wirtschaftsinformatik. Springer, Heidelberg (1998)
38. Möller, A., Prox, M., Viere, T.: Computer Support for Environmental Management Accounting. In: Schaltegger, S., Bennett, M., Burritt, R. (eds.) Sustainability Accounting and Reporting, p. 608. Springer, Dordrecht (2006)
39. Simon, E.J., Porto de Albuquerque, J., Rolf, A.: Notwendige und vorläufige Formalisierungslücken in Organisationen. In: Funken, C., Schulz-Schäffer, I. (eds.) Digitalisierung der Arbeitswelt: Zur Neuordnung Formaler und Informeller Prozesse in Unternehmen. VS Verlag, Wiesbaden (2008)
40. Hammer, M., Champy, J.: Reengineering the Corporation. Harper Collins Books, New York (1993)
41. Hlupic, V., Robinson, S.: Business Process Modelling and Analysis Using Discrete-Event Simulation. In: Proceedings of the 1998 Winter Simulation Conference. IEEE Computer Society Press, Washington (1998)
42. Kieser, A.: Moden und Mythen des Organisierens. Deutsche Betriebswirtschaft 56, 1 (1996)

Utilising the Internet to Improve Peasant Artisan Incomes: Evidence from Mexico

John Dobson[1] , Richard Duncombe[2], and Brian Nicholson[1]

[1] Manchester Business School, The University of Manchester, Booth Street West, Manchester, Gtr Manchester M15 6PB, UK
[2] School of Environment and Development, The University of Manchester, PO Box 88, Manchester, M60 1QD, UK
john@southoftheborder.ca, richard.duncombe@manchester.ac.uk, brian.nicholson@manchester.ac.uk

Abstract. This paper examines whether the Internet can be used to improve peasant artisan incomes by connecting producers directly with global markets. The paper surveys previous research which suggests that Business to Business artisan portals within most Developing Economies have failed to deliver expected benefits. This paper identifies some of the significant obstacles to successful implementation and presents an institutional framework that provides for rational incentives. Drawing upon new institutional economics, we propose that the Internet can be the catalyst for positive change in artisan incomes. To illustrate the argument, we examine institutions within the Mexican handicraft market and highlight current challenges. The proposal presented involves readily available technology for both artisan and small retail stores to exploit their comparative advantage, leading to a sustainable model for artisan economic development.

Keywords: New Institutional Economics, Livelihoods and Markets, Innovation, Handicrafts, Development, ICT, Internet, Developing Economies.

1 Introduction

Travellers to developing economies (DEs) often encounter locals selling handicrafts. Products can be locally made or brought in from various regions of the country to satisfy tourist demand for 'authentic' goods. Purchasing such items is considered integral to both the visitor's tourist experience and an important part of livelihood strategies for peasant communities. Based on these premises, handicraft production has historically been identified as an invisible export and part of a survival pattern for peasant communities [1]. This area of trade and development is important and a number of organisations such as UNESCO through their 'Seal of Excellence' and the Fair Trade Movement are attempting to improve artisan incomes that derive from the expansion of global markets for handicrafts. The sustainability of these ventures is based on the ability to gain and maintain market share. However, sustainability of

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 292–309, 2010.

development initiatives is difficult to maintain with low quality production. The issue of poor quality (e.g. cracks, poor fit and finish) must be overcome to complete the transactions and ensure repeat business. However, defects can also be passed off as normal characteristics of handmade items that perhaps add authenticity to the product. The sale may have an implicit acknowledgement of unsatisfactory quality by one or both parties if during negotiation the vendor mentions or the buyer considers the charitable benefit associated with completing the exchange.

Based on an analysis of evidence from the Mexican handicraft industry, this paper will discuss the causes of low quality production and the resulting low artisan incomes.Research indentifies potential benefits of Information Communication Technology (ICT) for increasing DE participation in international trade [2, 3]. This paper builds upon Boateng's research plus that of Pare [4] to examine the causes of high failure rates of Information Communication Technology for Development (ICT4D) initiatives. While there tends to be general agreement on the potential benefits of ICT4D, the results have been disappointing. Some researchers identify structural problems such as limited access, high cost and lack of human capital to successfully implement ICT4D [5]. Other research [2] examined institutional barriers that contributed to the high failure rates. Successful Business to Business (B2B) projects require contextualising technology applications to local conditions.

While there is a concern that globalisation has undermined peasant livelihood options, Medina and Santos [1] highlight the opportunity for economic development through the exploitation of indigenous handicrafts. The Ricardian model of comparative advantage calculates that world trade should be 500% higher [6]. Where is the missing trade? Pare [4] proposes that Transaction Costs of these types of B2B portals are still too high for these initiatives to be successful. Institutional theory builds upon the transaction cost paradigm to help explain why markets fail to realise opportunities. Our research focuses on how peasant artisans can utilise the Internet to further sustain economic development.

There may be applications for development practitioners attempting to establish sustainable livelihood initiatives in other DEs. We highlight opportunities for handicraft producers from DEs to use ICT to exploit their comparative advantage (i.e. low production costs, product customisation) while moving up the value chain. ICT may be viewed as a tool that can bypass the current obstacles (blocking agents) to successful development and it can be coupled with the application of new institutional economic (NIE) theory to e-commerce projects. NIE theory can assist in developing sustainable solutions by contributing knowledge on: establishing rational incentives to produce higher quality products, increasing accountability, providing information feedback and establishing innovation rents. ICT may foster institutions that will encourage innovation and permit sustainable peasant artisan development. Once the technical implementation and infrastructure is built, peasant entrepreneurs should be able to work at the margins [7] to dramatically improve incomes.

We attempt to provide an initial theoretical approach for practitioners and researchers. By combining NIE theory with market based approaches (or business theory) the paper attempts to build a new framework for researching ICT4D initiatives. An NIE perspective of participant behaviour could yield opportunities to change incentives within specific industries to make livelihood projects more sustainable. The development practitioner may discern more complex explanations for

project underperformance and identify new approaches that will increase the likelihood of future implementation success.

The paper is divided into three sections. The first section will examine both NIE and ICT4D literature. We examine North's seminal work on the role of institutions in successful development and review current ICT literature from an institutional paradigm, to understand the general causes of development failure. Section two examines the specifics of the Mexican handicraft market. Game theory is used to highlight behaviour that tends to deviate from modern business practices and often results are both low quality production and sub-optimal welfare outcomes for peasants. Artisan survival behaviour must be understood prior to successful implementation of future development initiatives. The third section attempts to provide a way forward for both researcher and practitioner. ICT is a tool that has dramatically lowered transaction costs, yet development has failed to materialise. ICT can be an effective tool in creating sustainable community development by altering the incentives within the handicraft industry to rationally connect artisans with global markets. The relationship requires careful management for both the buyer and the artisan. A development manager (DM) helps lower the transaction cost while mitigating risk for the buyer and seller. The role of the DM is critical and manages both buyer and seller expectations of the transactions given these parties come from vastly different societies. While understanding the need to contextualise technology to local conditions, this ICT4D proposal identifies institutional transformation within the handicraft industry, as a key to sustainable development. Providing artisans with rational incentives to improve quality should dramatically increase incomes. The paper provides a theoretically sound approach to B2B relationships in DE. Future research will be directed at piloting the proposed implementation concepts.

2 Literature Review and Relevant Concepts

The ability to maintain market access may be ultimately determined by the ability of producers to respond effectively to market requirements. The first suggestion to improve artisan production builds upon the concept of Lean Production successfully used by Toyota. Toyota, after WWII rebuilt production with depleted resources by creating 'just in time' production. Peasant artisans with limited capital can benefit from a similar production approach by first finding the buyer and producing to meet demand. The second aspect is then to ensure a quick response to market demands. Zara Clothing Company (Zara) created a competitive advantage by using this strategy [8]. The lessons from these two approaches can be applied within the handicraft market to establish a supply chain. The process involves converting previously considered weaknesses, of limited capacity and primitive technology, to create a competitive advantage of shorter production cycles, customisation and 'just in time' delivery. Historically the dramatic drop in transportation and communication costs facilitated specialisation and promoted international trade. The Internet is a tool that may provide opportunities for small scale producers to market directly to small retail consumers, thereby aligning production capacity with consumption or market needs.

Research done [2] tends to group ICT4D literature into three main themes. The first area of research focuses on the potential benefits and constraints of e-commerce to

further development. This includes the need to contextualise ICT initiatives to local realities. While acknowledging the role of institutions in creating challenges, it tends not to address the institutional constraints. This research tends to simply be content to indentify the problem. This presents institutions as unexamined black boxes that can be signalled as part of the causes for development failure. The second main theme deals with the technical barriers of B2B initiatives. This research tends to focus on limited access in DE, proportionally higher costs in DE versus Developed Countries, or the lack of human capital to successfully implement ICT4D. This approach could be identified as the 'field of dreams' explanation: "If we build it, development will happen". Mann [9] argues that once the technical obstacles are overcome developing economies will leapfrog. The third theme deals with support and implementation of initiatives. The topics tend to discuss issues of support by government and practitioners [2].

There is a widening gap in economic performance between many DE and Developed Economies that is caused by insufficient input spending on IT (software and equipment) rather than productivity shortfall [10]. Some of the technical issues include accessibility; research finds that in Mexico, Internet access consumes 5% of disposable income. The two most important barriers to successful e-commerce tend to be cost and limited resources [5]. Further hindering decisions to invest, in B2B initiatives, is inability of disadvantaged firms to absorb financial losses [11]. The research done by Pare [4] indentifies other technical problems such as; issues of quality, payment settlement, logistics and customs as still impeding development.While acknowledging that technical deficiencies must be addressed prior to successful introduction of modern factories and realisation of economies of scale, most ICT4D research was not concerned with macro economics, but examined industries, communities or individual firms. The technical explanation fails to explain why available technologies are not adopted and people do not utilise existing knowledge to maximise profits or product quality [12].

Heeks and Wilson [13] argue that a technical explanation tends to present a very narrow view of the development challenges and fails to recognise the complex interplay of social, cultural and economic arenas within any industry. Technology should be appropriate within a socio-cultural environment and attempt to build trust [2]. Boateng further argues that there is a knowledge gap between understanding the potential benefits and the ability to contextualise the problem within societal institutions. The research shows that there is an unrealised potential. There is a major incentive for (artisan) firms to adopt ICT and gain market access [2]. However, the Internet is primarily used for email and most had never used the Internet for market research [2]. Unfortunately, research done by Pare [2] found that the benefits may be overstated. More discouraging were Batchelor and Webb [14] who were unable to find a single Internet based B2B transaction and many of the ventures studied have closed. Stating the Internet has limited prospects for selling handicraft, they recommend that initiatives should focus on "ethical (fair trade) tourism" [13]. The diffusion of technology is making the process easier, but it does not make it automatic [15].

The drop in communication costs have failed to create new markets even though buying direct presents the potential of substantial price savings. Flexible manufacturing and mass-customization have been topics of managerial research for some time. Given the extensive ability of e-Commerce applications to capture user preferences and behaviour, it is odd that researchers have not fully explored the challenges and

consequences of integrating these systems with mass-customization design and manufacturing systems [3]. Development practitioners proposed that DE handicraft development could similarly benefit from vigorous adoption of ICT. Rabinovich et al [16] find that Internet based purchases are able to deliver efficiencies by allowing buying decisions to be postponed. The efficiencies benefit both the supplier and consumer [17]. Yet most retailers have avoided buying directly and continue to use traditional distribution methods such as sales reps and trade shows. A reason cited by Pare [2] is that the introduction of the Internet has not reduced the transactions costs to an extent where a significant impact on Artisan B2B sales takes place. The portals have not lowered the coordination costs or lowered information asymmetry sufficiently to encourage the adoption of this new supply chain. While tending to agree with the conclusion reached by Pare, there is still an element missing from the discussion. It is counter intuitive that the substantial price difference between the LDC market price and the DC market price has not encouraged entrepreneurial investment. The lack of sustainable ventures tends to indicate that the vast majority of investments fail. Examining institutional deficiencies is required to help explain these setbacks.

Repeat business is critical to provide the incentive to improve quality. Online feedback mechanisms have emerged as a viable mechanism for fostering cooperation among strangers in such settings by ensuring that the behaviour of a trader toward any other trader becomes known [18]. The trust mechanism in e-commerce must be built [19]. The international customer would have the ability to order products as required with minimum investment. Rabinovich et al [16] find that Internet based purchases are able to deliver efficiencies by allowing buying decisions to be postponed. Retail buyers are able to customise products in small batches. This presents the small scale artisan with a potential advantage.

NIE incorporates a much more complex explanation of deficient institutions and perverse incentives than can be covered in this paper[1]. The focus here is on some aspects of NIE that deal specifically with market mechanisms. The implications are that by altering institutions to provide rational incentives, economic development would develop organically. The process involves altering market demand for handicrafts. The current paradigm involves maximising profits, price competition, high discount rate, low loyalty, poor quality and ultimately low artisan income.

NIE theory [12, 20] provides an explanation for why states fail to develop robust institutions and the resulting development failure. The infrequency of “late late” developers indicates the difficulty in successfully overcoming socialised behaviour. There is extensive research on ICT readiness. A common theme focuses on the technical obstacle (costs of infrastructure and access) to sustainable B2B projects. B2B initiatives focus on business to business portals. Researchers further examine the need to appropriately introduce ICT within local contexts [2]. While agreeing that any ICT4D initiative must be contextualised within the normative rules of society, we argue that ICT can potentially by-pass the barriers to development and create new institutions.

Entrepreneurs must consider many factors in determining investment decisions. The overriding consideration is the likelihood that the investment will generate a

[1] For a more detailed explanation see [38] and [39].

profit to warrant the risk incurred. While opportunities will vary between industries and countries, Neo-classical economics indicate that profitability should be greater in a DE, since the ratio of labour to capital is lower [21]. This does not reflect the historical pattern of investment. NIE emerged as an effort to explain failure of DEs to develop, by building on the neo-classical model of scarcity and adding a role for institutions [20]. Game theory concept of cheating[2] may be considered part of an unresolved distributional conflict. In the Mexican handicraft industry it results from low sanction and accountability mechanisms. In pre-modern societies relationships were clan or family centred, resulting in low transaction costs and high accountability, therefore ideology and culture can help explain the persistence of 'inefficient' markets [20]. When opportunities for innovation or trade occurred, existing institutions must undergo adaptation. It is institutions that reduce uncertainty and permit non-personal exchange, allowing for specialisation and realisation of economies of scale [21, 22]. However, in most societies misaligned incentives result in suboptimal economic performance. The inability to resolve the conflict between institutional constraints and economic opportunity makes the process of economic development prone to breakdown.

Individuals invest based on the certainty that deferring consumption in favour of accumulation will result in a high payoff [21]. Insecure property rights discourage economic growth. The process of improving quality requires healthy competition that permits innovation rents. Historically, organisations like champagne fairs and trade guilds enforced scarcity and guaranteed quality [23]. What makes champagne valuable is the precise balance of scarcity and reputation for quality that has developed based on competition from various producers within the region and external competition with other producers of sparkling wine. The medieval world was able to have non-personal exchanges dispersed across continents. It did not seem to matter if products or money were sent first [24]. Societies had been able to institutionalise community responsibility.

It is generally understood in development literature that perverse incentives that reward cheating lead to underdevelopment. This results in low quality production for much of the Mexican handicraft industry. When examining the handicraft industry we find millions of artisans struggling to acquire the very basics for human existence [25] in an industry dominated by the most marginalised members of peasant communities [26]. The marketing is mostly carried out by women and children at various markets and town squares throughout the country. This process leads to path dependence which places a sub-sector of society on the road to continuous underperformance. The condition, while not permanent is difficult to change once behaviour has become socialised [20]. In comparing successful developers from unsuccessful "there is little doubt that the 'good' institutions established in the settler colonies formed the foundation of current prosperity" [27]. The institutional framework that marginalises these populations facilitates the emergence of blocking agents which conspire to thwart economic progress by undervaluing handicraft production.

[2] The literature reviewed on game theory use the terms 'cheat', 'appropriate' and 'defect' interchangeably.

3 The Handicraft Market - Today

Throughout the world artisans live on the fringes of societies, a marginal and precarious existence [28]. Artisan production is influenced by market forces and non market forces such are societal obligations [26]. Production is usually carried out by landless peasants, who hope to earn enough to gain access to land to become subsistent farmers. Handicrafts are a viable income option for peasants, since products are usually made from readily available local materials. Products are extremely profitable on a per unit basis. The input material costs tend to be about 30% of wholesale pricing leaving a 70% residual[3]. Artisan handicraft production is mostly done at home with most members of the immediate family playing an active role. Artisan families tend to divide labour with men producing and working mechanised equipment while the women and children focus on marketing the products at local or regional markets and tourist locales. Women may also assemble beaded jewellery or other manual task while at markets. Handicraft production tends to be done during leisure time and around survival activities (like planting, harvesting or tending flocks) and societal obligations (like religious festivals, family commitments and community events). At times of strong market demand, production tends to be postponed ensuring survival activities are completed. If additional staff is considered, the first choice is an immediate family member or close friend. It is rare to find non-family members working within an artisan family business since there is a much higher risk of piracy. In these types of home based firms innovative artisans are unable to realise economies of scale by specialising the production process.

The artisan market consists of a matrix of both wholesale and retail/tourist customers comprising both domestic and international buyers. Each buyer type will be discussed. The domestic/tourist buyer tends to purchased out of a moral sense of charity. In Mexico the buyer inserts a perverse incentive for the producer since the buyer's decision is based on moral and not economic / welfare optimisation grounds. The handicraft market relies on charity in a society that tends not to be charitable [26].

The Domestic wholesale customer tends to buy at local markets to re-sell the product at tourist resorts. There is little respect for design property rights. The focus is on the lowest price to maximise profits. There is a high discount rate, since tourists at these resorts tend not to return with defective products. Mexican silver has a negative brand caused by the cumulative effect of millions of tourist buying low quality products. The international wholesale buyer often behaves similarly to the domestic wholesale buyer in the search for the best price. When and if the international buyer attempts to introduce rational incentives or western business practices there is institutional resistance. The infrequency of buying trips (only a few times per year) results in the producer having a high discount rate. "Handicrap" is a term often used by international buyers to describe the quality of products. Products often require high discounts to retail pricing once defects are discovered. Artisans rationally adjust time and effort in production in response to anticipated returns. It is in the artisan's best interest to maximise short term profits. The ability to credibly commit to repeat business is undermined by the high transactions costs associated with international travel both in terms of time and expense. ICT/Internet is able to eliminate the travel costs.

[3] Detailed research done on various handicraft cluster in Mexico for my MSc dissertation.

The low cost of accessing these products, via the Internet, has the potential of increasing transaction frequency. The added benefit of virtual travel is to substantially reduce carbon footprint which improves the sustainability of both the business model and the environment.

Game theory can help illustrate several aspects of decision making which may lead to sub-optimal welfare outcomes [29]. We will apply game theory concepts to the Mexican handicraft industry. A variation, called Agency Game, was developed to examine business cooperation. In this game the principal acts first in deciding whether to invest in a business venture or technological innovation. Then the agent has the option of cooperating or appropriating. If the agent cooperates, both parties gain and divide the residual [30]. However, the agent has an incentive to appropriate the investment since this would earn a larger wage. If there is no consensus over behaviour and deviation is not penalised, then opportunism will dominate. Culture matters, in that once punishment becomes socialised it becomes a re-enforcing mechanism which is easily maintained. High enforcement results in almost total efficiency [30]. Low enforcement results in increased appropriators and sub-optimal outcomes for society. This explains a significant aspect of artisan production behaviour and resulting low incomes. Altering the rules of the game has the potential of dramatically improving artisan incomes. Part of the solution to ensuring cooperation is to lower the discount rate on future business. The Internet is able to encourage repeat play by easing future buying.

Agency game presents a peculiar twist in the Mexican handicraft industry. Research indicates that in rural Haciendas of the 18th Century, it was the peasant that deliberately assumed large debt to guarantee employment [31]. The societal institutions that created artificial land scarcity and labour surplus provided perverse incentives for individuals to become indentured. Game Theory indicates that appropriation should preclude repeat play. In the Mexican handicraft market workers still respond to the scarcity of few buyers by appropriating cash deposits to ensure future income.

The Principal provides the Agent with cash from advance from which they are to buy materials for their piecemeal work. The Agent must have a low discount rate, since appropriation will earn the highest income if there is no repeat play. Appropriation usually occurs within the first two years, as the Agent is 'forced' to take the cash advance; the usual cause is a social commitment, or unforeseen medical emergency. There is very little legal recourse available. First, the amount of the loan is relatively insignificant to the principal. Second the peasant can simply hide until the buyer leaves town. Third the time and costs involved pursuing legal recourse often exceeds the loss. Consequently appropriation, rather than disqualifying the Agent, in fact serves to guarantee employment as long the Principal remains in the industry. The agent will promise to re-pay the 'loan' in the form of future production. Many foreign buyers are unwilling to accept this type of theft will write off the loss and discontinue buying. The regularity of this occurrence[4], leads to the conjecture that Mexican workers continue to utilize this modern version of indentured service which can be described as Mexican Agency Game. The Principal is forced to limit investments to

[4] While appropriation can be considered part of unresolved distributional dispute; the regularity of appropriation in all parts of Mexico indicates that this is still used as an employment guaranteeing strategy.

willingly forfeitable amounts. Orders are small and dispersed amongst various producers of similar items.

The buyer may at times request various artisans to make the same item to mitigate the risk of appropriation. The artisan has low incentive to innovate for a market that readily pirates designs. The result is low innovation and constant competition on price. Any attempt by Artisans to earn an innovation rent from design or quality is quickly undermined by the buyers the willingness to accept duplication from other producers. The process in Mexico is called 'Malbaratada', literally translated 'cheap and poorly made'. The market is continuously being supplied with cheaper less well made products which offer the potential for higher profits [32]. The low sanction for piracy and the difficulty in determining quality provides strong incentives to reduce the inputs and maximise profits. Beyond normative adherence to honesty there are few mechanisms to guarantee quality.

A relevant example occurred during a buying trip of one of the authors. After selecting a variety of items for a specific artisan and inquiry was made about a silver chain. The vendor seemed to have an unusually large quantity but the Artisan was quiet and hesitated in quoting a price. After some persistence he disclosed that the item was counterfeit Sterling. The chains had been made specifically for unsuspecting tourists but offered reassurance that the rest of the production was actually sterling. The Agent resisted cheating behaviour because he had a low discount rate for future business. However, a tourist that cannot commit to repeat business is subject to a high discount rate. The tourist would marvel at the great bargain, at least until their neck turned green.

The process of introducing rational incentives begins with understanding that producers have no incentive to improve quality because of the high discount rate and extensive piracy. An industry with low sanctions will reward cheating behaviour. This can be most easily accomplished by lowering the quality of inputs (materials, time, and effort). What has emerged is the 'Malbaratada' or market for lemons. However, Game Theory demonstrates that repeat play is sufficient credible commitment to increase welfare outcome. The goal is to successfully combine relevant aspects of NIE theory, such as property rights, innovation rents, lowering transactions and increasing non-personal exchange, to existing Internet technology. This approach has the potential of creating an institutional framework that can provide rational incentives to improve quality.

4 Moving Forward: Connecting Artisans to Global Markets

Altering the incentives may not be possible until blocking agents are removed. Mexican society inserts perverse incentives that undermine development of a rational industry. Within the silver industry, the national government involvement in promoting the silver industry may in fact undermine quality and encourage the production of unmarketable products. The Feria Nacional de Plata's mandate is to promote the Taxco Silver industry. The mandate states that Taxco's silver production is part of Mexico's pre-Hispanic heritage. Artisans from any region of Mexico are welcomed to submit products. Part of the mandate is to promote culture [33]. The National Silver

Fair has created the myth of Taxco as an ancient silversmith centre. Evidence shows that the industry actually began in 1931 when William Spratling started the first silver shop [34]. The mandate undermines the establishment of an innovation cluster by not limiting production to a geographic area, like Champagne. The winner of the design competitions is presented with a trophy of an Aztec warrior from the President of the Republic [34]. The artisan becomes a defender of Mexico's pre-Hispanic culture. The production of pre-conquest cultural representations has encouraged the production of non marketable items. Many of the best workshops in Taxco proudly display winning production. These items are readily offered for sale with very few buyers. The government's attempt to promote the silver industry misaligns the incentive structure and has encouraged artisans to misappropriate investments of time, effort and resources. NIE explains how behaviour once institutionalised is difficult to change.

The handicraft market could build new institutions to rationally align the principal/agent relationship or producer/buyer. Protecting artisan property rights, limiting piracy and credibly committing to repeat business should encourage innovation (and corresponding rents) and sustainable repeat business. The process is cost effective using existing Internet technology.

The project involves prototyping and establishing an Internet portal to connect producers to small retailers in international markets. Both these groups have failed to realise some of the potential benefits of globalisation because of their respective small size. Most small retail stores, in developed countries, have been unable to buy directly from overseas suppliers. The challenge is that manufacturing companies require minimum 40 foot container loads of any specific item. This is unrealistic method of purchasing for retail stores since the volume and cash flow requirements preclude this type of investment. The second difficultly is any attempt to buy directly from handicraft producers faces a high transaction cost. Therefore, most small retail stores continue to rely on traditional distribution systems. The inability to access DE suppliers results in sub-optimal performance when faced with competition from large multinational who realise these economies of scale. The current supply chain effectively excludes artisans from participation. Small producers are unable to meet the requirements of both quality and quantity manufacturing of large multi-nationals corporations. What is required is a unique supply chain that focuses on the strengths of both artisan producer and small retail consumer.

The proposed initiative requires the creation of an intermediary, or Development Manager (DM) to act as an agent of change, instituting NIE theory on the industry. This is accomplished utilising ICT to help create new institutions. The DM would be based in the artisan community with the job of coordinating the purchase from various artisans for international buyers. DMs are capable of changing the paradigm by using small scale production of various artisans as an asset instead of a liability. The Internet can connect producers, which can only produce small quantities with consumers that only require small amounts and require a lot of variety. A retail store is able to purchase as little as a small box to be profitable.

Retail stores do not currently capitalise on these potential profits because of the risks associated with international commerce. As well, because they only require small quantities the transaction costs of directly travelling to many regions of the world is prohibitive. An Internet portal could allow retail stores to buy small quantities directly

without travelling. The financial transactions would be handled through an intermediary company based in the developed world. This would lower the risks for buyers, since western businesses have historically adhered to reputation and honest business practices to lower the transaction costs [35]. This would serve to mitigate the risks associated with direct buying. This portal could connect thousands retail stores with hundreds of artisans employing thousands of artisans. The Internet is a tool to help build a solution. What is required is the establishment of incentives for quality and innovation. The role of the DM is to train and educate artisans to market demands and protect artisan design rights by allowing them to profit from innovation rents. The DM must therefore be an honest broker, ensuring the rights of the buyer and seller are protected. Prior research identifies how 3rd parties are able to increase trust in a system by minimising the potential of fraud [24].

The role of the DM is critical in ensuring property right protection. Assistance may be provided involving cosmetic changes in colour or patterns based on current trends or more substantive product modification. The goal is to take what is being produced and modify it to what customers actually want and when they want it. The process involves working within existing technical capacity to create the best possible product. Overcoming the discount rate is the difficult part, since the producers function in a market that seeks 'Malbaratada'. Establishing innovation rents should encourage investment in better products and increase the likelihood of repeat business. To establish rational incentives to innovate, the artisan maintains an innovation rents to their design within the Internet portal. As orders increase, the artisan will face increase demands on their leisure time. The profit potential should encourage some to invest in productivity enhancing technology or hiring of specialised labour. The risk of hiring non-family labour has already been discussed. Once an employee has been hired it would be difficult to prevent the designs from being appropriated and diffusing into the local market. This loss would be mitigated, for the artisan, if there are consistent Internet orders to offset losses in the local market. The piracy into the local market will be difficult to stop. It does have a positive spill-over effect of helping educate the other artisans of current trends in the market. This may help strengthen the existing local market and increase general demand.

The high margins and the ability to differentiate competitors will encourage repeat purchases of items that sell well. The process of repeat purchases will provide the appropriate information feedback for producers to learn market requirements. The process allows the customer to have product arrive just in time. The benefits of direct buying are significant for the retail store. Comparing traditional buying options against the Internet Portal Direct Purchase option shows that a B2B option is profitable. $5,000 in retail sales would yield a 50% increase in profits. The biggest savings comes from the Cost of Goods Sold. In this example the buyer replaces domestically sourced products (whether imported or not) with handicrafts at market prices from a DE. There are additional expenses associated with importing directly such are duties, brokerage fees and a commission to the DM. When comparing the bottom line buying direct is much more profitable. See Table 1 for detailed numbers.

In the previous section we discussed how the high travel cost would make frequent trips impossible. The ability to buy from Mexico without travelling is technologically

possible and potentially profitable. While a $1,000 wholesale purchase to a retail store is a small investment. The same $1,000 purchase in Chiapas or any other desperately poor region is a significant amount. This process would target income to the most marginalised sectors. A few orders would have the ability to double artisan income. The inability to provide enough variety presents a challenge, however the Internet portal can overcome this problem5. The portal would permit easier re-ordering. This would provide appropriate feedback and significant positive reinforcement. Consistent re-orders should encourage additional effort and reward innovation. This approach would improve quality and create a virtuous cycle of innovation.

Table 1. Comparison of Traditional and Internet Portal Direct Purchase (IPDP)

	Traditional Purchase		IPDP	
Retail Sales	$5,000		$5,000	
Cost of Goods Sold	2,500 [37]	50%	1,000**	20%
DM Commission	-		150	3%
Freight In	250***	5%	300^	6%
Duty & Taxes	-		100^^	2%
Brokerage	-		75^^^	2%
Expenses	2,750	55%	1,645	33%
Gross	2,250	45%	3,750	68%
Net Benefit of IPDP			$1,125^*	

[37] The average margin retail is nearly 50% (source Government of Canada Website)
** A 500% margin is not uncommon
*** Freight tends to run about 10%
^Air Freight: DHL, UPS, or Fedex
^^ Hypothetical Duty & Tax Rate, since handicrafts tend to enter US, Canada & UK Duty free
^^^ Flat fee brokerage
^* versus traditional wholesale buying, not factoring financing costs

The potential benefits for artisans can be significant. While a few wholesale sales per year would dramatically raise incomes. The Internet portal could deliver regular weekly or monthly orders from a various DC buyers. To be successful the Internet portal must provide artisans with regular re-orders. The competitive advantage of artisan production is small batch and short production cycle (1-2 weeks). The quick response would allow products to arrive on store shelves within 3-4 weeks, which would provide retail stores a competitive advantage. This approached is similar to supply chain management used by Zara Clothing which produces small batches which

[5] Each cluster should offer a minimum of 500 items, and be willing to customize production to customer needs. 10 clusters will offer 5,000 items from many small producers and could provide a large percentage of the product requirements for any retail store.

enables quicker response to market demand. Zara is consistently more profitable than its rivals. The benefits to Zara clothing are achieved quicker responses to consumer demand resulting in less discounting and lowering carrying costs [8]. The artisan would be able to fulfil orders in a similar manner, from various customers. If the network of a few hundred buyers was established, innovative artisans could realise more consistent and larger orders. The goal is to exploit all of the artisan's leisure time so that it becomes more valuable. This should lower the artisan discount rate and provide rational incentives for investment (labour or productivity enhancing activities) in anticipation of future business. The artisan may also decide that it is worth the effort to improve the quality and raise the asking price on response to the scarcity of leisure time.

The obvious question is 'Why no one has picked up this $1,000 bill?' [40]. The short answer is that it is difficult to change socialised behaviour. The obstacles to successful implementation of previously discussed concept do not involve setting up of development clusters. Artisan communities exist throughout the world, creating wonderful and often low quality products. Setting up handicraft clusters has been attempted at various times with varying degrees of success by various development agencies [4, 24, 36].

This process differs from previously projects in that objective is to create demand for the product by responding to market requirements. The process may require adaptation of products to reflect contemporary needs consumer needs and would create thousands of items that could be catalogued. The biggest hindrance is finding the markets (customers). The process requires a paradigm shift in livelihood initiatives. The process of creating demand should focus in the developed world. While it seems counter intuitive to spend money in the developed world to increase the success rate of livelihood initiatives in LDC. There are thousands of potential customers (retail stores) who have the ability and incentive to invest $1,000 many times over. There are two identifiable challenges; marketing and coordination. Marketing to potential customers could be substantially more expensive than actually making the products. Coordination issues can be addressed with current technology and the hiring of a DM. The integration process would lower transaction costs for retailers. Artisans could become crucial in the business strategy for small retailers. Artisans would help retailers differentiate product selection versus big box retailers and would become a profitable category. The development focus should be to encourage retailers to take advantage of the price differential and not attempt to impose additional costs to the transaction in the form of 'charity rents'. The focus on the profit motive, what is significantly different about this proposal is the attempt to impose NIE theory into a B2B portal. Building new institutions is difficult. The potential profit motive is the motivational tool.

Figure 1 presents a flow chart of the order and delivery process. The Internet portal would allow DC retailers to purchase products without actually travelling to DE handicraft clusters. The process would be environmentally sustainable as well as lowering the transaction costs. The order process ensures non-personal transactions. The DM is an agent for the buyer and the role is to coordinate the transaction while mitigating risk by verifying product quality. (S)he has a permanent presence on the

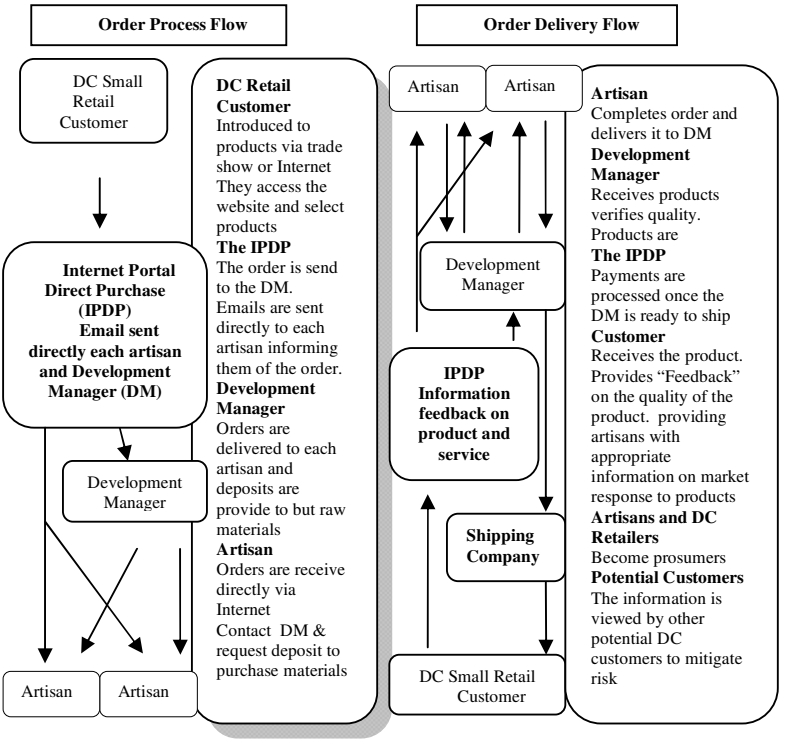


Fig. 1. Order process and delivery flow chart

community which minimises risk of artisan appropriation. The DM would work to ensure the buying process is similar to current practices in DC and is adapted to DE behaviour. The organisational structure attempts to minimise piracy and overcome the tendency to produce low quality 'Malbaratada' products. The items selected could come from various artisans allowing buyers' access to many producers. Emailing each artisan directly (if they have email) of new orders will help ensure honest DM behaviour. The artisan would be aware that there was an order and would contact the DM to arrange payment. The DM would coordinate the distribution of micro loans to facilitate the purchase of raw materials. Once production was complete the DM would arrange accept delivery of products, verify quality, pay artisan, and prepare and ship product. The DC retailer can accept product delivery with 2-3 weeks. Once product is delivered the DC retailer provides feedback on both service and products. The feedback mechanism serves multiple purposes. It provides both the artisan and DM with feedback on their service delivery. Feedback would be posted on the website. Permitting all parties to gain knowledge by 'prosuming' (producing products and information for the website while consuming information others have posted). There is a potential for learning from feedback about market demand. The DC retailers' feedback allows better decision making by current and potential customers. This process could successfully insert artisans into the global economy.

Artisans that respond to market signals would receive appropriate information feedback and quickly learn what the customer wants and adapt production. The result will be substantially improved living standards in artisan communities. The process could involve moving up the value chain by customising production or value added processes like packaging. This should create healthy competition and a virtuous cycle of innovation. Once a critical mass as been achieved of thousands of customers the development cluster concept can be replicated in other regions within Mexico or other parts of the world.

5 Conclusion

This paper attempted to build upon previous research that highlighted the high failure rate of ICT4D initiatives [4]. The goal of this paper was to provide practitioners with a framework to increase the success rate of future initiatives. This research focussed on the specifics of the Mexican handicraft industry, there may be some applications to other industries or regions. Early adopters of ICT will have to take a "leap of faith" and invest monies in anticipation of future profits. All uncertainty can never be overcome, and trust never completely secure. The entrepreneur must view any investment in a new service delivery mechanism as involving forfeitable monies. ICT4D is a tool with the potential of altering the dynamics within societies and between them.

Current approaches to livelihoods aid modality tend to focus on either charity rents characterised by the fair trade movements or supply side approaches to overcoming artisan poverty. This article examined the current method and proposed a shift in emphasis to a more market based approach. The literature presented dealt with NIE explanations for development failure in the Mexican handicraft industry. A number of aspects of NIE were presented and discussed with reference to handicraft production. The concept of Agency Game theory was used to help demonstrate how basic business processes have tended to undermine both the producer and buyer in the current handicraft market. The current market involves a matrix of buyers. The overlying feature is a few wholesale and many retail/tourist (single purchase) customers. These groups of buyers undermine the successful development of the industry because their low credibility to repeat purchase encourages artisans to cheat on inputs. A new approach is needed to overcome development failure. ICT has the potential of transforming institutions and artisan incomes by connecting producers directly with global markets. Pare's [4] previous research low success rate of DE B2B initiatives. Some artisans and practitioners will always identify the difficulties; the infrastructure may never be world class, the risk too great and the profits insufficient. Internet access, as a percentage of disposable income will probably remain higher for the LDC artisans for the foreseeable future. These technical difficulties fail to fully explain why the B2B ventures have been unsustainable. The Internet is able to provide significant market information to potential buyers. The Internet has been unable to lower the transaction costs sufficiently to encourage the emergence of a B2G handicraft portal. The coordination costs or information asymmetry may still prevent successful entrepreneurial investment unless an eternal agent or DM is able to introduce elements of NIE to the industry. Success depends on overcoming institutional failure by rationally aligning the principal agent relationship. The work should be done on the margins and

almost clandestinely to avoid institutional suppression. It requires an insertion of external agent or DM to both mitigate risk and coordinate the transaction while limiting the tendency to cheat by either party. Artisan's designs should be protected to encourage innovation. Aspects of NIE could be introduced within a non-personal transaction portal. Networks of retailers in the developed world could collectively credibly commit to repeat business. Strong property rights should promote investment in some technology that is lacking. Neo-classical theory indicates that exploiting an artisan's leisure time should encourage investments in productivity enhancing technology. While the Internet technology is readily available it is only an instrument. Success depends on building new institutions that will by-pass the current blocking agents. The focus of livelihoods projects should now include market based solutions that respond to market demand. ICT provides the possibility of connecting producers to global markets to improve livelihoods options. Research is still required on both ICT4D and contextualising NIE to local conditions.

The research presented was a theoretical explanation of low quality production. It is intended to provide development practitioners with a better understanding to some of the causes of development failure. Previous research highlighted some of the causes of B2B high failure rate. This paper provides new insights into possible solutions for the successful application of ICT4D in DE. Building a prototype will transform the concepts presented in the paper into a research project. We anticipate future research will help unlock the black box of development failure. Helping improve livelihood options for some of the most marginalise peoples.

References

1. Medina, J.F., de los Santos, E.: The Globalization of Indigenous Art: The Case of Mata Ortiz Pottery, July 22-25. American Intercontinental University Online. The University of the Incarnate Word, San Antonio (2008)
2. Boateng, R., Molla, A., Heeks, R.: E-Commerce in Developing Economies: A Review of Theoretical Frameworks and Approaches. In: Rouibah, K., Khalil, O., Ella, H.A. (eds.) Emerging Markets and E-commerce in Developing Economies, pp. 1–56. IGI Publishing, Hershey (2009)
3. Wareham, J., Zheng, J.G., Straub, D.: Critical themes in electronic commerce: a meta analysis. Journal of Information Technology 20, 1–19 (2005)
4. Pare, D.J.: Does This Site Delvier? B2B E-Commerce Services for Developing Countries. The Information Society 19, 123–134 (2003)
5. Wymer, S.A., Regan, E.A.: Factors Influencing e-commerce Adoption and Use by Small and Medium Businesses. Electronic Markets, http://www.informaworld.com/smpp/title~content=t713698725 (accessed on May 1, 2010)
6. Eaton, J., Samuel, K.: Technology, Geography, and Trade. Working paper, econ. dept. Boston University (2000)
7. Wood, C.M.: Marketing and E-commerce as Tools of Development in the Asia-Pacific Region: A Dual Path. International Marketing Review 21(3), 301–320 (2004)
8. Dutta, D.: http://3isite.com/articles/ImagesFashion_Zara_Part_I.pdf (accessed in April 2010)
9. Mann, C.L.: E-Commerce in Developing Economies Policy And WTO Negotiations. In: Working Paper 00-3. Institute for International Economics, Washington, DC (2000)

10. Jorgenson, D.W., Vu, K.: Information Technology and the World Economy. The Scandinavian Journal of Economics 107(4), 631–650 (2005); Published by Blackwell Publishing on behalf of The Scandinavian Journal of Economics, http://www.jstor.org/stable/3441018 (accessed on May 15, 2010)
11. Molla, A., Licker, P.S.: E-Commerce adoption in developing countries: a modeland instrumentn E-Commerce Adoption: An Commerce adoption in developing countries, http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6VD0-4F65K74-1-C&_cdi=5968&_user=1069281&_pii=S0378720604001314&_orig=search&_coverDate=09%2F30%2F2005&_sk=999579993&view=c&wchp=dGLbVtz-zSkzV&md5=403d63956a10079fae55ac35ec23f0d2&ie=/sdarticle.pdf (accessed on May 1, 2010)
12. Mokyr, J.: Innovation and its Enemies: The Economic and Political Roots of Technological Inertia. In: Olson, M., Satu, K. (eds.) A Not-So-Dismal Science: A Broader View of Economics, pp. 61–91. Oxford University Press, Oxford (2000)
13. Heeks, R., Wilson, G.: Technology. In: Allen, T., Thomas, A. (eds.) Poverty and Development: into the 21st Century, 2nd edn., pp. 23–48. Open University/Oxford University Press, Oxford (2000)
14. Batchelor, S.J., Webb, M.: E-commerce options for Third World craft producers: Final technical Report. DFID Knowledge and Research Project R7792' (2002)
15. Goldstein, A., O'Connor, D.: E-commerce for Development: Prospects and Policy Issues. Working Paper 164. OECD Development Centre, Paris (2000), http://www.oecd.org/dataoecd/37/61/1922730.pdf
16. Rabinovich, E., Bailey, J.P., Carter, C.R.: A Transaction-efficiency: Analysis of an Internet Retailing Supply Chain in the Music CD Industry. Decision Sciences 34(1), 131 (2003)
17. Mukhopadhyay, T., Kekre, S.: Strategic and Operational Benefits of Electronic Integration in B2B Procurement Processes. Management Science 48(10), 1301 (2002)
18. Dellarocas, C.: The Digitization of Word of Mouth: Promise and challenges of online Feedback mechanisms. Management Science 49(10), 1407–1424 (2003)
19. Gefen, D., Karahanna, E., Straub, D.W.: Consumer trust in B2C e-Commerce and the imortance of social presence: experiments in e-products and e-services. Omega 32(6), 407–424 (2004)
20. North, D.C.: The New Institutional Economics and Third World Development. In: Harris, J. (ed.) The New Institutional Economics and Third World Development, pp. 17–26. Routledge, New York (1995)
21. Leblang, D.A.: Property Rights and Economic Growth. Political Research Quarterly 49(1), 5–26 (1996)
22. Bardhan, P.: The Nature of Institutional Impediments to Economic Development. In: Olson, M., Satu, K. (eds.) A Not-So-Dismal Science: A Broader View of Economics, pp. 245–267. Oxford University Press, Oxford (2000)
23. Greif, A.: Contract Enforceability and Economic Institutions in Early Trade: The Maghribi Traders Coalition. The American Economic Review 83(3), 525–548 (1993)
24. Ba, S.: Establishing Online Trust through a Community Responsibility System. Decision Support Systems 31(3), 232–336 (2001)
25. Liebl, M., Roy, T.: Handmade in India: Preliminary Analysis of Crafts Producers and Crafts Production. Economic and Political Weekly 38(51/52), 5366–5376 (2003); Published by Economic and Political Weekly (2004), http://www.jstor.org/stable/4414435

26. Cook, S.: Price and Output Variability in a Peasant-Artisan Stone working Industry in Oaxaca, Mexico: An Analytical Essay in Economic Anthropology. American Anthropologist, New Series 72(4), 776–801 (1970), http://links.jstor.org/sici?sici=0002-7294%28197008%292%3A72%3A4%3C776%3APAOVIA%3E2.0.CO%3B2-V (accessed on August 21, 2007)
27. Acemoglu, D., Simon, J., James, A.R.: The Colonial Origins of Comparative Advantage: An Empirical Investigation. American Economic Review 91, 1369–1401 (2001)
28. Scrase, T.J.: Precarious Production: Globalisation and Artisan Labour in the Third World. Third World Quarterly 24(3), 449–461 (2003), http://www.jstor.org/stable/3993379
29. Aggarwal, V.K., Cedric, D.: Collaboration and Coordination in the Global Political Economy. In: Ravenhill, J. (ed.) Global Political Economy, pp. 28–49. Oxford University Press, Oxford (2005)
30. Cooter, R.D.: Law from Order: Economic Development and the Jurisprudence of Social Norms. In: Olson, M., Satu, K. (eds.) A Not-So-Dismal Science: A Broader View of Economics, pp. 245–267. Oxford University Press, Oxford (2000)
31. Knight, A.: Mexican Peonage: What Was It and Why Way It? Journal of Latin American Studies 18(1), 41–74 (1986), http://links.jstor.org/sici?sici=0022-216X%28198605%2918%3A1%3C41%3AMPWWIA%3E2.0.CO%3B2-T (accessed on August 7, 2007)
32. Stromberg-Pellizzi, G.: Coyotes and Culture Brokers: The Production and Marketing of Txco Silverwork. In: Nash, J. (ed.) Craft Markets of the World: The Impact of Global Exchange on Middle America Artisans, pp. 85–102. State University of New York Press, New York (1993)
33. National Silver Fair Government of Guerrero. Silver fair promotion, http://www.guerrero.gob.mx/pics/legislacion/505/DIFNPEG.pdf (accessed in May 2010)
34. Government of Guerrero website, http://www.guerrero.gob.mx/?P=readart&ArtOrder=ReadArt&Article=7331 (accessed on May 5, 2010)
35. Macaulay, S.: Non-contractual Relations in Business: A Preliminary Study. American Sociological Review 1, 55–67 (1963)
36. Tambunan, T.: Promoting Small and Medium Enterprises with a Clustering Approach: A Policy Experience from Indonesia. Journal of Small Business Management 43, 925–950 (2005)
37. Government of Canada Website, http://www.ic.gc.ca/eic/site/retra-comde.nsf/eng/h_qn00148.html (accessed on May 15, 2010)
38. Olson, M., Satu, K. (eds.): A Not-So-Dismal Science: A Broader View of Economics. Oxford University Press, Oxford (2000)
39. North, D.C.: Institutions, Institutional Change, and Economic Performance. Cambridge University Press, Cambridge (1990)
40. Olson, M.: Big Bills left on the Sidewalk: Why Some Nations are Rich, and others Poor. In: Olson, M., Satu, K. (eds.) A Not-So-Dismal Science: A Broader View of Economics. Oxford University Press, Oxford (2000)

Part 2

Critical Information Infrastructure Protection Conference (CIP 2010)

Society – Totally Dependent Upon ICT? Introduction to the CIP-2010 Conference Proceedings

William Caelli

Information Security Institute, Queensland University of Technology, GPO Box 2434, Brisbane, Queensland, 4001, Australia
w.caelli@qut.edu.au

At the 50th anniversary of the formation of the International Federation for Information Processing the simple fact that national economies and international commerce alike have become totally dependent upon the reliable and secure operation of national and global information infrastructures has been accepted. Moreover, the realization that societies are moving towards so-called *"digital economies"* has been acknowledged by all, from the citizen to the highest leader of a nation. From the early days of 1960, with a perceived competitive advantage through computer usage, to today's acknowledgement of total dependence upon computer systems and integrated data networks on a global scale, the realization that the emerging digital economy in nation states, as well as national security and societal well-being, depend upon necessary critical information infrastructures has been accepted by governments and all enterprises worldwide. From banking and finance systems to healthcare record maintenance to "e-Government" all societal activities are affected.

In particular the theme of this IFIP first CIP conference acknowledges that all basic or national critical infrastructures themselves, from electrical power systems to telecommunications structures to water/sewerage systems and so on, whether owned and operated by the public or private sector, depend fundamentally upon a national and critical information infrastructure. On a global scale the evidence is clear that nations as well as international enterprises of all natures in a global economy have moved to address this reality through relevant draft legislation, regulations, industry codes and the like.

At the same time there is recognition at the United Nations level that the rapid and almost unchecked rise of cybercrime is a reality and the concepts and reality of "information operations" and "cyber warfare" have been examined in recent years. Thus there is also recognition that imperatives for national defence have moved into cyberspace as well. Even topics related to the position of information assurance at national levels; the political, ethical and legal position related to the use of "information operations" and appropriate responses to detected "cyber-attack"; the problems of "hardening" national information infrastructures through public sector leadership and public/private sector cooperation and like themes are now topics discussed in the open media globally and almost daily.

The topic of CIIP, NIIP, NCI, or whatever term or anagram is used to describe this change, of necessity brings together the skills of computers scientists and mathematicians, engineers, information technologists and others to combine with the vital efforts of legal professionals, public and defence policy researchers, social

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 313–314, 2010.

scientists and psychologists, anthropologists, political scientists and related disciplines to address a common goal to provide effective and acceptable solutions to the growing threats.

CIP-2010 is a first and small attempt by IFIP to address these concerns with an emphasis on the international imperatives, in line with the very nature of IFIP itself. The papers in this small conference address current thinking and research in some aspects of these vital global concerns and demonstrate the varied nature of the problems identified, including the vital need for education and training efforts in the area. The conference presents a unique opportunity, at a time when nationally, regionally and internationally associated policies and legal regimes are under development, to both ponder those activities as well as to provide research leadership at both technical and policy levels.

C-SAW: Critical Information Infrastructure Protection through Simplification

Ian Ellefsen and Sebastiaan von Solms

Academy for Information Technology, University of Johannesburg,
Cnr Kingsway and University Road, Auckland Park, South Africa, 2006
iellefsen@uj.ac.za, basievs@uj.ac.za

Abstract. The importance of Critical Information Infrastructure Protection (CIIP) cannot be overlooked, as many critical systems utilise information infrastructures in order to operate. However, should these information infrastructures be targeted by cyber attacks, it would severely affect the effectiveness of many of these critical systems. Attacks on information infrastructures are not be limited to a single geographic location, all nations suffer from a collective vulnerability through interconnection, and as such nobody is immune to cyber attacks. Many nations have created internal structures to manage and react to cyber attacks on their information infrastructure. However, these structures might not always be suitable to deploy in areas where there is no CIIP mechanisms in place. In this paper we aim to present a model for a CIIP structure that will provide protection for critical information infrastructures in a manner that is cost-effective and focused on the gradual, effective deployment of a CIIP structure.

Keywords: Critical Information Infrastructure Protection, CIIP, C-SAW.

1 Introduction

Critical Information Infrastructure Protection (CIIP) is of primary concern for all nations. Many critical systems rely on large-scale interconnected networks in order to function. However, if these networks were to be attacked, many of these critical systems could be disrupted, or prevented from operating. This would cause widespread financial and economic devastation, and there is even the possibility for loss of life.

There are many different CIIP models that have been created. CIIP structures, such as Computer Security Incident Response Teams (CSIRTs) [8, 11] provide a well-understood platform for providing CIIP.

The implementation of CIIP models in developing nations is an area of concern. Many developing nations are investing in information infrastructures, but they do not have CIIP structures in place to deal with the expanding infrastructure.

CIIP structures are widely diverse, yet they all subscribe to a simple underlying philosophy; to provide support services for computer security-related incidents [2]. Generally these models are tightly coupled, and can be expensive to implement [5], which would limit their initial effectiveness in developing nations.

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 315–325, 2010.

In this paper we aim to discuss a model for providing CIIP through an analysis and simplification of the services required to create a CIIP structure. Firstly, we will begin our discussion with an introduction into CIIP. We will then present a high-level, conceptual model of current protection structures, and then present a number of drawbacks of this model specific to the developing world. Finally, we will then present the Community-oriented Security, Advisory, and Warning (C-SAW) Team that aims to address these drawbacks, and provide a platform for the creation of a mature CIIP structure. We will then discuss future work, and finally present our conclusions.

2 Critical Information Infrastructure Protection (CIIP)

A major area of focus is that of Critical Information Infrastructure Protection (CIIP). This is particularly true as the number of cyber attacks are on the increase [1]. The attacks on Georgia [9], Estonia [7], and the more recent attacks on Google [3], demonstrate the ability of cyber criminals to attack high-profile targets. However, CIIP is instrumental in negating the effects of cyber attack and as such it should be at the heart of all Information Technology policies, and governance procedures.

CIIP policies cannot only be concerned with local cyber events as the nature of interconnected networks, such as the Internet, increases the risk of a wide reaching cyber attack. Global reaching cyber attacks, such as those directed against the Domain Name System (DNS) root servers in 2002 and 2007 [6, 10], would have had worldwide effects had they been successful. This highlights an important fact; due to the nature of the Internet the world suffers from a level of vulnerability through the global interconnection of systems. As such, a cyber attack targeted at one system can affect many other systems.

Many different CIIP structure have been implemented to try to mitigate the effects of a cyber attack on national information infrastructures and critical systems. In the following sections we will discuss protection structures that are used to provide CIIP. We will then present a generalised structure in order to remove the complexities and isolate the core functionally of the many CIIP models that exist.

3 Protection Structures

There are many forms of CIIP protection structures that have been developed. Each country that implements a CIIP structure will tailor it to their environment, their procedures, and policies. In order to eliminate the eccentricities of each unique CIIP structure, we will discuss a generalised Computer Security Incident Response Team (CSIRT) structure. The aim of this approach is to isolate the core functionality that is required for a CSIRT.

CSIRTs are primarily concerned with providing protection for an assigned constituency [11]. A constituency is defined as being the group of individuals, organisations, or governmental entities for which the CSIRT is responsible. The services and structure of a CSIRT will largely depend on its constituency, and the level of protection it should provide.

The definition of a CSIRT is somewhat open-ended; however a CSIRT can be defined as a group that responds to cyber security incidents which threatens its

constituency [2, 8]. A further definition of a CSIRT is a group that provides computer security incident response services to its constituency [11]. Although the description of a CSIRT can be vague and dependent on its operating environment, there are descriptions of baseline capabilities for a CSIRT available [4] which allows the core functionally of a CSIRT to be identified.

Although a CSIRT structure can exist in many forms, a generic model can be derived. CSIRT structures can be defined in terms of several different layers, namely, the national coordination layer, the regional layer, and a number of specialisation sub-layers. However, the names given to these layers are dependent on the implementation of the CSIRT. A highly conceptual model of a CSIRT structure can be seen in Fig. 1. It is important to point out that international cooperation and participation is vital to the functioning of any CSIRT. A complete CIIP solution is provided through interaction between all the layers of a CSIRT hierarchy. CSIRTs provide a vital CIIP function, however they do have a number of drawbacks that we will outline in the following section.

Fig. 1. This figure demonstrates the high-level structure of a CSIRT. An important aspect of a CSIRT structure is the international relationships between CSIRTs. This allows for a high level of international cooperation and communication.

3.1 Drawbacks

The setup of a CSIRT structure has a number of drawbacks, which may prevent a developing nation from implementing an effective CIIP solution. Most importantly CSIRTs are expensive [5]. CSIRTs require investment in two main areas, personnel, and technology.

Personnel who operate a CSIRT must be highly trained and highly competent. For developing nations this could introduce a major hurdle, as an inadequately staffed CSIRT will not operate effectively. Together with personnel, CSIRTs require a large

investment in technology to operate effectively, however without the supporting technology, a CSIRT cannot adequately service its constituency.

A CSIRT structure may also be complex to implement "out-of-the-box", and investment would have to be made to contract expert knowledge to get a CSIRT structure operational.

Nevertheless, the drawbacks presented above do not outweigh the benefits of a CSIRT; however these constraints have to be addressed in order to create an effective CIIP structure. In the following section we will discuss our model for providing CIIP in which we aim to eliminate the need to make a large initial investment in the setup of a CIIP structure, while still providing effective and comprehensive protection.

4 Community-Oriented Security, Advisory and Warning Team

The Community-oriented Security, Advisory and Warning (C-SAW) Team model aims to provide a simplified approach to the construction of a CIIP solution. The C-SAW model will rely on the implementation of a number of C-SAW Teams, which will be designed to be deployed and become operational quickly, with a low cost overhead.

As discussed in the previous sections, a full CSIRT structure may be too expensive to set up and maintain, both in terms of personnel and technology costs. Furthermore, facilities and services provided by a CSIRT structure may be too expensive for an initial CIIP deployment; this would detract from the primary goal of a CIIP structure, which is to provide support and protection for critical information infrastructures.

In the following sections, we will discuss the construction of a C-SAW structure by attempting to identify the core services and facilities through a process of simplification. We will then discuss the possible construction of a C-SAW structure.

4.1 Simplification of Services

To identify the CIIP elements required for a C-SAW Team, we will attempt to simplify current CSIRT structures to determine what services a C-SAW Team would be required to provide.

Traditional CSIRTs provide many different services, aimed at providing a holistic approach to CIIP. These services fall into a number of different categories, namely Reactive Services, Proactive Services, and Security Quality Management Services [11].

A CSIRT structure must provide incident handling services [11], which is a mechanism for providing support for computer security incidents. This is a fundamental requirement of any CIIP structure, and will define the core of any service that is provided to the constituency. Therefore C-SAW Teams will have to provide such a service.

Many of the other services a CSIRT provides can be seen as "icing on the cake" for a CIIP structure. These services are not essential and therefore not initially required. These services could be introduced at a later stage to improve the service offerings.

At a minimum, any CIIP structures must provide these incident handling services. Services such as vulnerability and artefact handling can be beneficial to the overall service offering which a C-SAW Team could provide, but are not essential to the overall operation.

Simplification of the overall service offerings of a C-SAW Team will produce a solution that allows for a high-level of cost effectiveness. However, cost effectiveness has to be balanced with a level of quality of service. Incident handling alone will not provide adequate levels of service. In order to complement the incident handling services of a C-SAW Team, Vulnerability Management could be integrated to supplement the service offerings of a C-SAW Team, and thus increase its overall effectiveness.

To provide a good service quality to cost ratio, C-SAW Teams will aim to initially provide both Incident Handling, and Vulnerability Management services. This should be considered the bare minimum service level for a C-SAW Team. The identification of these two services types will become clear in the sections to follow.

In the following sections we will discuss the construction of a C-SAW Team, with regard to the services identified in the above section.

4.2 Construction

The construction of a C-SAW structure should be carefully considered, as this will determine the overall effectiveness of the particular solution. Ideally, a C-SAW Team should be able to support a number of attributes through its construction; we will discuss these attributes in this section.

In order to provide effective CIIP, the construction of a C-SAW Team will be analogous to that of a "user group", which is a common concept in technology circles, however the overall construction will the more formal in nature. A national CIIP structure could be constructed by creating a number of independent C-SAW Teams. These teams would provide computer security advice and expertise to a community of users.

For ease of the following discussion, a community will be defined as being a group of geographically related computer users, which are personal, commercial, or governmental in nature, and have a vested interest in computer security. The primary goal of a C-SAW Team will be to provide computer security advice and expertise to an assigned community.

There are a number of design goals that must be considered for the construction of a C-SAW structure. These goals will allow for a concrete definition of how a C-SAW Team will operate in relation to both its environment and to other C-SAW Teams. These goals are:

- Community Oriented
- Autonomous
- Geographically Independent

Each of these aspects of an individual C-SAW Team is important to define the overall operation of such a structure. Each of these goals will be discussed below.

4.2.1 Community Participation

A key aspect of the construction of a C-SAW Team is that of community participation, this will allow C-SAW Teams to provide effective and focused computer security advice and response. A C-SAW Team will be designed to provide computer security advice and response to a predefined community. The concept of a C-SAW community is analogous to that of a constituency in a CSIRT structure;

however a C-SAW Team will rely heavily on participation from the community in order to provide an adequate level of service.

The community will not be responsible for the day-to-day operation of a C-SAW Team; it will only provide an auxiliary support function. Community support and participation will allow security information to be distributed and discussed in an efficient manner. Members of the community can use the support functions provided by the C-SAW Team and the greater community, to facilitate the transfer of knowledge and to encourage the sharing of information. For instance, if a community member is experiencing a computer security-related problem, advice and assistance could be gleaned from the C-SAW Team and the community at large, this would allow problems to be identified and corrected quickly and efficiently.

Community interaction will be vital to the success of a C-SAW Team in terms of the active role the community will play in the wider education of other community members. Education of community members should be at the heart of all C-SAW services, especially in developing nations where computer security education is not widely undertaken.

Together with providing a support function, the success of a C-SAW Team will rely heavily on community participation. In the initial stages, a C-SAW Team will rely on the community in order to provide awareness, and to build a trusted base for the distribution of computer security advice and awareness. Without this initial community support and participation, a C-SAW Team will struggle to provide an adequate service. Community participation is therefore essential to the success of a C-SAW Team as an effective CIIP structure. In the following section we will discuss the autonomy of a C-SAW Team; this will allow a C-SAW Team to effectively operate without having to rely on external CIIP structures, and external communication channels.

4.2.2 Autonomous

The concept of autonomy plays an important role in the construction of a C-SAW Team. It refers to the notion that a C-SAW Team is able to function independently, and without the assistance of a controlling organisation. This concept will allow a C-SAW Team to serve its allocated community, regardless of the state of other CIIP structures.

Although C-SAW Teams would normally operate through cooperation with other C-SAW Teams, the ability to operate autonomously would allow C-SAW Teams to operate regardless of the underlying communication medium. This is especially important in developing nations where critical systems, such as electricity, and telecommunications, can be unreliable at times.

In the event of regular communication channels becoming unavailable, due to technical fault or even cyber attack, a C-SAW Team should be able to continue to operate. This will allow C-SAW Teams to service the community during periods when their services would be most required.

The ability to operate autonomously will rely on two factors, namely the technical ability of personnel, and the use of alternate communication mediums. The technical ability of personnel, especially in the spheres of information security, will allow a C-SAW Team to operate effectively, even if consultation with other CIIP structures is not possible. This will allow the C-SAW Team to provide a constant and consistent level of service to its community.

The use of alternate communication mediums will also allow a C-SAW Team to communicate effectively with its community and other CIIP structures. Reliance on a single communication medium, or underlying communication channel would prevent the C-SAW Team from operating in the event of the communication channel becoming unresponsive. By embracing and utilising alternate technologies, such as Cellular networks, WiFi connections, and Fax messages, a C-SAW Team can continually service its community, and provide many levels of redundancy in their ability to communicate effectively.

The ability for a C-SAW Team to operate autonomously, will greatly improve their ability to service their community even in the event of regular communication channels becoming inoperative. In the following section we will discuss the geographic independence of individual C-SAW Teams as a mechanism to maximise their effectiveness in a national CIIP structure.

4.2.3 Geographically Independent

The notion of geographic independence is a simple one, but should be discussed to fully describe the construction of a C-SAW Team. The operation of a C-SAW Team must be constrained to a particular geographic region; this partition will depend on the country that will be implementing the CIIP structure.

Constraining a C-SAW Team to operate in a particular geographic region will serve a number of purposes. Firstly, it will allow a C-SAW Team of focus on its assigned community. Secondly, it will allow the community to identify with the C-SAW Team and lastly it will prevent overlap of services with other C-SAW Teams.

The geographic independence of C-SAW Teams will allow individual teams to effectively service their community and to focus on providing an effective response to computer security incidences. Each of the three discussed construction goals for a C-SAW Team will allow for an effective and robust CIIP structure. This structure will be highly community focused and able to effectively address the needs of the assigned community. In the following section we will discuss communication between C-SAW Teams in order to build up a net of protection.

4.3 Communication

Communication within a C-SAW structure is vitally important. The communication between a C-SAW Team and its community will facilitate the transfer of knowledge and provision of services. Equally important is that of inter- C-SAW communication; this will allow teams to communicate problems, experiences, and successes to all C-SAW Teams involved in a CIIP structure.

Due to the nature of the Internet and other information infrastructures, there has to be communication between all stakeholders in a CIIP structure. Any CIIP effort without effective communication mechanisms in place will not be able to adequately provide a sufficient level of service. This would be to the detriment of the whole CIIP effort.

When a computer security threat or incident is encountered, information must be able to spread quickly and efficiently to all parties, both within the CIIP structure, and those with mutual interests in the information infrastructure. The effective flow of information will allow for a quick and decisive response to protect information infrastructures.

Communication between C-SAW Teams and communities also is important to construct a net of protection, which will be elaborated on the in the following section.

4.4 Net of Protection

Important to the creation of a C-SAW structure, is the notion of a net of protection. This refers to a protection structure being constructed of a number of small or medium size teams, with each team providing protection for a fixed sized community. The accumulative effect of a number of teams operating in unison, will allow a number of C-SAW Teams to act together to provide a complete CIIP structure.

Computer security and cyber-events should be caught and handled by the collaborative effort of a number of C-SAW Teams. As discussed above, through the use of effective communication mechanisms, information can spread quickly through the CIIP structure. This will result in effective handling of any cyber-event.

An important aspect to the construction of a C-SAW structure is the development of the C-SAW Teams. Each C-SAW Team will progress through a number of stages in its development. In the following section we will discuss each of the stages of development for a C-SAW Team as an effective CIIP structure.

4.5 Stages of Development

The development of a C-SAW Team will be divided into a number of different stages; each stage will see a marked difference in the size of the community, the number of incidents handled, and number of services offered by the C-SAW Team. The three stages of development are: the initial stage, the intermediate stage, and finally the mature stage. The nature of the relationship between the size of the community, number of incidents, and the number of services can be seen in Fig. 2. In the following section we will discuss each of these stages, focusing on the community, number of incidents handled, and number of services offered.

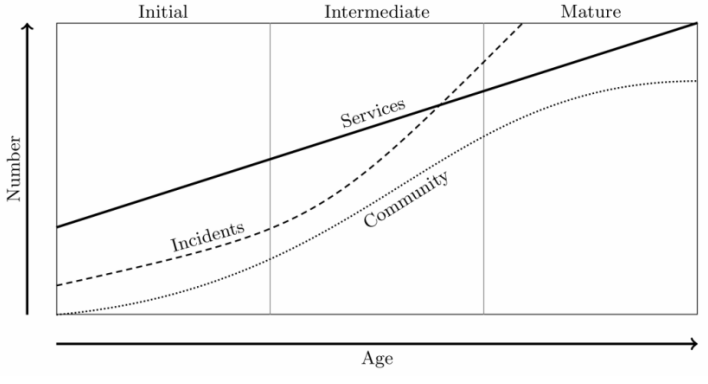


Fig. 2. This figure shows the stages of development for a C-SAW Team. The three stages of development are; the initial stage when the C-SAW Team is newly created; the intermediate stage, where the C-SAW Team has active community involvement; and the mature stage where the C-SAW Team is operating at capacity, the C-SAW Team may need to be migrated or merged to continue providing an effective service.

4.5.1 Initial Stage

The initial stages of the life of a C-SAW Team will be marked by a number of important milestones. During the initial stages, the C-SAW Team will be establishing itself, creating and deploying services to the community, and growing the size of the community.

Initially the C-SAW Team will be limited to only handling a small number of incidents; however, this will depend largely on the size of the community, and the scope of the services that will be provided. Along with growing the community base, the C-SAW Team will establish important communication links with other CIIP structures.

The number of services offered by the C-SAW Team should steadily increase during the initial stages, as the demand and requirements of the community are understood. In the following section we will discuss the intermediate stage in the life of a C-SAW Team.

4.5.2 Intermediate Stage

The intermediate stage in the life of a C-SAW Team will see rapid growth in the size of the community, the number of incidents handled, and the number of services offered. As the C-SAW Team matures, the requirements of the community will be identified, and the number and scope of services will reflect that.

The number of incidents handled will also see a marked increase. This will be due to the increasing size of the community, the increasing capacity of the infrastructure, and the increasing sophistication of computer security incidents over time. The size of the community will see the greatest growth during this period. Awareness and education of community members will contribute to this growth. The number of services offered during this stage should also be steadily increasing to maintain service levels to the community.

The intermediate stage will be marked by the greatest levels of growth in all operating areas of the C-SAW Team. Following the intermediate stage, the mature stage will introduce the greatest number of challenges for the C-SAW Team. In the following section we will discuss the mature stage of development for the C-SAW Team.

4.5.3 Mature Stage

The mature stage will introduce the greatest number of challenges to the C-SAW Team, both in terms of the ability to function, and the ability to service the community. This will be due to reaching the operating capacity of the C-SAW Team. The growth in the number of community members will stabilise during this stage, as this will be a side effect of the C-SAW Team reaching operational capacity.

Although the number of community members will stabilise, the number of service will need to continue to increase, to allow the C-SAW Team to provide an effective level of service. Along with reaching operating capacity, the number of handled incidents will continue to increase dramatically.

The danger is that during this stage, the C-SAW Team will be unable to cope with the increasing demands on its available resources. Contingency plans will have to be put into place to ensure that the C-SAW Team will continue to operate.

Steps will have to be taken by the C-SAW Team in order to continue to provide security advice and services to the community. Either the C-SAW Team must be

migrated to an alternate CIIP structure, or a C-SAW Team could be merged with other C-SAW Teams to provide a greater combined level of operational capacity.

Each of the stages of development of a C-SAW Team will bring with it its own set of challenges, specifically in terms of community, service provision, and incident handling and response. The C-SAW Team will have to continually adapt to these challenges, to allow it to provide adequate and continuing levels of service. In the following section we will discuss the question of interaction between CSIRTs and C-SAW Teams.

5 CSIRT and C-SAW Interaction

Closely related to the notion of the net of protection discussed above, is the question of the possible interaction between a CSIRT and a C-SAW structure. Although the C-SAW model is intended for deployment in an environment where an existing CIIP structure does not exist, the C-SAW model is flexible enough to be added to an environment where there is an existing CSIRT.

This would present a number of benefits to the overall CIIP structure, chief among these is the strong sense of community engagement which is key to the C-SAW Team, which is sometimes absent in a traditional CSIRT structure. A further application would be for an existing CSIRT to be used as a primary contact point for a national CIIP initiative, and a C-SAW Team to be used as a conduit for providing accessible computer security information.

However, a new CIIP structure which relies on both CSIRT and C-SAW components could limit the initial effectiveness of the C-SAW Teams, and the CIIP structure as a whole. In the following section we will discuss areas of future research, and we will then present a conclusion to this paper.

6 Future Work

This area of CIIP offers a vast number of research opportunities; as such we plan to conduct research into the impact of a C-SAW structure as an effective CIIP solution. We further plan to expand our area of focus into the role of CIIP in the developing and newly industrialised world. This will allow us to formulate CIIP models that are appropriate for these regions. In the following section we will present a conclusion to this paper.

7 Conclusion

As discussed above, Critical Information Infrastructure Protection is of vital importance for all nations. There is an ever-pressing need to define a CIIP model that is cost-effective, easy to understand, and quick to establish. In this paper we presented the Community-oriented Security, Advisory and Warning (C-SAW) Team, which aims to satisfy the above mentioned requirements.

In order to effectively discuss the application of C-SAW Teams, their construction, and their stages of development must be fully understood. The transition from a small-scale, community-based, CIIP structure to a large-scale, broad-range, CIIP

structure is a perceived strength of the C-SAW structure. This can hopefully be achieved through a careful understanding of the operational environment.

We started the discussion by introducing the need for Critical Information Infrastructure Protection in the modern world. We then presented a high-level conceptual model of existing CIIP structures. We then discussed a number of drawbacks of the current models. We then introduced the concept of C-SAW Team. We focused our discussion on the possible construction, communication, and the stages of development of such a model. We then discussed our future work in this area, and finally we presented our conclusions.

References

1. Ahamad, M.: Emerging Cyber Threats Report for 2009. Tech. rep., Georgia Tech Information Security Center (2008), http://www.gtiscsecuritysummit.com/pdf/CyberThreatsReport2009.pdf
2. Brownlee, N., Guttman, E.: RFC2350: Expectations for Computer Security Incident Response. RFC (June 1998), http://www.ietf.org/rfc/rfc2350.txt
3. Drummond, D.: A new approach to China. Electronic (January 2010), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html
4. ENISA: Baseline capabilities for national / governmental CERTs. Tech. Rep. (December 2009), http://www.enisa.europa.eu/act/cert/support/baseline-capabilities
5. Harrison, J., Towsend, K.: An Update on WARPs. ENISA Quarterly Review 4(4), 13–14 (2008), http://www.warp.gov.uk/Marketing/enisa_quarterly_12_08.pdf
6. ICANN: Factsheet: Root server attack on 6 February 2007. Electronic (March 2007), http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf
7. Korns, S., Kastenberg, J.: Georgia's Cyber Left Hook. Parameters 38, 60–76 (2008), http://www.carlisle.army.mil/usawc/Parameters/08winter/korns.pdf
8. Kossakowski, K., Stikvoort, D.: A Trusted CSIRT Introducer in Europe. M&I/Stelvio, Amersfoort, The Netherlands, 2nd edn. (February 2000), http://www.kossakowski.de/ti-v2.pdf
9. Richards, J.: Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security. International Affairs Review 18(2) (2009), http://www.iar-gwu.org/node/65
10. Vixie, P., Sneeringer, G., Schleifer, M.: Events of October 21, 2002. Electronic (November 2002), http://d.root-servers.org/october21.txt
11. West-Brown, M., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R., Zajicek, M.: Handbook for Computer Security Response Teams (CSIRTs), 2nd edn. Carnegie Mellon Software Engineering Institute, Pittsburgh (April 2003), http://www.cert.org/archive/pdf/csirt-handbook.pdf

On Planning of FTTH Access Networks with and without Redundancy

M. Tahir Riaz, Gustav H. Haraldsson, Jose G. Lopaz, Jens M. Pedersen, and Ole B. Madsen

Aalborg University, Networking and Security Section, Fredrik Bajers vej 5, 9220 Aalborg, Denmark
tahir@es.aau.dk, gustav.haraldsson@gmail.com, jgl@es.aau.dk, jens@es.aau.dk, obm@es.aau.dk

Abstract. This paper presents a planning analysis of FTTH access network with and without redundancy. Traditionally, access networks are planned only without redundancy, which is mainly due to lowering the cost of deployment. As fiber optics provide a huge amount of capacity, more and more services are being offered on a single fiber connection. Therefore, as a single point of failure in fiber connection can cause multiple service deprivation, redundancy is very crucial. In this work, an automated planning model was used to test different scenarios of implementation. Cost estimation is presented in terms of digging and amount of fiber used. Three topologies, including the traditional one "tree topology", were tested with a combination of various passive optical technologies.

Keywords: FTTH, Network Planning, Future Networks, Reliability, Broadband, ICT infrastructure, Modeling, Passive Optical Networks.

1 Introduction

Data communication over the Internet has been exponentially growing since the 90's. The Plain Old Telephone System (POTS) network has been great in meeting the demands of increasing bandwidth (with Integrated Service Digital Network (ISDN), asymmetrical digital subscriber line (ADSL), Symmetric digital subscriber line (SDSL), etc.) demands over its copper network. However the POTS network is already being pushed to its limit in trying to offer more bandwidth with new technology over the coppers. The downside is that the user has to be closer and closer to the connecting equipment.

Today more and more services are being introduced through the copper based network, not only the Internet, therefore making it an all-purpose network. These services (VoIP, VoD, other Internet applications) are demanding a lot of bandwidth, therefore it is apparent that though the current network media holds, it is becoming exhausted and a new type of media in which to use this all purpose network, is required. Optical fiber is one possible successor in planning a new installation, upgrading or expansion of, and to, an all purpose network. Optical fiber offers new

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 326–337, 2010.

possibilities compared to the older medium of copper based communication systems. One of these possibilities is Fiber To The Home (FTTH), where the complete network infrastructure is fiber, from the supplier all the way to the Network Termination (NT) - end user. By doing so the NT has a greater amount of capacity available.

All NTs are thus now more than ever becoming reliant on the reliability of an all-purpose network, since all these services are now being transferred to this all it. However, today's network planning has mainly focused on the upper levels of the network when creating redundancies, rather than planning the access networks with non redundant topologies. But as NTs in the access network are relying on the network, some research is needed to offer redundancy to the access network without introducing too much extra cost.

This paper contributes with an analysis of implementing FTTH with redundancy at the infrastructure level, which includes digging and amount of fiber optic used. The paper also introduces a new topology, namely eartree topology, which is seen as a compromise for lowering the cost of infrastructure, hence still providing good redundancy [1].

The structure for the rest of the paper is as follows: Section 2 provides terms and definitions used in the paper. Section 3 presents the planning method. Section 4 presents different topologies for the FTTH access network. Section 5 presents a case study where the area of Hals (rural area in Denmark) was chosen as a test subject. Section 6 lists phases and implementation scenarios with achieved results. And finally Section 7 provides a conclusion to the work.

2 Terms and Definitions

Some terms and definitions are used throughout the paper in order to explain different aspects of the network. The Swedish ICT commission [2] has standardized some terms used in planning a fiber network. In order to clarify these terms they are explained here as they are used throughout the paper.

2.1 Network Architecture

Figure 1 shows how the network architecture is a set up of 3 network layers and is as follows:

Main network: The main network, sometimes called the backbone network, is the highest level in the municipality's network hierarchy. This layer connects the municipality to the external network with links going out of the municipality and also down to the distribution network.

Distribution network: The distribution network consists of distribution nodes and lines, which connect the access network. In this paper the distribution network is the municipal network.

Access network: The access network is a network of Network Termination points (NTs) connected to the distribution node. NTs nodes are households, apartment buildings, business and government places. This paper will not distinguish between them.

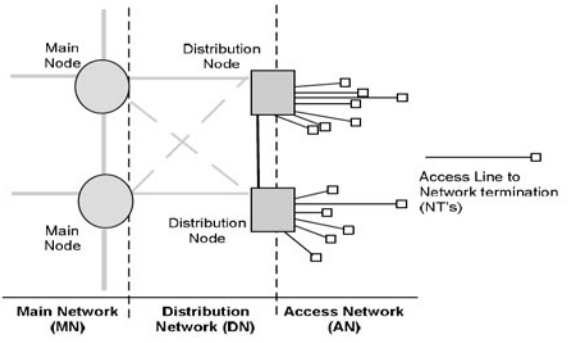


Fig. 1. Network architecture hierarchy

3 Planning Method

3.1 GIS System

A map can be used to represent real things that are in the real world; for example, roads, rivers or buildings.. This map information can be stored in a digital form in a system like GIS. As GIS data can store roads, rivers, bridges and other structures in a digital format, it is ideal for network planners to use it. Network planning with GIS data makes it easier to locate possible places through population density for Central Offices (COs) etc., as well as placements of pipes and lines for the communication infrastructure.

3.2 Automated Network Planning

Manual planning has a lot of drawbacks, i.e. it takes more time, costs more, and mistakes are easily made. If an access network is planned automatically it can reduce the degree of problems and drawbacks that can be observed in a manual process of planning an access network. To automate the planning process, GIS data and a set of algorithms were used to make the planning process more automatic. Network objects are modeled as nodes and links. The network model contains logical information such as connectivity relationships among nodes and links, directions of links or segments, and costs of nodes and links. With logical network information, it is possible to analyze a network.

The automated planning method consists of several steps, which are carried out in an iterated manner. In the first steps, the finding of potential traces for placing fibers and normalizing GIS data for traces are performed. When the GIS data is normalized, the parameters are set and different algorithms are applied to generate the plans. The flow diagram of the planning method is depicted in Figure 4. The key elements of the automated planning model are the trace normalization and planning algorithms. In the trace normalization, the digital road network is simplified by reducing the number segments. When the trace network is normalized and the parameters set, the trace network is processed further by a set of graph algorithms. In this study: spanning tree, shortest path, and various modified path algorithms were used. The algorithms

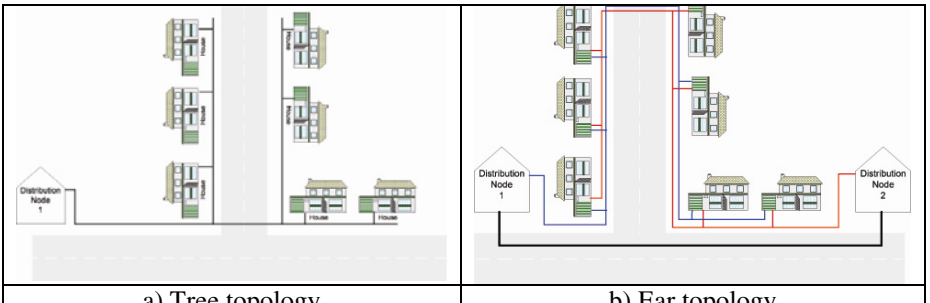
perform calculations for the laying of fiber cables and ducts based on the specified parameters. The planning algorithm selects the traces for fiber, which gives optimal paths (i.e. shortest or cheapest).

4 FTTH Access Network Topologies

The basic idea behind network topologies is to explain a network and is determined by the configuration between the nodes in a network. While some network topologies show simple means in connecting a network, other network topologies are more focused on offering redundancy and availability in a network.

4.1 Topologies

Today access networks are planned in a cheap manner and without redundancy. This means that in most case with a tree topology, as seen in Figure 2a, it branches out to each NT in the shortest and cheapest way possible. It is clear that this type of network topology offers no redundancy, so in the case of a line break near the root of the tree, it would cause several NTs to be affected. A topology designed for the access network might be able to offer redundancy by cutting projected cost. Figure 2b shows the ear topology and its design cut extra costs by reducing the extra digging needed [3]. Here two fibers are planned for each NT from two different distribution nodes, creating a closed loop to each NT, and therefore, redundancy.



a) Tree topology | b) Ear topology

Fig. 2. Access network topologies

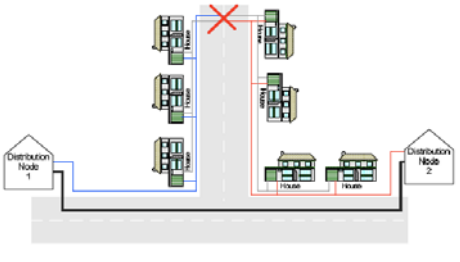


Fig. 3. Ear topology with single point of failure

The digging is then done by placing the fibers in the same trench but coming from opposite directions reducing the cost of digging with the reuse of trenches. There is a golden rule to be used with the ear topology which is: Trenches can never be shared in the same direction to - or within - the same districts. In the case of a failure the NTs can switch to the active line, keeping the connection available, as can be seen in Figure 3. A previous study has shown that by reusing trenches extra digging costs were cut and the amount of extra fiber was tripled using ear topology [4]. That study however, only used the manual planning approach.

4.2 New Topology, Splicing Points and Districts

A new topology is also introduced, which is the combination of two previously mentioned topologies - the tree topology and the ear topology. The new topology referred

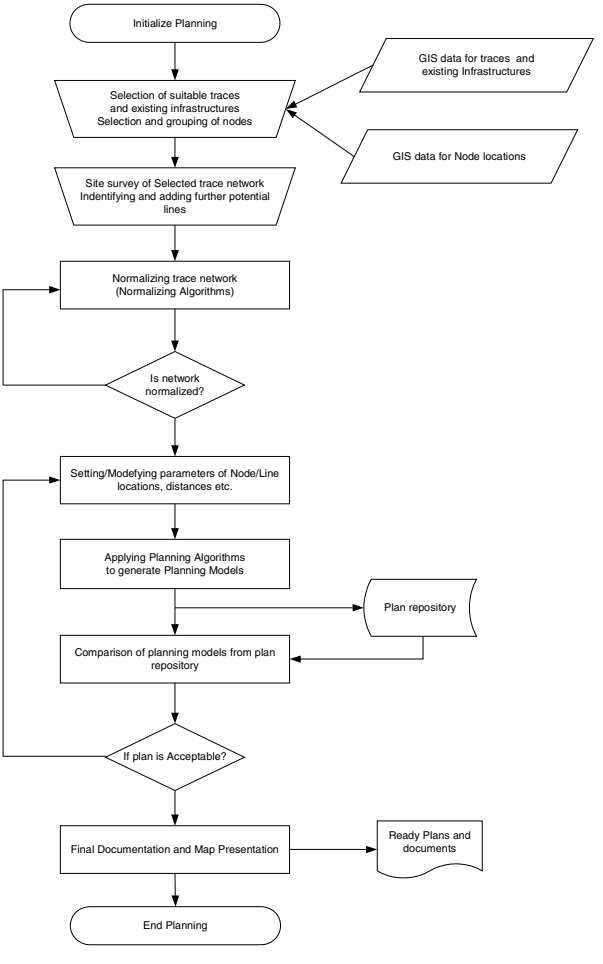


Fig. 4. The flow diagram of automated planning method

hereafter as the "eartree topology" utilizes both ideas, that of the ear topology from the DN to splicing points (SPs) and the tree topology from the SP to NTs. The eartree topology can be seen in Figure 7a and Figure 7b.

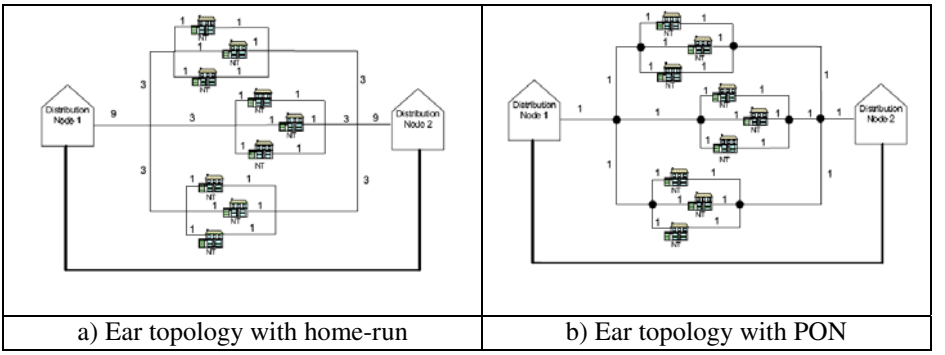
That means that each SP would have two separate fibers from two separate DNs causing the SP to be redundant. From the SP to the NTs the tree topology is used. So the main amount of extra fiber shown in the previous study [4] of the ear topology is addressed. It is obviously not as redundant as the ear topology, but that loss of redundancy is minimized because the most important part of the way is redundant.

Districts are created in correlation with the SPs and by doing so we can simplify the automated network design process by linking the NTs within a distance to a SP. It is also possible to view the affect that different sizes of district have on the cost of the eartree topology. As single fiber cables cost relativity more per NT then a multi strand cable does, it is also interesting to see what affect decreasing the size of each district, and having the SPs closer to the NTs, has. By finding the right balance we might be able to decrease fiber cost while make the design more redundant at the same time.

4.3 Home-Run and Passive Optical Network (PON)

The home-run (HR) architecture is a network that can be realized with a pair of fibers that runs from the CO to each NT, due to this reason the home-run architecture is also called point-to-point architecture [5]. This architecture uses a larger amount of fibers, that all demand separate termination at each end. Figure 5a shows the home-run architecture. The main drawback of this type of architecture is the fiber cost [6].

A PON is a point to multi-point network over a passive fiber plant comprising fibers, splitters and an active equipment at the end [5]. The PON architecture is used to reduce the amount of fibers terminated in the COs. Figure 5b shows the PON architecture. That is a single fiber leaving the CO may support several NTs, depending on the splitting ratio. This architecture gives an important reduction in costs but also an increase of complexity. In this case, there is one fiber to be shared between all users and the amount of fiber is reduced.



a) Ear topology with home-run | b) Ear topology with PON

Fig. 5. Configuration for Ear topology

5 Case Study

For the case study, the area of Hals is presented here. The Hals area is a small rural community in Denmark, with approximately 3500 private households and 11500 inhabitants spread over 191 square km.

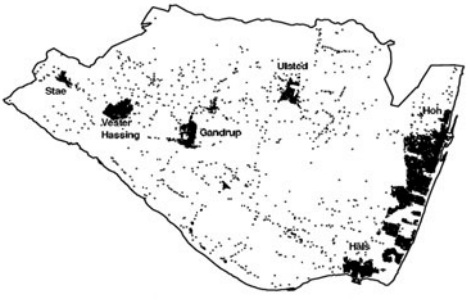


Fig. 6. Distribution of NTs in the Hals area

There are as much as 3400 summerhouses. The private households, public institutions and businesses are mainly situated in villages, while the agriculture is more spread out. Figure 6 shows the distribution of NTs in Hals area. The existing infrastructure is representative to the infrastructure in similar rural areas around the country. There are 7 central offices owned by the former national telecom, TDC. The existing central offices were chosen for the access network nodes. Only 5 ANs are decided that were located in rather big towns.

6 Phases and Implementation Scenarios

The study conducted the testing in two phases. The first phase focused on the dense local area and tested and compared several scenarios.. While the second phase focused on taking the results from phase one and applying the best solutions on a larger area, including rural areas.

6.1 Phase One

Basically there are three types of scenarios that are considered in this work, these are tree topology, ear topology and eartree topology. Further, each scenario was tested with HR and PON, and also with DN, in the same or different locations. This was done in a small focused area in Hals.

6.1.1 Phase One Scenarios

The scenarios were home run using the previous mentioned automated network planning and the GIS data. These scenarios are explained in table 1.

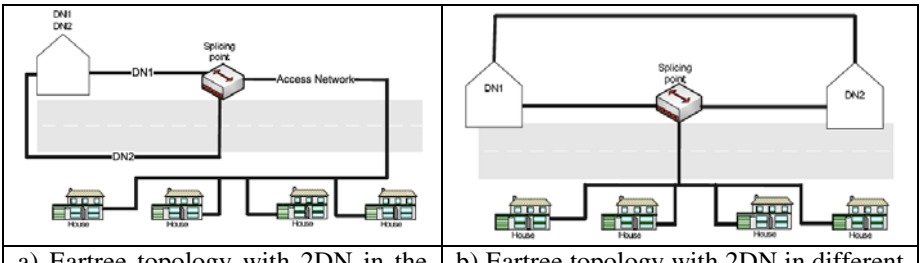
Figure 7a illustrates how the eartree topology was implemented with DNs in the same location, and adhering to the rules. Furthermore figure 7b illustrates how the eartree topology is done with DN´s on separate locations.

Table 1. Scenarios and topologies

Scenario 1	Scenario 1.HR.1	Tree topology with home-run and 2DN in the same location
	Scenario 1.HR.2	Tree topology with home-run and 2DN in different location
	Scenario 1.PON.1	Tree topology with PON and 2DN in the same location
	Scenario 1.PON.2	Tree topology with PON and 2DN in different location
Scenario 2	Scenario 2.HR.1	Ear topology with home-run and 2DN in the same location
	Scenario 2.HR.2	Ear topology with home-run and 2DN in different location
	Scenario 2.PON.1	Ear topology with PON and 2DN in the same location
	Scenario 2.PON.2	Ear topology with PON and 2DN in different location
Scenario 3	Scenario 3.HR.1	Eartree topology with home-run and 2DN in the same location
	Scenario 3.HR.2	Eartree topology with home-run and 2DN in different location
	Scenario 3.PON.1	Eartree topology with PON and 2DN in the same location
	Scenario 3.PON.2	Eartree topology with PON and 2DN in different location

6.1.2 Phase One Results

The results obtained from the phase one - seen from Figure 8 - show that in comparison to the ear topology the amount of fiber is almost triple, making the cost difference about two and a half times more than in the tree topology. While a tree topology can place a splicing point (DN, or any kind of distribution point) in an optimal position to acquire the least amount of fiber. In order to offer the redundancy and offer savings on extra digging means the placement of the splicing points are faulty in this problem. Because it is necessary to situate them on each side of the district, the distance will grow more rapidly as we need to access NTs from each side and all over the area. This is actually noticed in the creation of the topology but as it was a theory, it is based on the fact that fiber prices are going down thus not making it a deciding factor. There are more important factors involved such as the blowing of the fiber.



a) Eartree topology with 2DN in the same location.

b) Eartree topology with 2DN in different locations.

Fig. 7. Configuration of eartree topology

All of this actually collaborated with the results acquired, making the ear topology expensive to deploy. The ear topology is still an interesting topology, if a method is found to decrease the fiber. Another solution is to look at it when the fiber prices have gone even further down, but then again, the tree topology cost would also decrease.

A new topology was introduced which could offer redundancy to the access network but not use an excessive amount of fiber like the ear topology. The result was the eartree topology, where each splicing point would be redundant. But from the splicing point the tree topology would be used. For this topology the absolute worst case scenario is that it would loose one district when either a splicing point would be made unavailable or a cut near the splicing point occured. The further the cut is from the splicing point, in most cases, the less the number of NTs that become affected. Now the only extra fiber needed is for doubling the main duct lines unaffecting the NT to splicing points fiber required. Now, this is done to limit the extra amount of fiber by not doubling the NT to SP. Comparing the cost it can be seen that the cost only increases around 25% between the eartree topology and tree topology throughout the scenarios - see Figure 8 - thus making eartree topology a feasible topology to investigate further in phase 2.

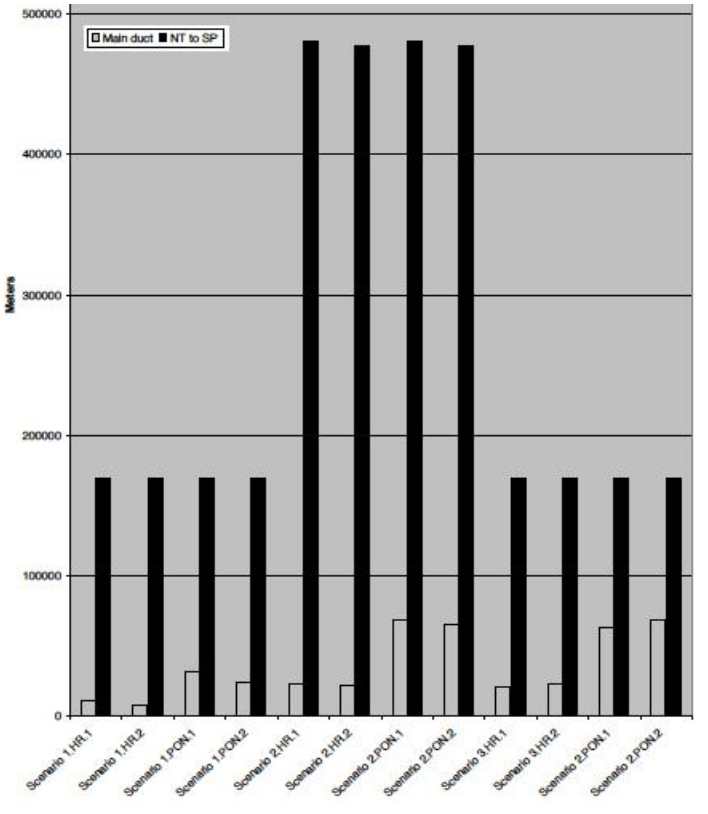


Fig. 8. Implementation results with amount of fibers

6.2 Phase Two

Phase two focuses on using the best findings from phase one and putting them in a more real life scenario. Set of criteria's was done for phase two.

6.2.1 Phase Two Criteria

The criteria for phase two were created from phase one and are as follow:

1. Large scale testing
2. Investigate with automatic district creation effect on different sizes of districts
3. Two network scenarios
   - Tree topology and ear topology
   - Home-run only
   - Distribution nodes in one location

Instead of using only one town in the municipality of Hals, the paper would now focus on the whole municipality, dense and rural areas. Several methods where tested for creating automatic districts, but the one chosen was a spanning tree algorithm starting from each DN. Placing of the splicing points was then done from the point with the shortest distance to all NTs.

6.2.2 Phase Two Results

In almost all cases smaller number of NTs per district shows decreased cost, this means that creating districts with only 30-40 NTs is the most feasible. This means that there is higher redundancy, where a single digging accident close to a splicing point will cause in the maximum 30-40 NTs to lose connection. Figure 9 illustrates the results from testing of size of districts in the ear topology.

Taking this result and applying the final cost for each topology shows only a 17% increase in cost between the use of tree topology and eartree topology. The results are very good and reinstate the fact that the eartree topology could be used as a viable

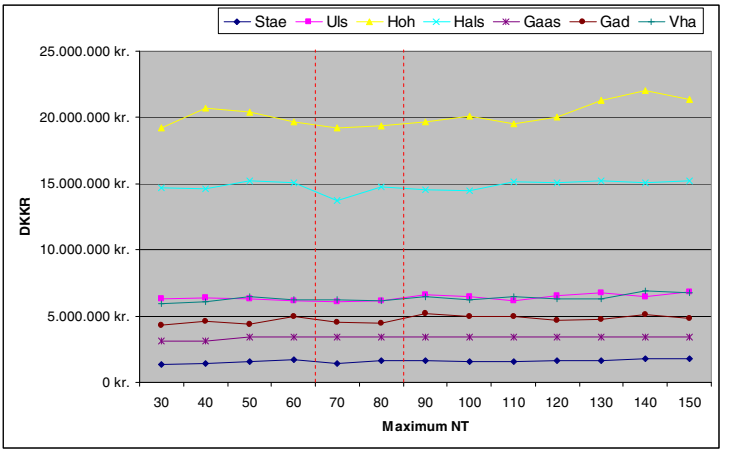


Fig. 9. District calculation result per town in the municipality

solution for future network planning. Now with that much added redundancy to the access network and not that much increase in cost, the eartree topology is definitely a feasible/cheap solution to offer redundancy as close to NTs as possible.

7 Conclusions

The paper presents an implementation study of fiber access networks with and without redundancy by using an automated planning method. The motivation for doing is that networks are moving towards becoming a multi purpose. This means that more services for the home are now being offered through this network. In order to ensure reliability of these services some physical redundancy is needed. To date no practical investigations have been done into offering redundancy in the access network, meaning that it should be considered a necessity to review this.

The results showed that PON had little or no affect on the cost as the district method already mimicked the PON affect. Furthermore it showed little or no difference in the fiber usage when using two DN locations or one. In Phase one, three scenarios where created with the three topologies in question. The PON and DN location was included in those scenarios as sub scenarios, but as explained, had little effect. This project was unsuccessful in reducing the fiber enough for the ear topology to become a cost efficient solution. The eartree topology showed some good results, and in comparison to the tree topology, the cost difference of the fiber showed to be only around 25%. Thus it was used in phase two.

In phase two the eartree topology was again compared to the tree topology, but now on a larger scale and focused with the criteria that showed best results. By looking at the district, and possibly making districts smaller and thus minimizing the need for single fiber, the cost could be reduced and the redundancy increased. This proved to be true as most areas showed that the sweet spot was 30-40 NTs per district. By using this, we were also able to reduce the difference in overall cost and the difference between the eartree topology and tree topology now only showed a 17% increase in cost, making this a highly feasible solution.

In conclusion, the results shown are quite good and are found to be a viable and interesting solution in offering redundancy or at least minimizing the affect of digging accidents to a few NTs. From this conclusion it is of interest to conduct further research on eartree topology in comparison to the tree topology in order to truly view whether redundant topology can be planned without costing more than a normal tree topology in a large scale environment.

References

1. Haraldsson, G.H., Beshir, O.: Automatic Network Planning for Access Networks in FTTH with and without Redundancy. Master thesis, Aalborg University (2007)
2. The Swedish ICT Commission. General guide to a future-proof IT infrastructure (April 2005)

3. Pedersen, J.M., Riaz, T.M., Knudsen, T.P., Madsen, O.B.: Designing Broadband Access Network with triple redundancies. Department of Control Systems. Aalborg University (2005)
4. Haraldsson, G.H., Pedersen, J.M.: Cost vs. Redundancy in FTTH access networks: A case study of a Danish village. In: CSNDSP 2006, Patras, Greece (July 2006)
5. Lin, C. (ed.): Broadband Optical Access Networks and Fiber to the Home: Systems Technologies Development and Strategy. Wiley, Chichester (2006)
6. Pedersen, J.M.: Structural Quality of Service in Large-Scale Networks, PhD thesis, Department of Control Systems. Aalborg University (April 2005)

A Distributed Denial of Service Testbed

Desmond Schmidt, Suriadi Suriadi, Alan Tickle, Andrew Clark,
George Mohay, Ejaz Ahmed, and James Mackie

Information Security Institute, Queensland University of Technology,
126 Margaret Street, Brisbane, 4001, Australia
d.schmidt@qut.edu.au, s.suriadi@qut.edu.au,
ab.tickle@qut.edu.au, a.clark@qut.edu.au, g.mohay@qut.edu.au,
e.ahmed@qut.edu.au, j.mackie@qut.edu.au

Abstract. The Denial of Service Testing Framework (dosTF) being developed as part of the joint India-Australia research project for 'Protecting Critical Infrastructure from Denial of Service Attacks' allows for the construction, monitoring and management of emulated Distributed Denial of Service attacks using modest hardware resources. The purpose of the testbed is to study the effectiveness of different DDoS mitigation strategies and to allow for the testing of defense appliances. Experiments are saved and edited in XML as abstract descriptions of an attack/defense strategy that is only mapped to real resources at run-time. It also provides a web-application portal interface that can start, stop and monitor an attack remotely. Rather than monitoring a service under attack indirectly, by observing traffic and general system parameters, monitoring of the target application is performed directly in real time via a customised SNMP agent.

Keywords: Distributed Denial of Service, Testbed Development.

1 Introduction

This paper discusses the design of the Distributed Denial of Service testbed being developed as part of a joint India-Australia research project entitled 'Protecting Critical Infrastructure from Denial of Service Attacks: Tools, Technology and Policy'.

It is divided into four parts. Part 1 provides a brief background to the problem and the role it plays within the research project. Part 2 critically assesses existing testbeds for studying DDoS attacks. Part 3 describes the our current testbed, Part 4 describes some experiments already carried out using it, and in Part 5 we describe future directions for the testbed.

Distributed Denial of Service (DDoS) is a serious and growing problem for corporate and government services doing business on the Internet. Some botnets now number in millions of compromised machines [1, 2]. As well as for other nefarious purposes, these botnets can be used to launch Distributed Denial of Service attacks, such as those recently carried out against Twitter, Facebook [3], and government websites in the US and South Korea [4]. Modern DDoS attacks can muster 49GBps of

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 338–349, 2010.

attack traffic, but more recently this type of flooding attack is giving way to more sophisticated, stealthy attacks designed to cripple a particular service [5]. The India-Australia project aims to address various aspects of this problem, and is divided into five sub-projects:

1. Probabilistic Packet Processing to Mitigate High-rate Flooding Attacks
2. DoS Defence Appliance for Web Services
3. Puzzles for DoS Mitigation in Protocols for Authenticated Key Exchange
4. Denial of Service Vulnerabilities and Challenges in Emerging Technologies
5. Harmonisation of Policy, Legal and Regulatory Environments for National Information Infrastructure Protection

Of these, the first four subprojects all require the use of a testbed facility. A DDoS testbed is an essential tool for preparing and testing the defensive strategies, appliances and protocols against such attacks as we are intending to research.

2 Existing Testbeds

Judging by existing implementations, a DDoS testbed needs to provide facilities to:

1. Specify, save and replay an experiment
2. Deploy, run and stop an experiment
3. Monitor the simulated DDoS attack in progress and to save the results to disk for later replay or analysis.

`There have been three basic strategies used for building a DDoS testbed:

1. Simulation. In this technique a network simulator such as ns-2 [6, 7] or OPNET [8] is used to specify and then instantiate a simulation on a single computer. The accuracy of such simulations and their suitability for DDoS experimentation has, however, recently been called into question [9, 10]. The attraction of simulation is that virtually any network topology can be created quickly and inexpensively; the prime disadvantage is that simulated networks when under attack may behave very differently from real or emulated networks [9].

2. Emulation. In this technique real machines are connected together to form the topology of the test network. Although the end-points of the network are mostly physical computers, the connections between networks are normally provided by soft-routers. Although more realistic than simulation, emulation suffers from scalability: it is hard to extend a local Ethernet network of PCs to model the performance of entire ISP networks that use powerful hardware routers, ATM, and multi-gigabit links.

3. The use of real networks cannot be discounted, but would seem to pose too many problems: (a) it is not possible to change the network to suit the experiment, (b) certain experiments, e.g. those involving Internet worms, could escape from the test and infect or damage the wider Internet, and (c) collateral degradation of network links may result from flooding attacks. Certain types of DDoS attacks, such as low-level stealth attacks, however, could conceivably be tested on a real section of the Internet like PlanetLab, a world-wide network of virtual machines [11].

2.1 The DETER Testbed

The DETER testbed [12, 13] is closest to the kind of design we are seeking, for a small to moderate size facility that allows experiments to be safely contained, and uses reconfigurable hardware and software. However, there are a number of reasons why we chose to deviate from the DETER design:

1. DETER uses the Emulab software. This has a GPL license, which only permits modifications under the same license. Since the terms of the India-Australia project specify that any software produced shall be licensed to the respective governments, not the general public, this is less useful to us.
2. The Emulab and DETER testbeds [6, 12] use a relatively large number of physical machines. We needed to build something with more modest resources.
3. The Emulab software design would be too complex to mimic, since it probably would cost more than the hardware it would run on [12]. For example, the ability to share and partition the testbed is not needed.
4. Our experiments comparing soft routers with hardware routers have shown that soft routers, even properly tuned, perform poorly in comparison to hardware routers with small-packet traffic, apparently because the host computer cannot process interrupts from the ethernet card fast enough to avoid dropped packets [14]. Under a DDoS flood attack a soft-router might thus introduce a serious anomaly.

The DETER testbed uses VLANs and soft-routers (but also some hardware routers) to provide flexibility. Experiments recorded as ns-scripts (in Tcl) can be quickly recreated by programming the VLANs and routers to generate the desired network topology. The advantages of ease of use, sharability, and remote access however, must be balanced against the disadvantages of higher cost in constructing, administering and maintaining the testbed.

3 The dosTF Testbed

The dosTF testbed has evolved organically in response to our own research needs. It may thus provide a useful model and alternative approach for other research groups wanting to construct their own small scale testbed for DDoS experimentation.

An example of our current experimental setup is shown in Fig. 1. The same or additional components could be rearranged as desired for a particular experiment. A total of 8 average PCs, installed with a mixture of Linux and Windows, are each fitted with two ethernet cards. These two interfaces ensure that all physical machines are dual-homed. The monitor network is on a single subnet, and is used to install software, launch and stop attacks and to monitor services during attacks. The attack network, consisting of two subnets joined by a physical router, is used to carry out attacks on particular services, to generate background traffic, or to host defense applications or devices. The physical PCs are intended to act as targets, although they may also participate as agents. One of these also acts as a point of remote access, and

another as a base for launching attacks. Three VMWare servers provide around 200 virtual hosts that may be used in simulated DDoS attacks. The driver of this design has been cost: it seems wasteful to maintain hundreds of physical machines, when most of them will only send low levels of data to the attack target. We intend eventually to evolve this design by acquiring more physical routers to study aggregation of traffic at focal points in the network topology. For now, it suffices to study the direct effects of flood and stealth attacks on applications from a range of IP-addresses.

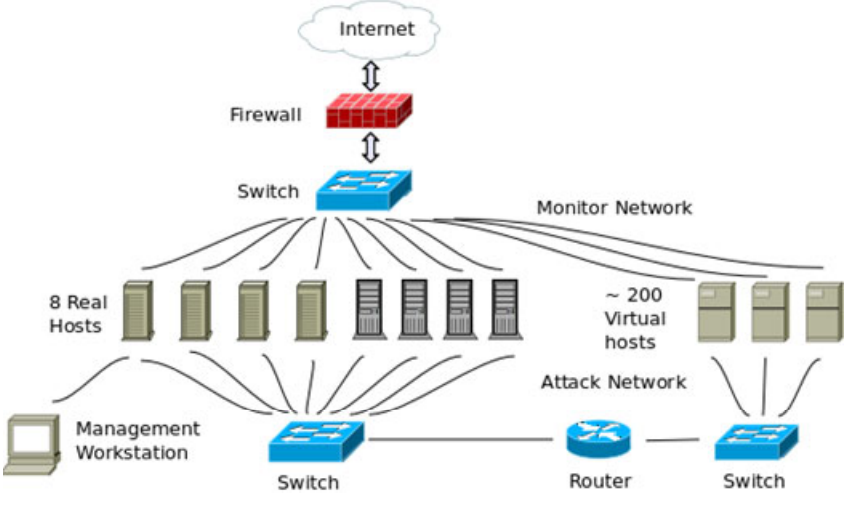


Fig. 1. Example dosTF Topology

The main difference between this design and the DETER model is shown in Fig. 2-3. Whereas in DETER a software layer is effectively introduced by the programmable VLANs and soft-routers, in our design the structure of the network topology has to be reconfigured manually. Our XML description of the experiment (or *scenario*) has no intervening software layer, and hence must refer directly to the physical testbed. This has the disadvantage that every change in the setup of the testbed will invalidate previously saved experiments.

Our solution to this deficiency is shown in Fig. 3: The scenario only stores an abstract description of the experiment: the number of attacking hosts, their operating systems, their preferred type (virtual or physical), the characteristics of the target and the software to be installed on them. When an experimenter launches an attack, the control application maps the abstract description of the experiment to physical machines using standard network discovery techniques. This approach yields the same degree of flexibility as in the DETER testbed, although the topology has to be wired manually.

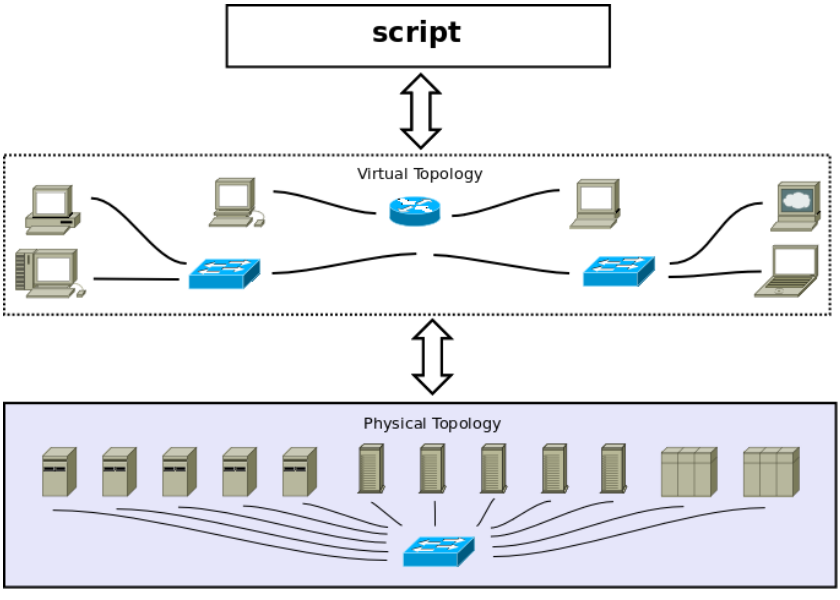


Fig. 2. DETER Testbed Model

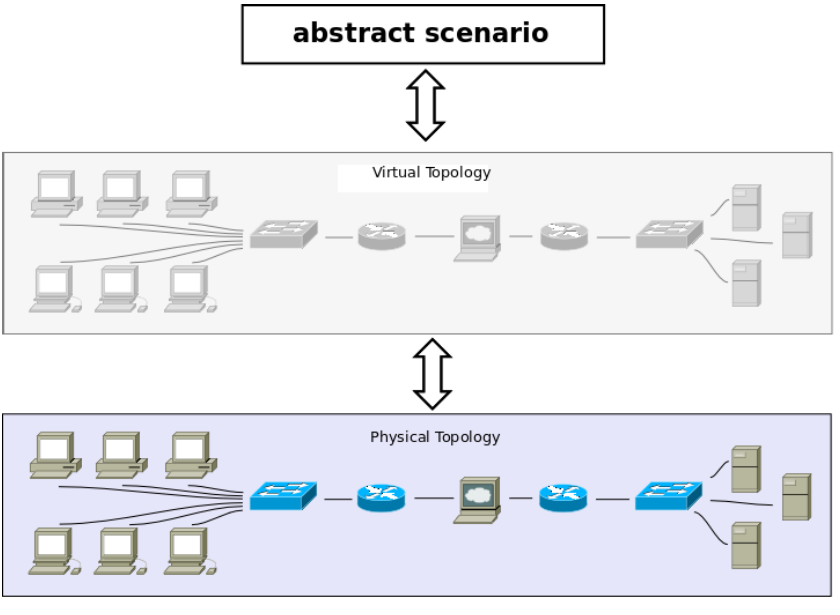


Fig. 3. dosTF Abstract Scenario

3.1 Monitoring

The monitoring of a machine under a DDoS attack involves an obvious and serious problem: how can an application respond promptly with information about its status, when it is already under attack? Even in severe attacks, however, the multi-tasking design of modern operating systems should allow enough responsiveness in the overall system to enable the gathering of basic statistics at regular intervals. The saturation of the attack network can then be easily dealt with by installing a second Ethernet card to use as the monitoring interface. This is also a feature of the DETER Testbed [12]. The advantage of using live feedback during an attack is that it becomes possible to see the performance of service applications as they buckle under the strain imposed by a DDoS attack, or recover as defensive measures are engaged.

The method we chose for live monitoring was to install an SNMP (Simple Network Management Protocol) service on each potential target. We could then query the target for a wealth of built-in MIB (Management Information Base) variables such as, for example, tcpOutRsts (requests to resend a TCP segment). Such information has sometimes been used to detect the presence of a DDoS attack [15]. However, these system-wide values are less useful when monitoring the effect of an attack against a single service. According to Mircovic *et al.* [16] Denial of Service can be effectively measured by monitoring only a select few application-specific parameters: chiefly memory and CPU usage, as well as responsiveness and goodput (the amount of data actually being received and sent out by the application).

Another drawback with the standard SNMP installation is that per-second monitoring of network-related MIB-values tends to tie up the CPU. In our case we observed 30% CPU utilisation with the default Linux SNMP agent running, when querying IF-MIB variables.

Our solution was to write a small custom MIB that would discreetly measure the following parameters on a per-second basis for any named service:

1. Percentage of system memory being used
2. Percentage of CPU being used
3. Number of active threads or forked children of a process
4. Response time in milliseconds to a generic query
5. Goodput - the actual data throughput of the service
6. Does the response to a given challenge match the expected value?

This is all we currently measure, but the custom MIB can be extended at any time. It is written as a separate agent that can be brought up or down without disruption to the main SNMP agent. Parameters 1, 2 and 3 can be measured by system commands that take only a few milliseconds to run.

Response time is measured in nanoseconds, up to a maximum of 15 secs, of a named service to a given challenge string, which usually consists of binary digits. The values for HTTP, TELNET, FTP, SSH and DNS query generic properties of their respective services, e.g. the HTTP challenge merely requests the server's options, and the DNS challenge requests the service's status. But it is also possible to override the default challenge, to define new services, to change ports and protocols *etc*.

Goodput can be computed without modification of the service, at least in the case of Linux, by using the Systemtap tool, or by modifying the kernel. This may be preferable to 'instrumenting' the service, *i.e.* by modifying it [16].

The advantage of using SNMP is that existing software libraries for querying and setting values, as well as command-line tools can be used. We also envisage that using these specific MIB values, rather than the general ones, may provide a more accurate way for an alarm system to *detect* Denial of Service.

3.2 The Scenario

An experimenter needs to specify what form an attack will take, and to save that information so it can be edited and replayed later. DETER uses Tcl largely for historical reasons [9], but this is a programming language with a fixed syntax, and is not ideally suited to the recording of an abstract experiment. XML [17], on the other hand, is a widely used markup language suitable for a variety of programming tasks. Many tools for reading and writing XML files already exist, and changing the scenario schema or structure in response to design changes is easy. Our schema contains the following basic elements:

Agents: may be one of attacker, traffic generator, defender or service. These are programs that can be launched from the command line. Each agent is specified by a set of runtime parameters, the system requirements, the number of hosts it should be copied to, and the type of hosts required (e.g. real or virtual, and desired operating system). The control application (described below) will then choose an appropriate binary to copy to the specified host.

Targets: There may be more than one, and each is specified simply by an operating system type and optionally by an IP-address. This latter facility is needed because otherwise the default choice of target may not be what is desired.

Views: These describe the layout of portlet windows in the testbed software, to be described below. This section is entirely optional, but otherwise there would no way to save the screen layout of the tools used for monitoring a particular experiment.

3.3 Command and Control

The experimental scenario described above needs to be activated by some means. Agents will first have to be copied to their assigned targets. This is achieved in dosTF via SFTP. This can be configured so that the payload will only be copied to the targeted host if the current file is more recent.

The attack command is then issued by the control workstation via ssh, using a standard username and password. Since the interface is simply the commandline, this allows us to leverage most existing tools. For example, the traffic generator D-ITG [18] can be easily configured within the scenario to generate various types of traffic.

In the third phase the experiment is monitored in real time by the control workstation via SNMP. The results are displayed on the workstation as a series of graphs and the values are logged to local files automatically.

Fig. 4. Pluto Portal Interface

3.4 Web Interface

DETER uses a desktop based GUI application to monitor and control experiments, and RPC for communications [13]. This introduces some complications, since user authentication has to be programmed in, and the application must be available on the computer connecting to the testbed. GUI development is inherently complex and expensive [19]. Changes to the functionality of the underlying program can cause expensive alterations to the GUI. This could easily lead to the GUI taking more time to develop than the underlying functionality.

Our solution to this problem was to use a modular web application interface for GUI development, such as a portal server. The GUI is accessed via an ordinary web browser either remotely or locally. The web interface is divided into a number of sub-windows, or portlets, which can be installed and arranged, or duplicated by the user to suit the experiment. Authentication is already built-in, as also (on some servers) user filespace management for saving experimental results. Fig. 4 shows the current state of the interface, and includes three portlets, one which edits the XML scenario file, another on the right that launches attacks, and a monitor portlet that graphs the chosen SNMP MIB variables and also logs them to disk.

4 Experimental Results

The dosTF testbed is designed to run experiments for any of the subprojects listed in Section 1. For example, Subproject 4 investigates DoS vulnerabilities in emerging technologies such as web services. This section describes two experiments from this area of the overall project as examples of simulated DoS attacks carried out on the

testbed. Each experiment starts as an XML scenario, which is then executed, causing the attack program to be copied to its respective hosts, then the attack was launched, and the results monitored using the custom SNMP MIB parameters.

4.1 Experiment 1

The first experiment exploits a vulnerability in the Ruby XML parser. The attack uses an invalid web service request payload containing a *deeply-nested* meaningless XML message (up to 100,000-levels deep), and then sends a flood of such requests to the Ruby server. The payload size is around 1.5 MB. A vulnerable XML parser will try to load each of the XML messages sent. The goal is to consume all of the memory available on the server, causing a potential denial of service to legitimate clients.

The single attack and victim machines are physical hosts on the same subnet as shown in Fig. 1. The victim server's resources include a dual-core 3 GHz CPU with 3.7 GB of memory. The SNMP monitoring provided by the dosTF testbed was used to track memory usage and CPU usage throughout the attack and after. The attack itself lasted for about 10 minutes. Requests were sent in bursts of 500, followed by a sleep of 0.1 of a second. The result of the experiment is shown in Fig. 5. Although the CPU usage quickly reached a maximum, the memory usage took longer to become exhausted, eventually causing the Web Service to fail, before restarting.

4.2 Experiment 2

The second experiment exploits a vulnerability in many web services that respond to unauthenticated requests for their service description files, or WSDL documents. This

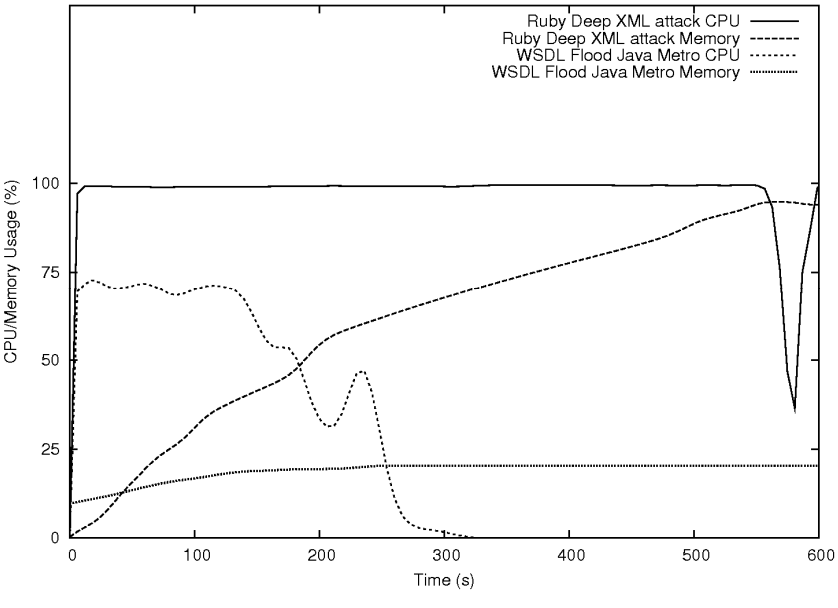


Fig. 5. CPU and Memory Usage for Experiments 1 and 2

experiment tested the effect of performing repeated requests for a WSDL document on a web service developed using the Java Metro library, and deployed on the Glassfish application server. By default, the WSDL document will be dynamically generated, requiring some processing by the server. Successive requests may thus have a significant impact on CPU and memory consumption, and on the response time for legitimate web service requests.

The three attack machines were real hosts, and the victim was a virtual host, as shown in Fig. 1, but without the intervening router. The victim machine's resources included a dual-core 4.8 GHz CPU and 3 GB of memory. Fig. 5 shows the application server response as tracked via the SNMP monitoring provided by the testbed. The attack lasted roughly 4 minutes, consisting of 250 bursts of 150 requests per machine. In contrast with the first experiment, memory consumption was virtually unchanged. After the attack CPU consumption soon fell back to normal levels.

5 Future Developments

As well as being a general DoS testing facility, the dosTF testbed can also provide a flexible framework for carrying out experiments involving specific devices. Subproject 1, for example, aims to develop a 'network flooding attack mitigation tool' capable of protecting security devices, such as an application-aware firewall. As shown in Fig. 6, the device will monitor the state of the firewall and, once a high-rate flooding attack is detected, will initiate corrective action to mitigate the impact of the attack.

Another application of the testbed will be the testing of vulnerabilities introduced by the use of the IPv6 protocol in an emulated SCADA network controlling a set of distributed resources, similar to those encountered in the monitoring and control of critical infrastructure, such as in the electricity and water utilities. The aim is to study the behaviour of such SCADA systems when known IPv6 vulnerabilities are exploited and to evaluate the effectiveness of potential mitigation techniques.

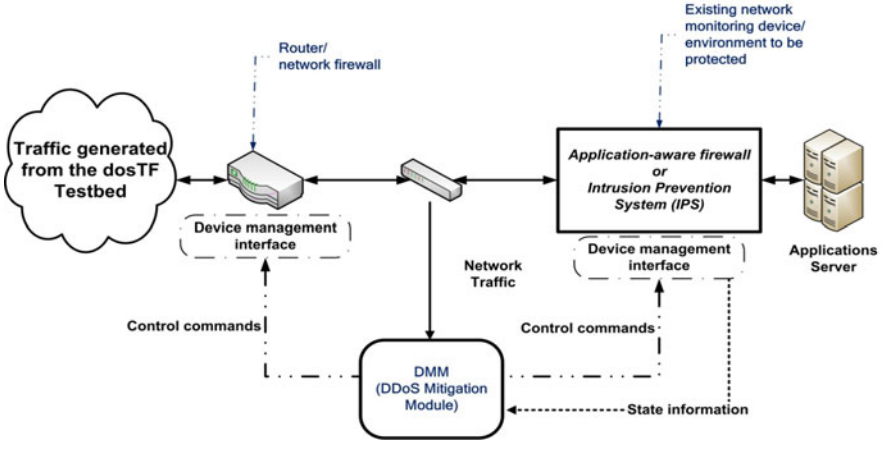


Fig. 6. DDoS Mitigation Module

6 Conclusion

The dosTF testbed is designed to provide an abstract means for specifying an experiment that can be run unchanged or with insignificant changes on various physical network topologies. By dispensing with the need to construct a virtual topology within the physical layout of a dedicated testbed it enables experiments involving new network appliances. This design, being simpler than the DETER model, allows for the construction and management of a private DoS/DDoS test facility at minimal cost, with some sacrifice in ease of use.

This research is supported by the Australia-India Strategic Research Fund.

References

1. Leyden, J.: Conficker botnet growth slows at 10m infections. The Register 26/1/09 (2009), http://www.theregister.co.uk/2009/01/26/conficker_botnet/
2. Chapman, S.: Massive 2 Million PCs Botnet Uncovered. Computerworld, UK, 23/4/09 (2009), http://www.cio.com/article/490454/Massive_2_Million_PCs_Botnet_Uncovered
3. Van Buskirk, E.: Facebook Confirms Denial-of-Service Attack. Wired, 6/8/09 (2009), http://www.wired.com/epicenter/2009/08/facebook-apparently-attacked-in-addition-to-twitter/
4. Nakashima, E., Krebs, B., Harden, B.: U.S., South Korea Targeted in Swarm Of Internet Attacks. The Washington Post, 9/7/09 (2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/07/08/AR2009070800066.html
5. Worldwide Infrastructure Security Report. Arbor Networks (2009), http://www.arbornetworks.com/report
6. White, B., Stoller, L., Ricci, R., Guruprasad, S., Newbold, M., Hibler, M., Barb, C., Joglekar, A.: An Integrated Experimental Environment for Distributed Systems and Networks. In: Proc. of the Fifth Symposium on Operating Systems Design and Implementation, Boston, MA, pp. 255–270 (2002)
7. Lam, H.-Y., Li, C.-P., Chanson, S.T., Yeung, D.-Y.: A Coordinated Detection and Response Scheme for Distributed Denial-of-Service Attacks. In: IEEE International Conference on Communications, ICC 2006, vol. 5, pp. 2165–2170 (2006)
8. Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., Jokerst, R.M.: Analyzing Interaction Between Distributed Denial of Service Attacks And Mitigation Technologies. In: Proceedings of DARPA Information Survivability Conference and Exposition, April 22-24, vol. 1, pp. 26–36 (2003)
9. Chertov, R., Fahmy, S., Shroff, N.B.: Emulation versus Simulation: A Case Study of TCP-Targeted Denial of Service Attacks. In: Proceedings of 2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities. TRIDENTCOM, pp. 315–325 (March 2006)
10. Mircovic, J., Fahmy, S., Reiher, P., Thomas, R.K.: How to Test DoS Defences. In: Proceedings of the Cybersecurity Applications & Technology Conference For Homeland Security, CATCH (2009)
11. Peterson, L., Bavier, A., Fiuczynski, M.E., Muir, S.: Experiences Building PlanetLab. In: OSDI 2006: 7th USENIX Symposium on Operating Systems Design and Implementation, pp. 351–366 (2006)

12. Benzel, T., Braden, R., Kim, D., Neuman, C., Joseph, A., Sklower, K.: Experience with Deter: A Testbed for Security Research. In: Proceedings of 2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities. TRIDENTCOM, pp. 378–388 (March 2006)
13. Mircovic, J., Reiher, P., Thomas, R., Schwab, S.: Automating DDoS Experimentation. In: Proceedings of the DETER Workshop (August 2007)
14. Bolla, R., Bruschi, R.: RFC 2544 Performance Evaluation for a Linux Based Open Router. In: Proc. of the 2006 IEEE Workshop on High Performance Switching and Routing (HPSR 2006), Poznan, Poland, pp. 9–14 (June 2006)
15. Yu, J., Lee, H., Kim, M.-S., Park, D.: Traffic flooding attack detection with SNMP MIB using SVM. Computer Communications 31, 4212–4219 (2008)
16. Mircovic, J., Hussain, A., Fahmy, S., Reiher, P., Thomas, R.K.: Accurately Measuring Denial of Service in Simulation and Testbed Experiments. IEEE Transactions on Dependable and Secure Computing 6(2), 81–95 (2009)
17. Bray, T., Paoli, J., Sperberg-McQueen, C.M., Maler, E., Yergeau, F.: Extensible Markup Language (XML) 1.0, 5 edn. (2008), http://www.w3c.org/TR/REC-xml
18. Botta, A., Dainotti, A., Pescapè, A.: Multi-protocol and multi-platform traffic generation and measurement. In: INFOCOM 2007 DEMO Session, Anchorage (May 2007), http://www.grid.unina.it/software/ITG/
19. Shneidermann, B.: Designing the User Interface: Strategies for Effective Human-Computer Interaction, 3rd edn. Addison-Wesley, Reading (1998)

Discrete Event Simulation of QoS of a SCADA System Interconnecting a Power Grid and a Telco Network

Ester Ciancamerla[1], Chiara Foglietta[1], Davide Lefevre[1], Michele Minichino[1], Leonid Lev[2], and Yosi Shneck[2]

[1] ENEA, via Anguillarese 301, 00100 Rome, Italy
[2] Israel Electric Corporation, Haifa, Israel
ester.ciancamerla@enea.it, chiara.foglietta@enea.it, davide.lefevre@enea.it, michele.minichino@enea.it, leonid.lev@iec.co.il, shneck.yosi@gmail.com

Abstract. Indicators of Quality of Service (QoS) of Fault Isolation and System Restoration (FISR) service, delivered by SCADA system are computed, discussed and correlated to quality indicators of power supplied to customers. In delivering FISR service, SCADA system, Telco network and Power grid act as a whole heterogeneous network. While SCADA system and Telco network can be well represented by means of discrete event simulators. To represent a Power grid a continuous simulator is typically required. In the paper, to compute QoS of FISR, SCADA system, Telco network and Power grid have been represented by a unique model by means of a discrete event simulator.

Keywords: Critical Infrastructures, SCADA, Quality of Service, Discrete Event Simulation.

1 Introduction

SCADA systems constitute the nervous systems of Power grids. They rely on SCADA communication links which are dependent upon Telco networks and represent one of the major channels for mutual propagation of disturbances and adverse events between Power grids and Telco networks. Power grids and Telco networks have a heavy impact on daily life and are typically referred to as Critical Infrastructures (CIs), since their correct operation is essential for the everyday life of our modern society. Dependent (bi)directional relationships and reciprocal influences among CIs are named (inter)dependencies. CIs are more and more reliant on information and communication technology and, largely through this reliance they have become more and more interdependent [1].

There is a growing interest in developing models and tools for CI interdependency analysis. In literature, a huge extension of modeling approaches is underway. A network topology analysis takes inspiration by [2]. [2] and underlines how a given topological network asset may improve network resilience in response to an accidental failure but may also expose the network to high vulnerabilities in the presence of malicious attacks. A simulative analysis in which a federation of multiple domain-specific simulators, [3]

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 350–362, 2010.

or the development of specific tools for the simulation of interdependent infrastructures, [4] is proposed. A service oriented risk analysis in which the problem is simplified, considering that CIs support and fulfill services [5, 6, 7].

There are also many studies, which investigate the reciprocal effect of interdependencies among Power grids and Telco networks. Many of the above studies are especially based on Power grid simulation and the SCADA system is not explicitly modeled, or it is considered in a very simple way. In this paper, we discuss the performance and rerouting calculations of a specific service delivered by the SCADA system, and their impact on the QoS of the power supplied to customers. In particular, we refer to the Fault Isolation and System Reconfiguration (FISR) service that detects and isolates faults in the Power distribution grid and then reconfigures the grid to supply the isolated customers. In delivering F ISR service, SCADA system, Telco network and Power grid act as a whole heterogeneous network. Here, we investigate the usability of the same discrete event simulator, NS2, which fits very well to represent the SCADA system and Telco network, also to represent the power grid, limited to the implementation of FISR service. To build realistic models we refer to an actual case study, named Reference scenario, defined with the expertise of Israel Electric Corporation (IEC) in the framework of the MICIE project [8].

2 Reference Scenario

A Reference scenario is needed to limit the extension of the real world to be included in the analysis, and to provide a concrete context of operation, concentrated on CI interdependencies. Reference scenario identifies the following items: a) services; b) the set of interconnected networks supporting such services (in terms of topologies, essential systems: i.e. Telco emergency power supply, cooling systems); c) interconnections and types of interconnections among networks and systems; d) sequences of possible adverse events (failures, attacks, congestions) that could impair the quality of such services (in terms of continuity, readiness, performances, time response) and may include e) operator procedures to implement services under consideration.

Figure 1 shows the top level view of our Reference scenario. Natural or internal (malicious or random) adverse events (left boxes) hit (specific components of) interdependent Electrical, Communication and Information Infrastructures (boxes 1, 2 and 3 inside the central dashed box) and may propagate to customers of the Medium Voltage (MV) grid in terms of interruption of power supply. The interdependent SCADA system, Telco network and MV power grid, under consideration to represent FISR services, are respectively included in boxes 3, 2, 1. FISR, performed by SCADA system by means of SCADA operator is a particularly critical service because its degradation affects the quality of power supplied to customers.

In Power grids, failures may cause de-energisation for a large number of power customers and need to be located, isolated and repaired quickly and safely. In Reference Scenario, FISR service is remotely operated by the SCADA operator, that implements a specific procedure (based on grid monitoring, loss of power sensing, Circuit breakers operations) by means of Remote Terminal Units (RTUs). For confidentiality reasons the networks considered in the paper are just realistic abstractions of the actual ones of a geographical district of Israel, specifically customized for MICIE EU Project [8] by IEC experts.

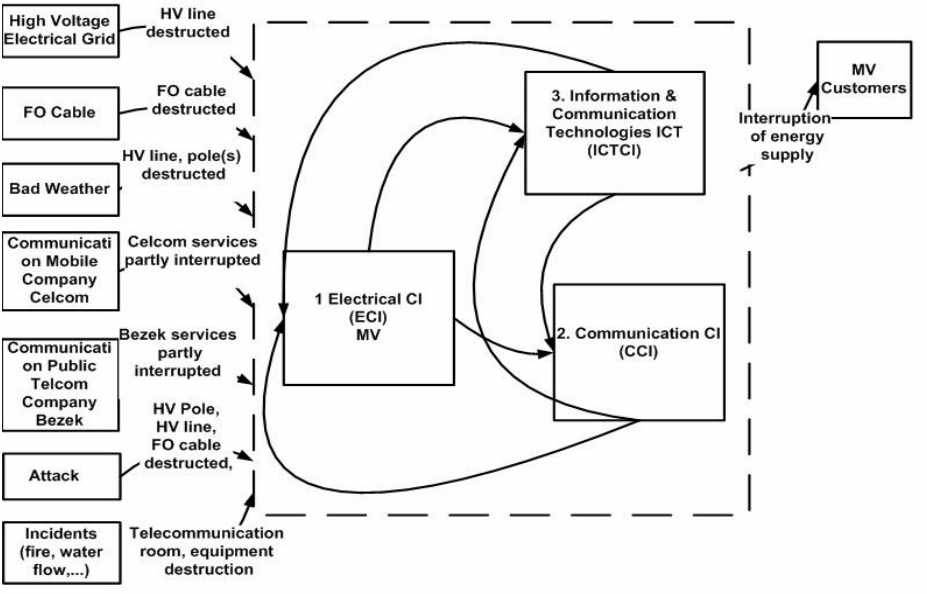


Fig. 1. Top level view of Reference scenario

2.1 MV Power Grid

Figure 2 shows the simplified view of the power distribution grid topology under consideration for FISR. It consists of a portion of a Medium Voltage (MV) grid at 22 KV, energised by two substations, named TF and CB.

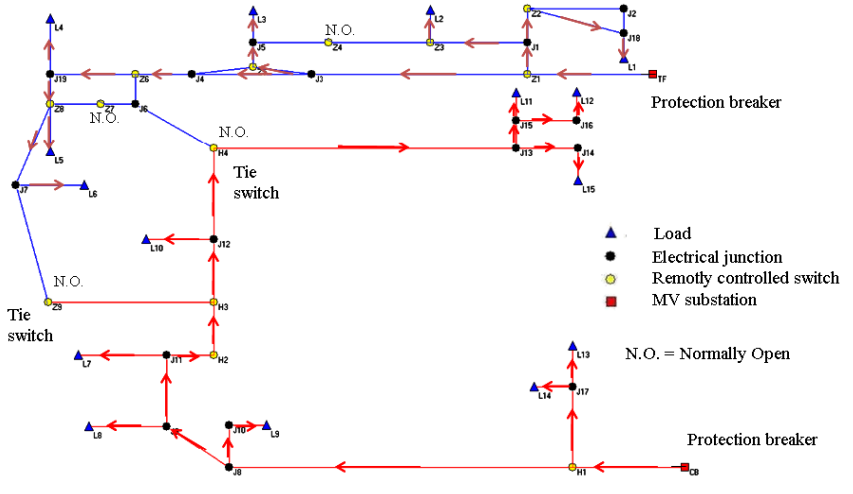


Fig. 2. A simplified view of MV power grid

Each substation feeds different types of loads/customers (public, commercial, industrial), throughout electrical sections, connected one to another by Normally Close Circuit breakers. TF and CB substations include Protection breakers. In normal operative conditions, customers are energised by either TF substation or CB substation, by means of two sub grids, separated one from the other by two, Normally Open, Tie switches, remotely controlled by SCADA system. SCADA is also interconnected with the MV grid by means of its Remote Terminal Units to monitor the grid status and act on their Circuit breakers for connecting/isolating grid electrical sections.

2.2 SCADA System

Figure 3 shows the portion of SCADA system under consideration for FISR. From SCADA Control Centre (SCC), the operator remotely manages and controls in real-time the power grid of figure 2, by means of RTUs.

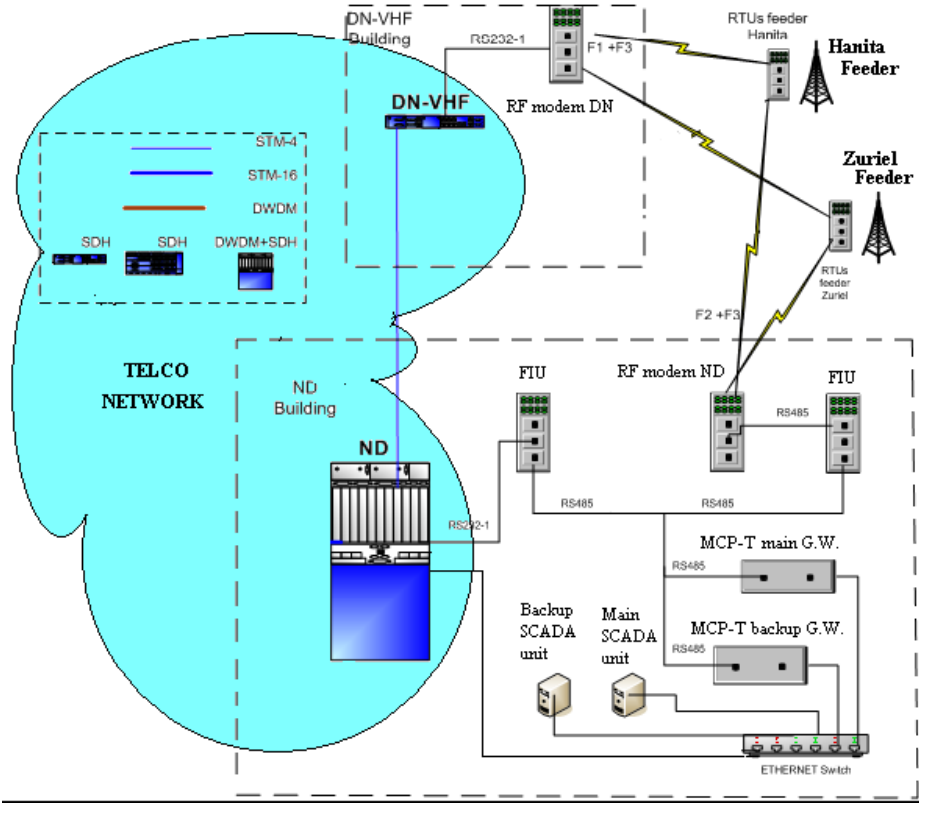


Fig. 3. SCADA system

Particularly, the following devices belong to the SCADA system:

- MCP-T gateway which converts a proprietary Data Link Communication (DLC) protocol to the TCP/IP protocol. DLC protocol is designed for radio channels and allows multiple logical communication channels per communication medium. For DLC and TCP/IP protocols, every transmission is automatically accompanied by an ACK message, ensuring the integrity of the transmission.
- Field Interface Unit (FIU), dedicated to RTU interrogation and routing of data messages to/from SCC. FIU comprises a Radio Frequency (RF) Modem Interface (RF Modem ND), that includes two VHF radio units (F2, F3), that connect RTUs to SCC throughout either F2 or F3 channels.
- Store & Forward (S&F) Repeater DN which communicates upwards with the SCC (via the RF Modem and FIU) and downwards with the RTUs using the two RF channels (F1and F3).
- RTUs; there are 13 RTUs sites, of which 9 belong to TF and 4 to CB.

SCADA system is fully redundant. In case of failure of the main SCADA unit, the backup SCADA unit is enabled. The main communication path between SCC and the RTUs traverses the main Gateway and the main FIU. In case of failure on the main path, data are rerouted on the backup path that traverses the backup Gateway, the backup FIU, the Telco network (Point of Presence ND and Local eXchange DNVHF), S&R repeater and then reaches the RTUs. In case the primary RF channel is not available for any reason, the system switches to the alternative RF channel.

2.3 Telco Network

It is composed by three hierarchical layers:

- A Backbone layer, where Point of Presence (PoP) devices (figure 4) are connected one to another in a meshed topology. Its application is transport, so its primary concern is capacity. PoP is a multiservice optical platform that integrates several technologies including Synchronous Digital Hierarchy, Synchronous Optical Network (SDH/SONET) and Dense Wavelength Division Multiplexing (DWDM) in a single platform.
- A Local eXchange layer (LeX) (figure 4), the closest one to customers at the edge of the Transit eXchange layer, represents the point of access at lower bandwidth of Telco network. In this layer, IP traffic, with its inherently asymmetric and unpredictable nature, is predominant, especially with real-time applications.
- Between these two layers, lies the Transit eXchange layer (TeX) (figure 4) that grants scalable traffic in multi-ring topology. A TeX device is based on SDH/SONET technology that aggregates data flows at different bit rates and retransmits them over long distances. It relies on optical rings constituted by ADM (Add Drop Multiplexer) and optical cables. ADMs perform signal multiplication (they gather many tributary signals and multiplex them into one signal at a higher rate), transmission over optical fibers and protection (by rerouting over the SDH ring in case of a single failure).

2.4 Heterogeneous Network Supporting FISR Service

SCADA system, MV power grid and Telco network constitute a single heterogeneous network that supports FISR service, as shown in figure 4. In figure 4, a box bounds the main SCADA devices (except RTUs and radio links), a box bounds Telco devices that support a SCADA redundant link, and a box bounds the Power grid. There are several interconnections among these networks. SCADA system interacts with MV Power grid by means of SCADA RTUs (in figure 2 and inside the Power grid box of figure 4). Also SCADA devices, including RTUs and devices in Control Centers, are powered by the same MV Power grid. SCADA system also interacts with Telco network by means of the redundant link, which traverse PoP ND and LeX DN-VHF devices, and by the communication link between SCADA Control Centre and PoP ND, as shown in figure 3.

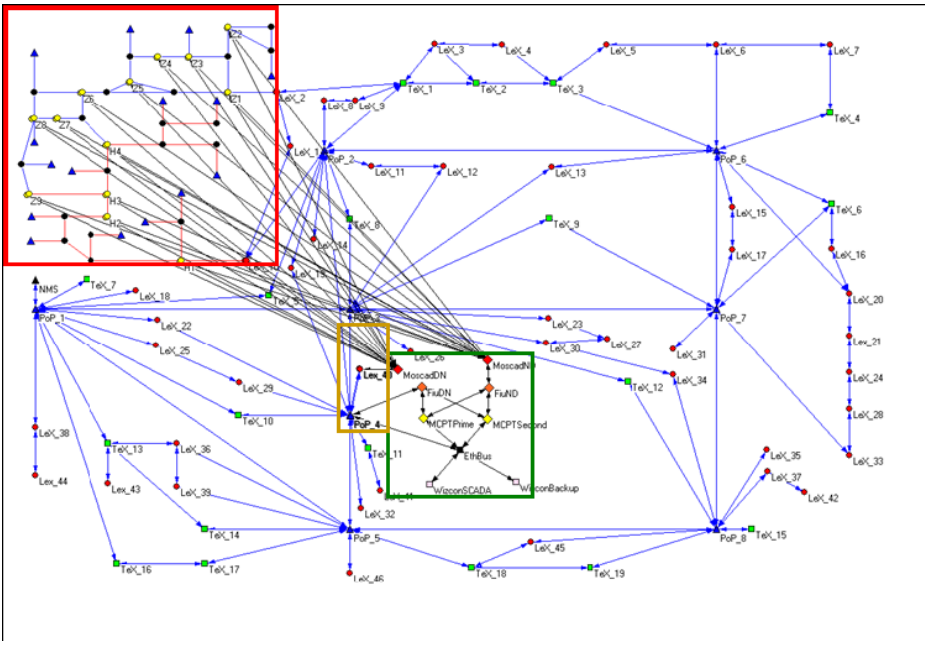


Fig. 4. Heterogeneous network supporting FISR service

3 Discrete Event Simulation of Heterogeneous Networks

QoS of FISR is computed by representing Power grid, SCADA system and Telco network as a single heterogeneous network in which continuous and discrete parameters coexist. Power grid mainly consists of elements that are typically modeled by continuous equations. Physical laws that dictate the behavior of electro mechanic elements of power grid are described by differential equations with some discrete dynamics needed to represent Circuit breakers. Then, to represent Power grids typically continuous simulators are used. The other way around, where SCADA and

Telco networks are packet switching networks, then they need to be represented by discrete event simulators.

In our case, to compute QoS of F ISR, we need a full scale representation of SCADA and Telco network which act to implement FISR on the power grid and a proper representation of the power grid, as it is observable by the SCADA control centre (SCC), for the service under consideration. In general, the Power grid is observable by SCC in terms of bus voltages, line, generator & transformer flows (MW, MVAR & Amperes, transformer taps & breaker status as well as other generator parameters (e.g. limits), frequency, requiring a full scale simulator for its representation. The concept of observability of power grid from SCC, limited to FISR service, can be simplified, by just representing the topology of the grid (substations, trunks, loads, junctions, RTU breakers), and the events involved in FISR service (remote On/Off operation of RTU breakers from SCC, presence/absence of the electrical flow from the feeding Substations to loads, according to electrical Junctions and RTU breaker positions, and occurrence of possible failures in any electrical section of the grid). For such a limited representation of the Power grid, we may resort to a discrete event simulator. Among discrete event simulators we choose NS2, one of the most widely used open source network simulators [9]. NS2 allows to simulate packet based local/wide area networks and wired/wireless networks and then it may well represent SCADA and Telco networks. First, we built a separate NS2 script for SCADA system, Telco network and power grid, than we integrate them to have a whole FISR model that relies on the heterogeneous network shown in figure 4.

4 Quality of FISR Service

The quality of FISR service is critical because it is strictly correlated to the quality of power supplied to customers. There are different indicators of the quality of power supplied to customers, such as the duration of power interruptions for a customer per year, the number of long/short power interruptions for customer per year, etc. Values of such indicators are typically regulated by a National Electric Authority. A timely actuation of FISR service, consequential to a permanent failure of the grid, reduces the outage duration and then contributes to keep indicators of quality of power supplied to customers within prefixed values. On the contrary a delayed actuation of FISR service gets the worst such indicators.

Here, we investigated *FISR response time* and correlated it with indicators for quality of power supplied to customers. *FISR response time* is considered a *composed* indicator because its values depend upon the values of indicators of performances and reliability of the networks that support such a service, here referred to as *basic* indicators. We investigated *s-t dynamical path* and *s-t Round Trip Time* as basic indicators of FISR. *FISR response time* is intended as the time between the occurrence of loss of power supply to customers (due to a grid failure) and the restoration of power supply to customers. We correlate it with the duration of grid outage and the percentage of customers affected by the outage. *S-t dynamical path* is intended as the path of nodes traversed by a packet from a source to a destination. It dynamically changes in consequence of network re-configuration caused by network congestion or link/node failures. It is computed between SCADA Control Centre and RTUs. *S-t packet Round Trip Time* (RTT) is intended as the packet transmission time,

from a source to a destination plus the ACK time (from destination to source) – for TCP-IP protocols. It is computed between SCADA Control Centre and RTUs.

5 Model of FISR Service

FISR service is delivered by SCADA operators, according to procedures which may vary from one case to another. To represent FISR we account the following procedure [10]. Initially, MV power grid (Figure 2) is in its operative conditions. Then, randomly, a permanent failure occurs on any electrical section of the sub grid fed by either CB or HF substations. As a consequence the Protection breaker at the substation will trip. After two automatic reclosing attempts, the Protection breaker remains open, de-energizing all of the sub grid. The loss of power is sensed by each RTUs and using its backup battery, it opens the corresponding Circuit breaker,at this point, the "failure detection process" starts by re-closing progressively all breakers, starting from the one closest to the electrical substation up to the detected failed section.

On the attempt of the re-closure of the breaker at the head of the failed section, its RTU senses the loss of power and immediately re-opens the breaker and sends an alerting message to SCC, which acknowledges it. The re-opening of this breaker ensures that the failure is isolated. During such failure detection and isolation process all the customers included in the portion of the sub grid between the head of the failed section and the Normally Open Tie switches remain de-energised. At this point the "power restoration process" starts, remotely performed by the SCADA operator. The actual implementation of such a process depends upon the location of the failure inside the sub grid, and may include, if necessary, the closure of Normally Open Tie switches (thanks to request/response messages between SCC and RTUs) in order that all customers, except those included in the failed section, can be energised by the other substation. After the repair of the failed section, the grid can be reported to its initial configuration.

5.1 Sub Model of Telco Network

Telco network under consideration (figure 4) is composed of 74 nodes: 8 PoPs of the optical Backbone, 19 TeX, 46 LeX and 1 NMS (Network Management System).

Table 1 summarizes the main modeling assumptions. To generate a realistic traffic over the network, we consider that it hosts reliable traffic (i.e. for real time control devices and equipment, including SCADA) and less reliable traffic (i.e. enterprise traffic). We assume traffic generation according to two types of transport layer protocols of the IP (Internet Protocol) family, TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) that provide network services for applications and application layer protocols. TCP and UDP perform their services by employing IP to route packets to their destination. TCP provides connection-oriented, reliable, bytestream packet delivery. UDP is a connectionless, unreliable message delivery protocol. The routing policy of the network nodes is a DV (Distance Vector) type. The queue of each link is Drop-Tail, which implements FCFS (First Come First Served) scheduling and drop-on-overflow buffer management.

Table 1. Assumptions on Telco network

Link Type	Backbone (DWDM)	TeX (STM-16)	LeX (STM-4)
Capacity	10 Gbps	2.5 Gbps	600 Mbps
Source/Destination Node	PoP-PoP	PoP-TeX, TeX-TeX	PoP-LeX , TeX-LeX, LeX-LeX
Traffic Type	TCP+UDP	TCP	TCP
Traffic Bit-Rate	12 GB (TCP) + 8 GB (UDP)	12 GB	12 GB
Type of Agents	CBR for UDP		FTP for TCP
Number of Agents	100 for UDP		100 for TCP

5.2 Sub Model of SCADA System

The communication between main SCADA Centre and RTUs is implemented by a request/response application protocol that relies on the TCP/IP transport layer protocol. The radio links between RTUs on one side and RF modem ND or RF modem DN_S&F on the other side, were implemented as ideal wireless links by means of a 'no loss' model (i.e. no shadowing, fading,…). Connections and IP traffic among Control Centre nodes and RTUs as well as among the nodes within the Control Centre were implemented with reference to [11]. Connections between the SCADA Control Centre and the RTUs were implemented by installing a TCP agent over each RTU, and a symmetrical TCP agent over each node representing the Control Centre. Then, on each TCP agent we locate a CBR (Constant Bit Rate) traffic source that transmits a packet of 255 bytes length, conforming to [11], with regular intervals of 30 sec to simulate exchange of messages among RTUs and Control Centre nodes. The request -response mechanism between SCADA Centre and RTUs is implemented by means of the simulator's scheduler. Each Control Centre request to the RTU activates a CBR source on the RTUs as soon as the request is completely received. The TCP agent on the generic RTU will begin to transmit the response messages after a time interval, during which the RTU processes field data from the related electrical section of the grid. Table 2 summarizes the main assumptions.

Table 2. Assumptions on SCADA communication links

Link Type	Ethernet	RS-485	RS-232	VHF-radio
Capacity	100 Mbps	19.2 Kbps	19.2 Kbps	4.8 Kbps
Source/ Destination Node	SCADA - MCP_T – PoP	MCP_T-FIU FIU- RF modem	RF modem - Telco Nodes	RF modem - RTU
Traffic type	DLC (TCP)+ TCP	DLC (TCP)	DLC (TCP)	DLC (TCP)
Traffic bit-rate	256 bytes /30 sec	256 bytes /30 sec	256 bytes/30 sec	256 bytes /30 sec

Occurrence of failures of electrical sections are detected and transmitted by RTUs and Substations to SCADA Control Centre. SCADA sub model represents the main path and the back up path between SCADA CC and RTUs. In case of failure of the main SCADA unit, the backup SCADA unit is enabled. In case of failure of the main FIU and/or of the main Gateway, data are rerouted on a backup path. Queue types and

buffer sizes (the maximum number of packets can be stored before dropping) of links are defined as for Telco network sub model.

5.3 Sub Model of Power Grid

NS2 sub model of the grid consists of 49 elements: 2 substations, 13 Circuit breakers driven by correspondent SCADA RTUs, 19 junction nodes and 15 loads. In normal operation, the grid is separated into two sub-grids by means of Normally Open Tie switches. One sub grid, energized by TF substation, feeds 6 loads, while the other sub grid, energized by CB substation, feeds 9 loads. NS2 sub model of the MV power grid is interconnected with NS2 sub model of the SCADA system by means of Circuit breakers/RTUs. The status of Protection breakers at substations TF and CB is monitored by the SCADA Control Centre that can also actuate their remote reclosure.

To build a worthwhile NS2 sub model of the grid, careful attention has been paid to translate events and object of the electrical domain into adequate discrete modeling assumptions. The electrical current flowing from substations to loads is represented by CBR (Constant Bit Rate) packets transmitted from substation to loads by means of a static (source) routing protocol and a UDP transport layer protocol. UDP packets are sent almost continuously by an NS2 node representing the substation to NS2 nodes representing loads. On/off operations on the N.C. Circuit breakers, remotely driven by SCADA sub model, are represented by the occurrence of up/down events on the link that represents the electrical section posed immediately after (according to the direction of the electrical current in nominal conditions) the breaker. Along FISR implementation procedure, the direction of the electrical current on the grid may change upon operations on N. C. Circuit breakers or on N.O. Tie switches. Then the static routing policy of the NS2 model of the grid changes accordingly.

6 Simulation Results

In FISR model, we have grouped the occurrence of permanent failures on any electrical section of MV power grid as follows:

- failure in an initial section of the grid (bounded by the feeding substation and its closest RTU): the loads of failed sub-grid are energised by the other substation, up to the manual repair, that restores the initial configuration of the grid;
- failure in an intermediate section of the grid (bounded by two RTUs): the loads into this section are isolated, the loads bounded by failed the section and the tie switch are powered by the other substation, up to the manual repair, that restores the initial configuration of the grid;
- failure in a terminal section of the grid (bounded by RTU and loads): the loads of failed section are isolated, up to the manual repair, that restores the initial configuration of the grid.

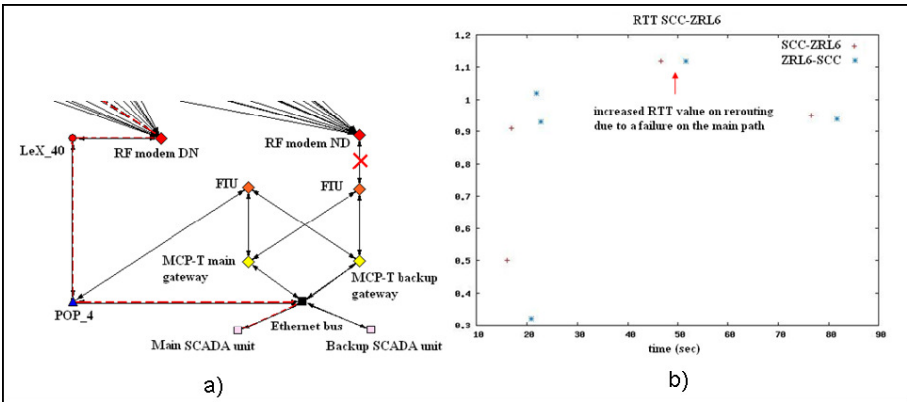


Fig. 5. a) S-t dynamical path and b) S-t RTT on failure in the main path of SCADA

Basic and *composed* indicators of QoS have been computed, under the following normal and failure conditions, by FISR model: *case 1)* normal condition of the SCADA system and Telco network; *case 2)* a failure of a SCADA element (i.e. the link between FIU and RF modem); *case 3)* a failure of a SCADA element (i.e. the link between FIU and RF modem) and a failure of a Telco network element (i.e. the link between PoP ND and LeX DN-VHF). Figure 5.a) shows, as dashed lines, the graphical representation of the *s-t dynamical path* between the Main SCADA unit of SCC and an RTU (ZRL6) in the presence of a failure of the link between FIU and RF modem ND of the SCADA system. Such a dynamical path is a back up path of the fully redundant SCADA system. Figure 5.b) shows, indicated by an arrow, the numerical value (sec.) of the *s-t Round Trip Time* of the messages between the Main SCADA unit of SCC and an RTU (ZRL6 RTU). This RTT value is greater than the corresponding RTT value with no failure on SCADA elements.

We have computed FISR response time and we have correlated it with the duration of grid outage and the percentage of the customers which remain isolated from the feeding substation (affected customers). The percentage is computed respect to the total number of the customers of the grid.

Table 3 summarizes the values of FISR response time and the percentage of affected customers for the three possible locations of the permanent failure on the power grid, and in different operative conditions (cases 1, 2 and 3) of SCADA system and Telco network. The first column of the table reports the failure location (within an initial, intermediate and terminal electrical section of the grid) that requires the

Table 3. FISR response time and % of customers affected by power outage

Section of failure	Response time case 1	Response time case 2	Response time case 3	% of affected customers	
				Before FISR	After FISR
Initial	18.4 sec.	18.6 sec.	> simulation time	46.6	0
Intermediate	34.8 sec.	35.2 sec.	> simulation time	26.6	0
Terminal	29.1 sec.	29.4 sec.	> simulation time	26.6	6.6

activation of FISR. Column 2 reports FISR time response with no failure of the SCADA system and Telco network (case 1). Columns 3 and 4 respectively report FISR time response under a failure of a SCADA element (case 2) and under a failure of a SCADA element and a Telco network element (case 3). FISR response time gets worst when passing from absence of failures up to a critical double failure. The percentage of the affected customers depends upon the section of the grid in which the failure is located. Failures in the initial section of the grid affect a higher percentage of customers. In case of a failure in the terminal section of the grid, there is a percentage of customers out of power service till the manual repair of the failure of the grid has been completed. The outage duration of the affected customers, in case 1 and 2, corresponds to the FISR response time plus the manual repair time when needed. Manual repair time is needed in case of failure in a terminal section of the grid. In case 3, FISR cannot be actuated remotely by SCC and the outage duration corresponds to the manual repair of the permanent failure of the grid.

7 Conclusions

The paper investigates the QoS delivered by interdependent infrastructures. Within a Reference scenario, the Quality of Fault Isolation and System Restoration (FISR) service, delivered by interconnected Power grid, SCADA system and Telco network has been investigated under nominal and failure conditions. We demonstrate the applicability, the advantages and the limits of using a unique discrete event simulator, to represent the three heterogeneous networks supporting FISR service. Basic and composed indicators of Quality of FISR have been computed and a correlation between them and Quality of Service to grid customers has also been discussed.

Acknowledgments. This research was partially motivated by EU projects MICIE http://www.micie.eu, IRRIIS http://www.irriis.org/ and the Italian MIUR project CRESCO http://www.cresco.enea.it/

References

1. Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K.: Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine 21(6) (2001)
2. Albert, R., Barabasi, A.L.: Statistical Mechanics of Complex Networks. Review of Modern Physics 74, 47–97 (2002)
3. Hopkinson, K., Wang, X., Giovanini, R., Thorp, J., Birman, K., Coury, D.: EPOCHS: A Platform for Agent-Based Electric Power and Communication Simulation Built From Commercial Off-the-Shelf Components. IEEE Trans. on Power Systems 21(2) (2006)
4. Dudenhoeffer, D., Permann, R., Manic, M.: CIMS: A framework for infrastructure interdependency modeling and analysis. In: Proc. of Winter Simulation Conference (2006)
5. Bonanni, G., Ciancamerla, E., Minichino, M., Clemente, R., Iacomini, A., Scarlatti, A., Zendri, E., Terruggia, R.: Exploiting stochastic indicators of interdependent infrastructures: the service availability of interconnected networks. In: Martorell, S., Soares, C.G., Barnett, J. (eds.) Safety, Reliability and Risk Analysis: Theory, Methods and Applications, vol. 3. Taylor & Francis, London (2009)

6. Capodieci, P., et al.: From heterogeneous modeling and analysis to an on line prediction tool to improve QoS of interdependent networks. Electricity, Tel Aviv, Israel (2009)
7. Bobbio, A., Ciancamerla, E., Diblasi, S., Iacomini, A., Mari, F., Melatti, I., Minichino, M., Scarlatti, A., Terruggia, R., Tronci, E., Zendri, E.: Risk analysis via heterogeneous models of SCADA interconnecting Power Grids and Telco Networks. In: CRiSIS 2009, Toulouse, France, October 19-22 (2009)
8. http://www.micie.eu
9. http://www.isi.edu/nsnam/ns/
10. http://www.itsinfo.com/doc/moscad_electric_power.pdf
11. IEC870-5-1 01/105 guidelines

Critical Infrastructure Protection Risk Modelling with Games Technology

Martin Masek, Adrian Boeing, and William Bailey

School of Computer and Security Science, Edith Cowan University, 2 Bradford Street, 6050 Mount Lawley, Western Australia
m.masek@ecu.edu.au, a.boeing@ecu.edu.au, b.bailey@ecu.edu.au

Abstract. Threats to critical infrastructure are not passive. Trying to identify what is in fact 'critical' is proving to be very difficult as threats constantly evolve. A major benefit of simulating the infrastructure is that security tests and risk modelling can be applied before infrastructure is built or its environment modified, allowing for lower cost design alterations to minimise vulnerabilities. By using the 3D environment of an existing Game Engine we can explore several possibilities for security analysis that existing tools, due to their global view of the problem, do not allow. Providing participants with a first-person view of the situation allows for more realistic role-play, whilst the networked gaming technology allows remote experts to interact in an intuitive environment and explore, identify and assess the critical components of the infrastructure.

Keywords: Critical Infrastructure, Real-time Simulation, Risk Assessment, Games Technology.

1 Introduction

In the Australian context, critical infrastructure has been described in the National Guidelines for Protecting Critical Infrastructure from Terrorism as:

"those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security" [1].

There are several reasons why critical infrastructure can fail. However the additional risk is that caused by terrorist or criminal activity. For example, the rupture of a pipeline is a technical failure. The risk of such technical failures can be determined through standard risk engineering, where risk is measured as the probability of failure multiplied by the severity of the consequences. Such risks can be mitigated by analysing the probability of failure and building in safety margins, redundancies, and maintenance processes to lower the risk to an acceptable level.

An additional cause for failure is deliberate interference and sabotage. Although a classical probabilistic-based risk approach is at times used to determine an appropriate level of protection, its validity is questioned for such cases. Manunta [5] identifies

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 363–372, 2010.

potential shortcomings that challenge some of the assumptions behind the use of classical risk based approaches. If a security specialist uses the probability of an attack to identify areas to defend, an attacker can utilise the same probabilities to identify areas that will not be defended. Such threats are not static and can evolve when they encounter counter-measures.

In today's security industry, there is still certainly the philosophy of protecting business interests against crime and in its purest form the "Crime Triangle" has certainly helped in identifying and assisting in the analysis of those threats. This then has to be translated in to the physical security measures we often see still in existence today, ranging from guards to access control and CCTV.

"A security consultant...is called on to...assess what types of threats or risk affect the assets to be protected, render an opinion on the probability of those threats or risks, and recommend a security or loss prevention plan to reduce the probability of those threats or risks" [6]. Often though, security was always considered as an afterthought, or a reactive approach to a negative event that has happened to an organisation.

Gibson [7] highlights that "Risk awareness in the corporate security function should be a practical discipline. Its aims should be explicit, open and objective." This approach ensures that the function is able to quantify the risk, the appropriate preventative measures and align the cost benefit to the organization against its overall strategic goals. The understanding of risk and consequence has helped the security professional to look beyond fortifying their assets or business to a more proactive and dynamic approach to risk. "The security function has traditionally been an experienced-based discipline. However security practitioners are utilizing management disciplines and theories of risk in order to compliment their experience" [7].

What is questioned here is not the "risk assessment" in itself, but it is the methods used to accomplish this assessment. Many organisations perform security risk assessments only once a year, although since September 2001, some organisations undertake reviews on a more frequent basis [7]. Manunta [5] questions the relevance of such ad hock reviews of risk, because by the time the results arrive, they tend to be outdated. The context will dictate the how quickly such results become invalid. But in the current security climate, the terrorist threat is dynamic, evolutionary, and able to adapt and learn.

2 Tools for the Analysis of Critical Infrastructure

Several tools exist for the simulation of critical infrastructure. Simulation tools provide an avenue for more frequent risk analysis using the simulation. Such tools also help bridge the gap in understanding between experts from different disciplines by determining the effect of changes to the system whilst hiding its complexity [8]. This makes each expert area accessible to the whole team, allowing the propagation of system failures and its extent to be determined. Pederson et al. [9] identified 30 simulation systems in a survey of research into critical infrastructure interdependency modelling. These simulations range in maturity from research to commercial systems and model a variety of infrastructure using various simulation types.

Most existing critical infrastructure simulations provide a simple single-user graphical visualization of the infrastructures and their interdependencies. This typically consists of a graph display, with infrastructure nodes connected by edges to show interdependencies. Some simulations are integrated with a Geographic Information Systems (GIS) application and the graph is overlaid over a top-down 2D map of the area. Such displays are useful for traditional risk-based analysis in the design and analysis of critical infrastructure systems, but not for producing a risk mindset based on local vulnerabilities that only a person on the ground would be able to identify.

A simulator that lets users take the roles of a person on the ground would allow for the enactment of realistic scenarios, allowing response times and behaviour patterns to be determined. Such a simulator, through role-play, would allow users to gain an insight into the mindset of an operative on the ground, whether it is facility architects seeking to determine how security guards might act, or response personnel playing the role of a terrorist in the simulation in order to understand how a terrorist might act. Finally, the inclusion of artificial intelligence (AI) controlled characters in the simulator would allow for the simulation of human activities. This is useful for automatic testing of the infrastructure and simulating the behaviour of large crowds, or for training personnel such as incident commanders without the need for physical personnel to take on the roles that are directed by the commander. A major benefit of simulating the infrastructure is that security tests can be applied before infrastructure is build, allowing for lower cost design alterations to minimise vulnerabilities.

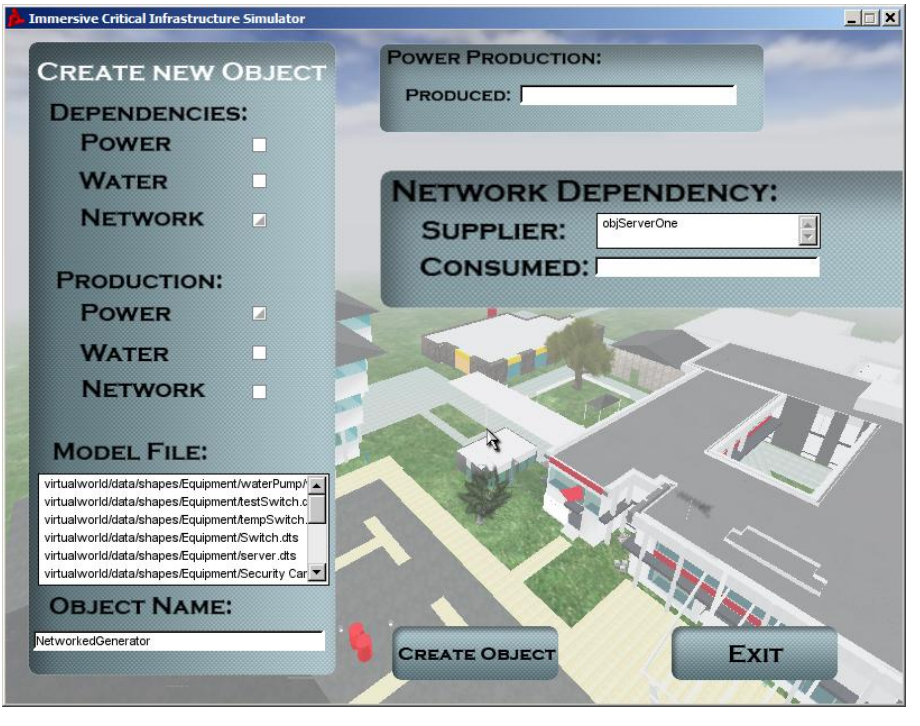


Fig. 1. Creating a networked power generator

By leveraging games technology there is the ability to present the “intruder” into the visual concept thus allowing for a greater assessment of the potential capability of actually inflicting damage. Many times this is a perceived threat that is not borne out by the reality of the known situation. Moreover, once a target has been identified there is the added ability to develop variations of target hardening, which can be tested prior to implementation. This has substantial cost benefits as it is not necessary to actually build in the suggested changes, in order to test them against the “intruder”.

3 Real-Time Interactive Critical Infrastructure Simulation

Our proposed solution is an interactive, high fidelity simulation tool built using existing games technology. This allows us to adapt the existing workflow typically used when producing a game to rapid scenario construction. The online nature of modern computer games gives greater opportunities for remote experts to perform security reviews and exercises.

To design and produce a virtual world for a computer game involves a large amount of iteration. An environment is designed by the positioning of obstructions to limit the player's movement, and the insertion of non-static objects such as enemy AI characters. The game is then repeatedly tested and modified in order to maximise its “effectiveness”. This need for repeated modification has given rise to tools that allow

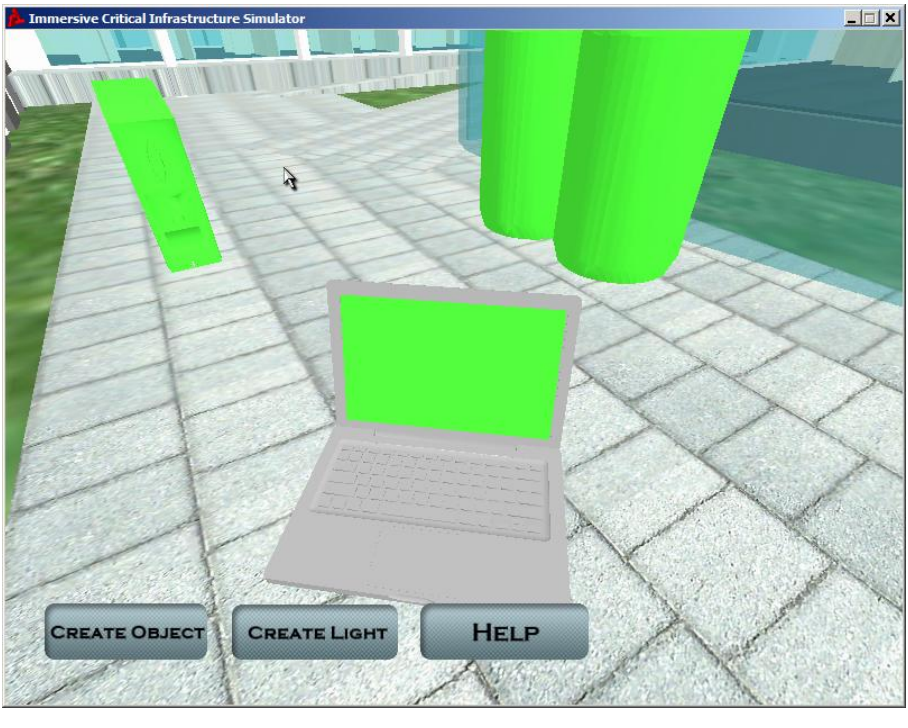


Fig. 2. Three objects are shown in the image, clockwise from top-left: server, power source, and computer representations in the simulator. The green colour indicates the `on' state.

for the rapid construction of worlds and scenarios, allowing designers to modify the game without an in-depth knowledge of programming. There is a similar need for rapid iterative design when seeking to design secure infrastructure, only the definition of "effectiveness" changes. A game is effective if the player is allowed to win whilst being challenged and entertained, whilst infrastructure is effectively protected if the adversaries cannot win.

Our work-in-progress, the Immersive Critical Infrastructure Simulator (ICIS), demonstrates how existing game production tools can be utilised. ICIS has been developed using Torque Game Engine technologies from Garage Games [10]. ICIS consists of an interactive 3D world in which computer networks, along with power and water producers and consumers and their interdependencies are modelled. Various aspects of the game engine are used in a simulation run of ICIS, some can be used unchanged, whilst customisation was performed to implement some features specific to infrastructure simulation.

3.1 Interdependency Simulation

Interdependencies between objects have been implemented using a directed acyclical graph architecture. For example, a light switch can be connected to a power source and a light associated with the light switch. The light can then be turned off by the player activating the switch, or turning off the power source. Similarly, objects can have dependencies on multiple resources. For example, a computer may rely on both the power and network infrastructures to remain operational.

In order to aid in the creation and configuration of nodes in the infrastructure network, a 2D graphical user interface has been overlayed on top of the 3D scenario. This allows objects to be created, assigned resources to generate and to consume, and a graphical representation to be assigned. Figure 1 shows an example of a new object being created, which will produce power and also depend on the computer network infrastructure. The object can be assigned the amount of the resource that is produce, and also which nodes it is connected to in order to service its dependencies.

Infrastructure nodes are assigned a graphical representation, with colour indicating the on (green) or off (red) states. Figure 2 shows the representation of a power source, server, and computer - all in the "on" state.

3.2 Environment Creation

Coupling a critical infrastructure simulator to a 3D environment provides several possibilities for security analysis. For example, accurate views from existing and proposed security cameras can be analysed, as can views from locations where infrastructure could be observed by an attacker. These visibility studies can be performed under various simulated environmental conditions. The ability to modify environmental conditions is possible through the world editor, a tool that is a part of the game engine. Through the world editor, parameters such as the position and brightness of the sun or the effects of precipitation and dust can be interactively adjusted to achieve a desired effect. Figure 3 shows two versions of the same scene with world parameters set to simulate a rainy and dusty day.

Fig. 3. Simulating different environmental conditions

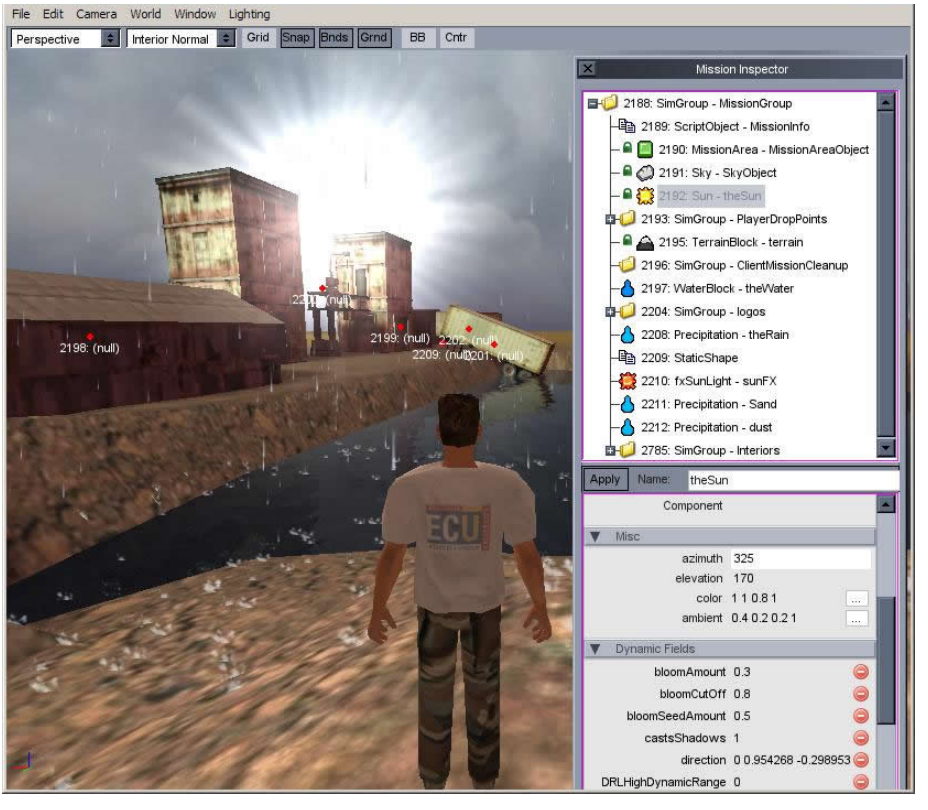


Fig. 4. The world editor allows for the interactive adjustment of the world

Figure 4 shows part of the world editor for the Torque Game Engine Advanced. Objects in the world are shown in a tree hierarchy and each object's properties can be modified interactively by non-programmers, the figure showing some of the properties available for the sun. Besides setting properties, the world editor can also be used to manipulate the objects in the world, allowing aspects of the built and natural

environments to be positioned, either to re-create a scene from the real world, or to create a proof-of-concept environment to be simulated.

The world can be viewed from several cameras, representing the view of different persons or actual cameras in the world. The top down view, much like the one in traditional “big-picture” simulators can also be gained by positioning a camera above the scene looking down, as shown in Figure 5. This kind of view can be used to gain a general overview of the scenario, and is also useful in a de-briefing situation offering a convenient perspective for re-playing a scenario that had been run previously.

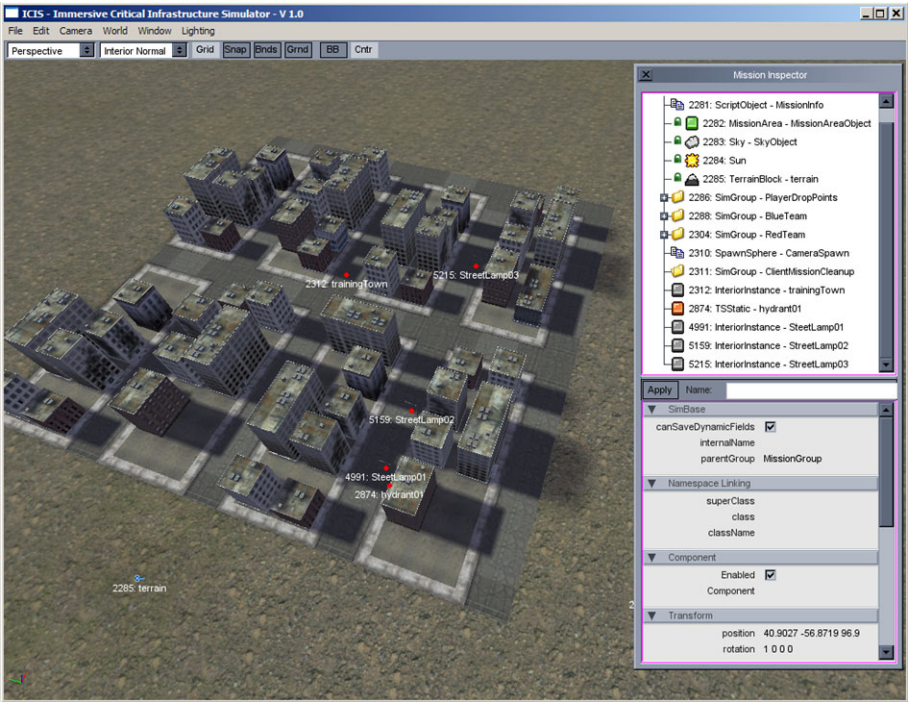


Fig. 5. A “Big-Picture” overview can be obtained using an overhead camera. This can be used by those acting in an observer role, or for re-playing missions as part of a de-briefing.

3.3 Network Architecture

Through the network facilities of the Torque Game Engine, ICIS has the ability to run place multiple users in the same environment. These users can assume a number of roles, including essential services staff and adversaries. The network architecture is based on the client-server model where a server computer runs the simulation, updating the state of the infrastructure based on its dependencies and keeping a global knowledge of the word. Each user interacts with the world through their client PC, which is mainly responsible for displaying graphics on the users monitor and transmitting the users input to the server. This architecture is quite common for game engines, as running the simulation on a central server rather than on each user's

computers reduces the scope for users to subvert the simulation code to cheat. For a simulation intensive use, such architecture is useful as only the server computer needs to meet the requirements to run the simulation in real-time, whilst the client computers can be lower specification machines.

4 Discussion

Through the use of game engine tools, combined with some custom implementation of infrastructure interdependencies it was possible to devise a virtual world simulator where scenarios could be created by non-programmers, and enacted through role-play by various personnel. Through interacting with the virtual world, participants can gain an insight into the mindset of various roles by having to devise strategies first-hand to protect or attack infrastructure.

The use of such simulators offer features with various advantages. Notably, every aspect of a scenario can be logged, allowing missions to be reviewed for analysis and post-mortem purposes. The saving of mission parameters throughout the mission can allow the team to re-attempt the mission from any point in time, thus allowing them to focus on identified weaknesses. Once a point of interest in a scenario has been identified (eg. a critical breach of security), the scenario can be re-played from that point in order to determine the best protection strategy.

Whilst directed acyclic graphs are useful to model infrastructure interdependencies at a high level (in terms of supply and demand for resources), each infrastructure node in a real system is typically reliant on a complex set of processes that may be disrupted through various means. Such processes may require specific modelling methodologies to work within the directed acyclic graph system and require a detailed understanding of the infrastructure nodes. As such, the issue of validation arises.

4.1 Validation

Our current system is undergoing testing, with future work to include the implementation of more types of infrastructure interdependencies and applications targeted towards specific environments and roles. In targeting a specific environment, for example a particular oil refinery or power plant, the issue of acceptable simulation fidelity arises. This issue encompasses the following:

- Correspondence between the response of the simulation tool and the actual infrastructure under normal operating conditions.
- Correspondence under emergency/hazardous conditions.
- Physical accuracy of the 3D environment and its mechanics regarding movement in the world.
- Visual accuracy of the 3D environment.

Correspondence in terms of critical infrastructure and its interdependencies between the simulator and the real world can be validated using historical data that exists for the actual infrastructure. Whilst this data may exist in adequate quantities to validate normal operating conditions, there may be a lack of data for certain kinds of emergencies, as discussed in [11]. For simulation of such situations, historical data can be used

in conjunction with extrapolation and predictive algorithms based on the physical properties of the infrastructure. As complex scenarios, such as attacks and emergencies depend on many parameters, the re-playability of the mission becomes an advantage as various possibilities can be explored.

Various means of validating visual and physical accuracy of the scenarios built environment exist. This includes comparison to plans, but also resources such as aerial survey data. Geographic data is relatively easy to obtain, with 90 metre per point data publically available for the world through the US Geological Survey [12] (with higher resolution data available for purchase through various sources). Quite detailed layouts of various installations are also publicly available using such resources as Google Earth [13]. Whilst imagery in tools such a Google Earth may not be as precise as plans – it does offer useful validation in terms of providing a 'living' plan of the site, where architecture and usage of areas may not actually match that given in the plans. Finally, the testing of a simulator by field experts can provide useful validation in terms of visual accuracy and that of the look and feel of the simulation.

5 Conclusion

Threats to critical infrastructure are not submissive. They constantly evolve, and so too must the ability to defend against such threats. An interactive high-fidelity simulation tool greatly adds to the ability of experts to conduct multiple risk assessments often without the need to physically deploy professional security advisors to the field, providing a considerable cost saving on both time and travel.

Leveraging games technology allows simulation scenarios to be rapidly constructed at a very high fidelity and immediately tested. The networked gaming technology allows remote experts to interact in an intuitive environment and explore, identify and assess the critical components of the infrastructure. The scenario can be modified and different configurations can be examined and tested to ascertain the impact of the change on the risks to the critical infrastructure in consultation with security experts.

Furthermore, the importance of understanding of "consequence" in overall security risk mitigation becomes more obvious because of the visualisation process. Understanding consequence helps in ascertaining the cost to implement mitigation strategies relative to security and return of investment; a crucial budget aspect for companies. With that in mind the consideration of consequence in today's security environment is not only relevant but important in resource determination for the allocation of funds and prioritisation. The use of this type of technology offers a substantial improvement on the cost of conducting a series of risk assessments in the field and allows a company to have a time relative working model of their whole complex. This can be used at any time to test and improve the security measures in place at minimal cost.

References

1. Trusted Information Sharing Network for Critical Infrastructure Protection: Critical Infrastructure Protection National Strategy, Canberra: Trusted Information Sharing Network (2004)

2. Radvanovsky, R.: Critical Infrastructure: Homeland Security and Emergency Preparedness. CRC Press, Boca Raton (2006)
3. Gosch, E.: WA gas supply cut 30pc by blast at Varanus Island, The Australian (2008), http://www.theaustralian.news.com.au/story/0,25197,23824148-5006789,00.html (accessed on February 11, 2010)
4. Sydney Morning Herald: WA faces $6.7b gas bill, Business Day, The Sydney Morning Herald (2008), http://business.smh.com.au/business/wa-faces-67b-gas-bill-20080710-3cxn.html (accessed on February 11, 2010)
5. Manunta, G.: Risk and security: are they compatible concepts? Security Journal 15, 43–55 (2002)
6. Thornton, W.E., McKinnon-Fowler, E., Kent, D.R.: Stalking security statistics. Security Management 35(4), 54–59 (1991)
7. Gibson, S.D.: The case for 'risk awareness'. Security Journal 16, 54–55 (2003)
8. Talend, D: Prototyping of the virtual type, ControlDesign.com (2008), http://www.controldesign.com/articles/2008/168.html (accessed on August 26, 2008)
9. Pederson, P., Dudenhoeffer, D., Hartley, S., Permann, M.: Critical infrastructure interdependency modeling: a survey of U.S. and International research. Idaho National Laboratory Technical Report (2006)
10. Garage Games: Torque Game Engine (2010), http://www.torquepowered.com/ (accessed on February 11, 2010)
11. International Atomic Energy Agency. Application of simulation techniques for accident management training in nuclear power plants (2003)
12. USGS – The U.S. Geological Survey (2010), http://www.usgs.gov/ (accessed on January 5, 2010)
13. Google Earth, http://earth.google.com

Wireless Sensor Networks for the Protection of an Electrical Energy Distribution Infrastructure

António Grilo[1], Augusto Casaca[1], Mário Nunes[1], and Carlos Fortunato[2]

[1] INESC-ID/IST, R. Alves Redol, 9, 1000-029 Lisboa, Portugal
[2] EDP Distribuição, R. Camilo Castelo Branco, 43, 1050-044 Lisboa, Portugal
antonio.grilo@inesc-id.pt, augusto.casaca@inesc-id.pt,
mario.nunes@inesc-id.pt, carlos.fortunato@edp.pt

Abstract. From a safety and security point of view, the electrical energy distribution infrastructure needs to be protected.. In this paper solutions to increase the safety aspects of substation components, power lines and power transformers are discussed. Also security solutions related to perimeter intrusion detection in substations and remote surveillance of power transformer installations are introduced. All the solutions are based on the deployment of wireless sensor and actuator networks in the substation, power lines and power transformers, which perform remote monitoring and provide alarms when required. The sensor network interacts with the SCADA system of the electricity provider to allow for centralised control of the protection system.

Keywords: Wireless Sensor Networks, Critical Infrastructure Protection, Electrical Energy Distribution Infrastructure.

1 Introduction

The electrical energy distribution infrastructure is a critical infrastructure that requires protection for safety and security reasons. The energy distribution infrastructure mainly consists of a set of substations, Medium Voltage (MV)/ Low Voltage (LV) power transformers outside the substation, MV power lines connecting substations to MV/LV power transformers and LV power lines from the MV/LV power transformers to the customers. Some industrial customers may also get direct MV power lines. Associated to this infrastructure we should also consider the SCADA system, which is a supervisory control and data acquisition system for the infrastructure. This infrastructure is illustrated in Figure 1.

For safety reasons remote surveillance of the electrical energy distribution network is already established to some extent based on wired sensors. The use of wireless sensor and actuator networks (WSAN) can lead to a more powerful and efficient protection scenario for the substations, power lines and power transformers. Their higher deployment flexibility allows wireless sensors to capture more status parameters than the existing fixed sensor infrastructure. Specific actuators can also be included in the infrastructure as part of the WSAN. The wireless nature of communication can also contribute to the avoidance of critical points of failure.

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 373–383, 2010.

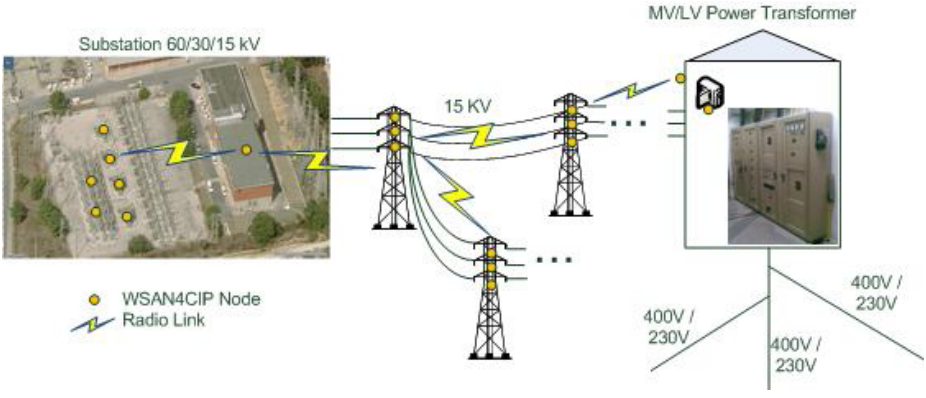


Fig. 1. MV/LV electricity distribution infrastructure

The Wireless Sensor and Actuator Networks for the Protection of Critical Infrastructures (WSAN4CIP) project, which is a European collaborative project running in the 7th Framework Program, has the high level objective of enhancing the reliability of critical infrastructures by providing surveillance data for the management of the infrastructure and to increase the dependability of the critical infrastructure security by providing self-healing and dependability modules for the WSAN. The feasibility of the approach developed in the project is demonstrated using electrical energy distribution and water distribution as representatives of critical infrastructures. In this paper we will focus exclusively on the energy distribution case and primarily at the application level.

From the safety and security analysis made in the project we have concluded that based on the WSAN we can provide a set of solutions capable of improving the protection of this infrastructure. From the safety point of view, some remote monitoring processes have been identified to be deployed, and from the security point of view, the use of cameras associated with WSAN can significantly improve the robustness of the solutions for the physical protection of substations and MV/LV power transformer installations.

In the safety area we have defined solutions for the remote active monitoring of: i) substation circuit breaker trip coil status; ii) substation power transformer oil temperature; iii) substation neutral reactance oil temperature; iv) substation neutral resistor coil box temperature; v) MV power line activity in all the three phases; vi) MV/LV power transformer hotspot detection. All the monitored parameters will be visualized at the SCADA system through a special-purpose interface and a graphical user interface. In the security area we will focus on substation perimeter unauthorized intrusion detection by using a combination of PTZ cameras, motion detectors and WSAN. Additionally, video cameras are also deployed and integrated with the WSAN in order to improve the physical protection of the MV/LV power transformer installations.

The requirement for video transmission and the long-distances between power line towers place additional requirements in terms of the communications and processing capabilities of the WSAN nodes. We have defined a sensor mote architecture which can be used in all these applications and that can run a standard operating system like

Linux. Communication interfaces capable of connecting to powerful communication networks like Wi-Fi are also part of this architecture.

The energy consumption of this WSAN node cannot be overlooked. Although the power distribution network carries energy by definition, its use as a WSAN power source presents many challenges. This is especially true in the MV power lines outside the substations, where the voltages are too high (e.g. 15 kV) to be used directly by the WSAN nodes, prompting the use of intelligent energy harvesting techniques.

The paper, in sections 2, 3 and 4, will make a detailed analysis of the application cases indicated for the protection of the electrical energy distribution network. In section 5 we will analyse the interaction with the SCADA system. The hardware and software architectures of the envisaged sensor mote solution will be discussed in section 6 and, finally, some conclusions will be drawn in section 7.

2 Application Scenarios in the Substation

For the protection scenarios implemented in the substation, four of them have the aim of increasing the safety of the infrastructure components, and a fifth has that of increasing security through the deployment of perimeter intrusion detection. The substation safety improvement demonstration scenarios monitor the status of essential components of the substation and the results can be generalized for other components. The target substation is located at S. Sebastião, Setúbal, Portugal, and belongs to the energy distribution infrastructure operated by EDP Distribuição, a company whose primary mission is the distribution of energy in Portugal. The S. Sebastião substation is an important element in the context of the wider regional grid it belongs to. The substation safety and security protection scenarios are described next.

2.1 Circuit Breaker Trip Coil Condition Active Status Monitoring

In this scenario we consider a sensor and actuator for periodically evaluating the operating status of the circuit breaker trip coil element. The trip coil is a fundamental component of the circuit breaker that sometimes breaks down even when under normal use. The trip coil activates the circuit breaker when a 110V DC voltage is applied at its terminals, cutting the energy supply to the power line. It happens that after activating the circuit breaker there is a chance that the coil may be damaged and the circuit breaker will not function properly in the next event.

This scenario aims to check the working status of this component in a pro-active way. A 5V DC voltage will be applied every 60 minutes by an actuator. The magnetic field generated by the coil will be measured by a Hall-effect transistor. In the event of failure, meaning that no magnetic field is detected when a 5V DC voltage is applied, the sensor will report the failure back to the network. The sensor will also test the coil after a trip. In an activation event, the circuit breaker coil is under an 110 V DC voltage for 50 to 150 ms, the Hall-effect sensor sampling rate shall be at least half of the shorter time, i.e. at least 25 ms. Thus, when the activation of the breaker happens, the sensor detects it and can program an extra test shortly after the activation, checking if the circuit break remains functional for the next time it is called into duty.

The sensor would also allow for on demand requests to immediately probe the coil and report back its status. The sensing and controlling of the trip coil test is done

locally. The information sent back to the sink consists only of the test results. In total there are 24 circuit breakers in this substation.

2.2 HV/MV Power Transformer Oil Temperature Active Monitoring

In this scenario we use a wireless temperature sensor for monitoring the oil temperature of the HV/MV power transformers in the substation (see Figure 2). The substation has four power transformers: two 60 KV/15 KV and two 60 KV/30 KV. Due to the value and importance of these elements to the EDP distribution network the scenario will monitor the temperature of all of them. A failure on one of the power transformers affects a series of power lines and all the downstream MV/LV power transformers, meaning thousands of homes and businesses are affected.

The temperature sensor probe is placed in the external side of the metallic oil tank, firmly and thermally attached to the tanks external wall. The sensor probe is isolated from the external environment with thermal foam. The sensor is driven by a 110VDC power source from the substation DC grid. Calibration of the sensor is needed and can be done by locally reading the analogue temperature gauge and the value read by the sensor.

On normal status a measure will be taken every minute, but uploaded to the network only every 15 minutes. When reaching a temperature 20% below the alarm threshold of 95ºC or when a 1ºC or higher increase happens over consecutive readings, the sensor will upload all temperature readings to the network and increase the sampling rate to one reading every one second. The temperature sensor will also allow for on demand temperature reading.

2.3 Neutral Reactance Oil Temperature Active Monitoring

In the third scenario we have a temperature sensor for monitoring the oil temperature of the neutral reactance element (see Figure 2). S. Sebastião substation has two neutral reactances for phase-earth failures limitation and detection on the 15KV power transformers. On a typical failure event this element is under great stress, dissipating 2.6 MW of power for as long as 4 seconds. If the defect persists the reactance may be under this heavy load several more times in a short period, causing it to overheat and raising the risk of failure spreading to other elements in the failing circuit.

Due to the importance of this element in the detection and prevention of failures on the network, and the protection it grants to other equipment (like the power transformer), this scenario will monitor the temperature of all the neutral reactances.

Each reactance tank is similar to a power transformer tank and the methodology used to monitor its temperature is identical to the previous scenario.

2.4 Neutral Resistor Coil Box Temperature Active Monitoring

In scenario four we consider a temperature sensor for monitoring the neutral resistor coils (see Figure 2). The substation has two neutral resistors for phase-earth failures limitation and detection on the 30 KV power transformers. The neutral resistor limits the current in a phase-earth failure to 300 A. On a typical failure event this element is under great stress, dissipating 5.2 MW of power for as long as 4 seconds. If the defect

persists the resistor may be under this heavy load several more times in a short period, causing it to overheat and raising the risk of failure.

Due to the importance of this element in the detection and prevention of failures on the network and the protection it grants to other equipment, this scenario will monitor the temperature of all the neutral resistors.

Each neutral resistor box has 4-5 coils inside. An internal temperature probe shall be placed inside the neutral resistor box near the top where the temperature rises quicker. An external temperature probe is needed for comparison and shall be placed on the outside of the box, in the north facing side and out of direct sun light.

The normal operating temperature should be the outside environment temperature, because at normal operation the voltage is 0V, hence no current is flowing through the neutral resistor and no power (heat) is being dissipated.

On normal status a measurement will be taken every thirty seconds, but uploaded to the network only every 15 minutes. When reaching a temperature 20% above the external temperature or when a 1ºC or more increase happens over consecutive readings the sensor will upload all temperature readings to the network and increase the sampling rate to one reading every second.

Fig. 2. Protected substation components: HV/MV Power Transformer (left), Neutral Reactance (centre) and Neutral Resistor (right)

2.5 Perimeter Unauthorized Intrusion Detection

This scenario is quite different from the previous ones. It aims to maintain the substation premises security against trespassers by detecting their presence and providing a video feed that can be served to a mobile or fixed terminal of security personnel. Movement detectors will be used to infer the area where the intrusion is taking place. Sensors placed at diagonally opposed corners of the substation square, monitoring two orthogonal sides of the fence can detect an intrusion from any direction and measure the distance to the intruder. The sensor can then quickly send an alarm to the network and sharply point its camera to the hot area.

While no intrusion is detected, the movement detectors send keep-alive messages every five seconds. Once an intruder is detected by a movement sensor, an alarm message is sent and one or more cameras are activated and start to transmit the video stream to the control center. The cameras can also be controlled remotely from the control centre. A diagram for this scenario is illustrated in Figure 3.

Fig. 3. Substation perimeter surveillance

3 Application Scenario in the MV Power Line

This scenario aims to monitor the status of an MV power line section, stretching from S. Sebastião substation to several MV/LV power transformers in the vicinity of the substation (less than 5Km). It is therefore possible to know centrally the location of a power line failure.

The power line chosen is a medium voltage 15KV line that feeds a set of urban and suburban MV/LV Power Stations in the city of Setubal. The line topology is a tree shape with several branch leaves, the leaves being the MV/LV power transformers (see Figure 1).

The physical measurement to be taken is the electrical current flowing through the line; a current transformer shall be used to measure its value and to derive a parasitic power source for the wireless sensor, eliminating the need for batteries on the sensor and at the same time posing no power constrains on the wireless protocols.

Each tower carries three 15 KV power lines (3 phases) in parallel, and each one needs its own sensor. Therefore, three current sensors will be placed in the lines in each tower. We also need three router nodes for bridging buried segments along the line. These router nodes shall be installed in the outside of MV/LV power transformers located between towers. The router shall be placed in high ground or at the end of a pole if more elevation is needed, to achieve line-of-sight to the next node site. The maximum distance between towers is 723 meters. The current sensor samples the current on the line every second.

4 Application Scenario in the MV/LV Power Transformer

In this scenario we use the wireless communications link built in the previous scenario to upload a video/image feed of the MV/LV power transformer house interior to the network. At the same time an infrared thermo sensor attached to the

camera will sweep the power transformer critical elements, such as the main switch board, for hotspots. The detection of a hotspot will trigger an alarm on the network.

This scenario also includes an actuator. The remote user shall be able to turn on the lights on the MV/LV power transformer house. Thus, the camera shall be night and day capable. The user can get a better color video stream, even at night, improving on the black-and-white stream available in night mode. This feature improves the remote MV/LV power transformer physical security.

While no intrusion or hotspot is detected by the infrared sensor, the latter sends a keep-alive message every five seconds. Once an event is detected by the infrared sensor, the latter starts sending alarms every second and the camera is activated, transmitting the video stream to the control center. The lights can also be controlled remotely from the control center.

5 Interaction with the SCADA System

The substation devices are nowadays monitored and controlled through the Supervisory Control and Data Acquisition (SCADA) system. The WSAN shall be integrated with this existing system in order to provide a unified power distribution infrastructure interface to the human operators, which also optimizes the hardware/software resources and learning effort.

The SCADA protocol architecture is generic enough to be operated in an Internet Protocol (IP) environment on top of different network technologies, such as Ethernet and SONET/SDH. However, the WSAN presents a specific networking environment where the energy and bandwidth optimization requirements are often incompatible with the request/response philosophy behind SCADA. For example, in some applications that involve the timely detection of critical events, it is more efficient to rely on the remote sensing device to take the initiative to send an alarm message when the event happens, rather than allowing the supervisory system to issue periodical queries with a very high frequency. These differences lead to the need of translating SCADA procedures to WSAN procedures and vice versa, which is the purpose of the SCADA/WSAN gateway. The gateway consists of a PC equipped with an Ethernet interface and WSAN radio interface; the Ethernet is connected to the SCADA supervisory system and the radio interface to the WSAN.

From the point of view of the SCADA system, the SCADA/WSAN gateway behaves as a database that responds to its queries about the status of WSAN devices. The application interface for these queries is based on Web Services [1], with the gateway implementing the server side. The use of the Web Service interface performs an adequate mapping of the SCADA data access mechanisms, which follows a client/server paradigm.

From the point of view of the WSAN, the SCADA/WSAN gateway takes the role of the sink node, which makes it the main destination of sensor data and the main source of queries and configuration/command requests. It also includes a database of sensing and management data, which serves as a buffer between the SCADA system and the WSAN.

6 Hardware and Software Architecture

The overall hardware architecture is depicted in Figure 4 and comprises three main components: SCADA supervisory station, SCADA/WSAN gateway and WSAN nodes. The latter has the capability to self-organize into a multi-hop network.

The SCADA station is PC based and will reside inside the Substation's main building. The SCADA/WSAN gateway fulfills also the role of a WSAN sink node, and hence must be equipped with a WSAN radio module able to communicate with the WSAN sensor and actuator nodes. The SCADA/WSAN gateway resides also at the Substation's main building, and hence will have access to 220 V AC line power. The most important critical requirements are related with the WSAN nodes, whose architecture is discussed next.

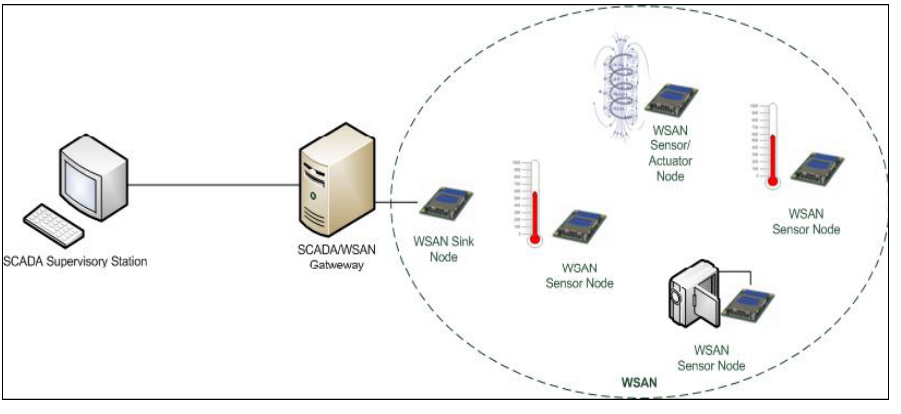


Fig. 4. High-level hardware architecture of the WSAN based system

The video surveillance service is incompatible with a low rate technology like IEEE 802.15.4 [2]. It demands the use of a broadband wireless technology such as IEEE 802.11 [3]. The latter also makes sense given the expected maximum distance between sensors. The ensemble of requirements led to the choice of the Silex SX-560 Intelligent Programmable WLAN Module [4] as the platform for the WSAN node.

The basic architecture of the WSAN node is depicted in Figure 5. The SX-560 core is common to all WSAN nodes. The PCB designed at INOV includes a common voltage converter able to generate 3.3 V DC to feed the Silex and 5 V DC to feed the USB interface (considered a part of the Sensor Interface Unit) based on an input of 6-20 V DC. The differences between the WSAN nodes concern the Energy Unit and Sensor Interface Unit, which depend on the deployment spot and attached sensor, respectively.

Three different energy units exist, which allow operation at the three different locations within the EDP Distribuição network:

- **Substation WSAN node:** the energy unit will use the 220 V AC power line, performing the conversion to a voltage in the range 6-20 V DC.

- **MV/LV power transformer WSAN node:** the energy unit will use the 220 V AC power line, performing the conversion to a voltage in the range 6-20 V DC.
- **15 KV power line towers WSAN node:** the energy unit is able to harvest energy from the 15 KV power line current, being able to generate a voltage in the range 6-20 V DC and a current up to 500 mA.

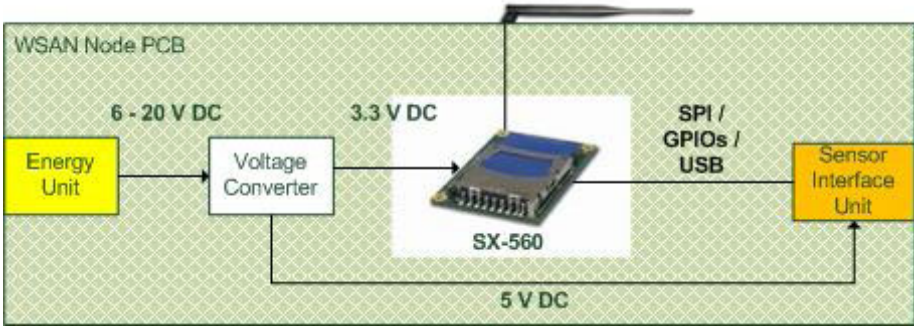


Fig. 5. Base architecture of WSAN node

The software architecture of the WSAN node is depicted in Figure 6. The selected Operating System is LINUX, which is supported by the Silex SX-560 module. Among the advantages presented by LINUX is the intrinsic support of the dynamic code update (DCU) function, avoiding the development of specific DCU software. It should be noted that the DCU functionality is very important in the case of the power line and MV/LV power station monitoring scenario, where sensor nodes can be located far away from the substation, preventing the update of the WSAN node software without significant costs.

The main software modules of the WSAN node are the following:

- **WSAN Sensor/Actuator Application Logic:** This software block implements the application logic of the WSAN node, which consists of three main functions:
  - To receive and process commands from the SCADA/WSAN gateway.
  - To retrieve sensor data from sensors and deliver it to the SCADA/WSAN gateway.
  - To manage the configuration MIB based on the commands received from the SCADA/WSAN gateway and the status of the WSAN node.
- **Dependable Protocol Stack:** The limited capabilities of the WSAN nodes demand an optimized protocol stack able to find the best compromise between energy-efficiency, communications reliability and communications performance. The Dependable Protocol Stack spans the MAC, Routing and Transport protocols. The transport layer consists of a secured version of the Distributed Transport for Sensor Networks (DTSN) protocol developed by INOV [5]. The protocol provides message delivery guarantees to applications, optimizing retransmissions based on intermediate node caching. DTSN runs on top of a secure routing

protocol. The latter will consist of a secured version of DSDV [6][7], optimized for WSAN applications (e.g. advertisement broadcasts limited to the sink node, and multipath forwarding for load and energy balancing and improved security). IEEE 802.11 is used for PHY and MAC layers.

- **Sensor/Actuator Device Driver:** Each different kind of sensor/actuator must be accessed in a different way and generates data and/or status of a specific type. This software block offers an abstract interface to the sensor/actuator hardware, allowing the design of the WSAN Application Logic to be as independent as possible from the intricacies of the sensor/actuator hardware.
- **Management Information Base (MIB):** This software block keeps the configuration parameters of the WSAN nodes, which can be changed by the SCADA/WSAN gateway.
- **Security Functions:** The WSAN constitutes a vulnerable part of the CIP System from the security point of view. Confidentiality, Authentication, Integrity and Non-repudiation solutions exist, which are part of the deployed WSAN.

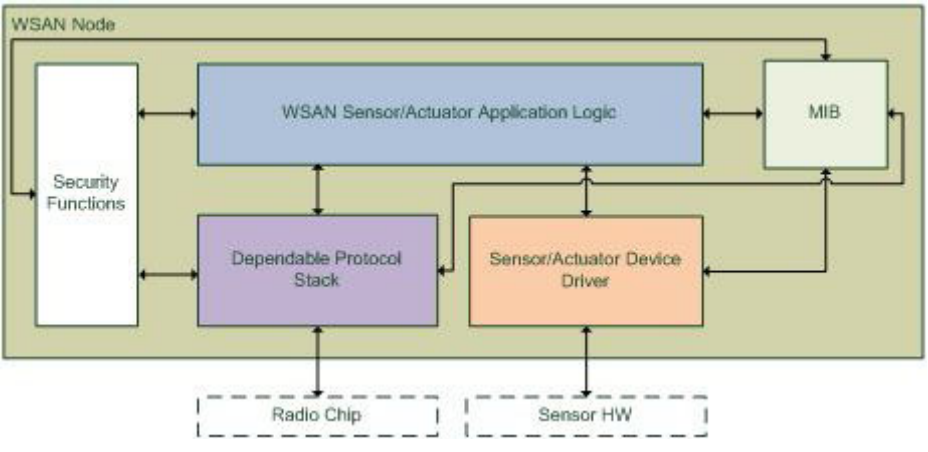


Fig. 6. Software architecture of the WSAN node

7 Conclusion

The electrical energy distribution constitutes a critical infrastructure in contemporary industrially developed societies, which requires protection regarding safety and security threats. The fact that this infrastructure is geographically spread across huge areas puts difficult technological challenges to real-time prevention, detection and precise localization of anomalies. This paper presented a WSAN-based solution to protect the core elements of an electrical energy distribution infrastructure at three interconnected locations: substation, MV power-lines and MV/LV power transformer. The presented WSAN system is under development as part of the FP7 WSAN4CIP project.

This paper has discussed the planned architecture and high-level implementation solutions for the WSAN system, including a description of the protected equipments, the hardware and software architecture. A pilot system will be demonstrated in a subset of the Portuguese energy distribution infrastructure operated by EDP Distribuição.

Acknowledgment. The research leading to these results has received funding from the European Community's Seventh Framework Programme under grant agreement no. 225186. Consortium: Eurescom, IHP Microelectronics, NEC Europe, INOV, EDP Distribuição, Budapest University of Technology and Economics, INRIA, Lulea University of Technology, Sirrix, Tecnatom, University of Malaga and FWA.

References

1. W3C, Web Services Architecture, W3C Working Group Note 11 (February 2004), http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/
2. IEEE Std. 802.15.4, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks, LR-WPANs (2003)
3. IEEE Std. 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (1999)
4. Silex Technology, SX-560 Intelligent Programmable WLAN Module, SX-5602009EN (2009), http://www.silexeurope.com/media/datasheets/SX-560-ds_en_0902.pdf
5. Rocha, F., Grilo, A., Pereira, P., Nunes, M., Casaca, A.: Performance Evaluation of DTSN in Wireless Sensor Networks. In: Cerdà-Alabern, L. (ed.) EuroNGI/EuroFGI 2008. LNCS, vol. 5122, pp. 1–9. Springer, Heidelberg (2008)
6. Perkins, C., Bhagwat, P.: Highly Destination-Sequenced Dynamic Distance Vector Routing (DSDV) for Mobile Computers. In: Proc. of the ACM SIGCOMM 1994, London, UK, pp. 234–244 (1994)
7. Grilo, A., Piotrowski, K., Langendoerfer, P., Casaca, A.: A Wireless Sensor Network Architecture for Homeland Security Application. In: Ruiz, P.M., Garcia-Luna-Aceves, J.J. (eds.) ADHOC-NOW 2009. LNCS, vol. 5793, pp. 397–402. Springer, Heidelberg (2009)

Risk Modelling the Transition of SCADA System to IPv6

Suriadi Suriadi, Alan Tickle, Ejaz Ahmed, Jason Smith, and Hasmukh Morarji

Queensland University of Technology, GPO Box 2434,
Brisbane, QLD 4001, Australia
s.suriadi@qut.edu.au, ab.tickle@qut.edu.au, e.ahmed@qut.edu.au,
j4.smith@qut.edu.au, h.morarji@qut.edu.au

Abstract. SCADA is one of a set of manufacturing-and-control systems that are used to monitor and control critical infrastructure. Such systems extensively utilise communications network protocols such as TCP/IP to interconnect a diverse array of components. A major forthcoming change within TCP/IP is the adoption of the IPv6 protocol and inevitably this change will affect SCADA systems. However IPv6 introduces its own set of vulnerabilities. Hence, given the scale and complexity of current SCADA systems, there is a need for organisations to be able to model and review the risks emanating from the propagation of identifiable vulnerabilities in IPv6 prior to actual operational deployment. This work shows how the required tools can be constructed by complementing the Information Security Management (ISM) risk modelling tool with the formal technique of Coloured Petri Nets (CPN). The results of the application of the tools in a case study confirm the utility of the approach.

Keywords: SCADA, IPv6, Risk Modelling, Formal Methods, Coloured Petri Nets.

1 Introduction

SCADA is one of a set of manufacturing and control systems used to monitor and control critical infrastructure particularly in utilities such as energy and water [1]. One of the key enabling technologies underpinning such systems is the TCP/IP suite of network protocols which facilitates the interconnection of a diverse array of components such as those found in manufacturing and control systems. Within the Internet community, the impending change from the current version of the IP protocol (IPv4) to the IPv6 implementation offers a number of potential benefits to corporate networks and the Internet at large [2, 3], including SCADA systems. For example, the significant increase in the number of public IP addresses and the auto address configuration feature of IPv6 make it possible to deploy hundreds, if not thousands, of SCADA components, such as smart meters, in a relatively efficient manner. Furthermore, the anycast addressing feature of IPv6 may also increase the reliability of a SCADA system.

However, any new technology comes with its own inherent vulnerabilities. For IPv6 this is true both in its ultimate deployment as well as during the transition from

J. Berleur et al. (Eds.): HCC9/CIP 2010, IFIP AICT 328, pp. 384–395, 2010.

IPv4 [3]. Currently, the opportunities for organisations to examine the behaviour of their SCADA systems under IPv6 are limited to test systems [1] which makes it difficult to predict how the operational SCADA over IPv6 systems will behave.

This paper discusses some of the results of a project to apply a set of tools that could be used to perform a risk analysis of operational SCADA systems. There are two processes involved: (1) a study of how IPv6 vulnerabilities can manifest themselves as threats to a SCADA system running over IPv6, and (2) an analysis of the level of risks that the identified threats pose to the system.

The main contribution of this paper is the proposal of an approach to combine a well-known formal method of Coloured Petri Nets (CPN) [4] with a risk analysis tool, called the Information Security Management (ISM) Tool [5,13,15], in executing the two processes identified above. A formal method approach is used because the underlying mathematical nature of formal modelling and analysis enables a precise system modelling and potentially complete threat detection, depending on the validity and the details of the model of the system. Furthermore, it is also a cheaper and less time consuming in comparison to deploying a real SCADA system.

Once the threats of IPv6 vulnerabilities to a SCADA system are identified using CPN, we can then feed these threats into the ISM Tool for risk analysis. Knowing threats alone is not sufficient as, ultimately, the goal of threats detection and identification is to allow the management to allocate resources proportionately to the risk that these threats carry. Thus, a risk analysis is needed. The ISM Tool is chosen as a risk analysis tool mainly because of its flexibility: it can be used as threats documentation tool as well as a risk model generation tool which facilitates straightforward risk analysis. It also provides a simple graphical interface which makes it easy to use. Furthermore, it has a long and solid development history of over 15 years [15-17].

This paper starts with an overview of the vulnerabilities of IPv6 (Section 2) followed by an explanation of how we can detect potential threats to SCADA systems resulting from IPv6 vulnerabilities using the formal technique of CPN (Section 3). This is followed by a description of the ISM Tool for analysing risks of SCADA systems deployed over IPv6 networks (Section 4). The result of a case study of using the ISM Tool is detailed in Section 5, followed by a conclusion in Section 6.

2 Known IPv6 Vulnerabilities

While IPv6 offers a number of significant improvements over IPv4, it also introduces a number of new vulnerabilities [6]. These vulnerabilities can be broadly categorised into two main groups. The first group comprises vulnerabilities that are intrinsic to the IPv6 itself. The second group of IPv6 vulnerabilities arises from the IPv4 to IPv6 transition where the two protocols stacks must co-exist.

Of the vulnerabilities that are intrinsic to IPv6, there are three that potentially are of greatest concern in SCADA networks. The first of these vulnerabilities arises from the Neighbour Discovery (ND) and Address Auto-configuration mechanism (RFC 2461 [7] and RFC 3756 [8]). The second key vulnerability arises from the adoption of the Mobile IPv6 extensions which were an optional add-on feature for IPv4 networks but which are an implicit feature for IPv6 networks (RFC 3775[9]). The third important

vulnerability arises from IPv6 extension headers. In addition to the vulnerabilities that are intrinsic to IPv6, there are also vulnerabilities that arise as a result of IPv4 and IPv6 co-existence (RFC 4942 [10]). For the purposes of illustration, in this paper we limit our discussion to the vulnerabilities arising from the IPv4 to IPv6 transition and the Neighbour Discovery (ND) mechanism.

Within IPv6, the role of the Neighbour Discovery (ND) mechanism is to create and maintain the mapping between the IP-layer address and the link-layer address. This is achieved through a process of Neighbour Solicitation (NS) and Neighbour Advertisement (NA). However this same process offers a vector through which an attacker is able to compromise system integrity by redirecting traffic away from the intended recipient. This attack could, for example, be initiated by injecting spoofed NA and/or NS messages either remotely or locally thereby corrupting the link between IP address and the corresponding link-layer address (see RFC 3756 and RFC 3964 for details [8, 11]). While such an attack is similar to the ARP spoofing attack within IPv4, there are few known mitigation techniques for the NA spoofing attack [12] particularly since, in IPv6, such an attack can be launched remotely (see RFC 3964 [11] for details).

An alternative vector of attack and one that could potentially arise in the IPv4-IPv6 transition process is to exploit the 6to4 tunnelling process. An attacker can spoof the source address on the inner IPv6 packet to a victim's address (for example, a 6to4 relay router). Without proper security checks, the attacker's IPv4 address (which is contained in the outer IPv4 packet) is discarded when the outer IPv4 header is de-capsulated. The net effect is (1) to make the attackers' actual IP address untraceable, and (2) to 'reflect' reply packets to the victim's IP address thereby creating a (distributed) denial of service attack as described in RFC 3964 [11]. As will be discussed, the key purpose of the work undertaken is to demonstrate how to detect threats and analyse their risks should the vulnerabilities described above be exploited in a control system environment.

3 Detection and Identification of IPv6 Threats to SCADA Systems

In Section 2, we described the two selected IPv6 vulnerabilities viz. IPv6 Neighbour Discovery (ND) vulnerabilities and IPv4-to-IPv6 transition mechanism vulnerabilities. However, in order to use the ISM risk modelling tool to perform a risk analysis of a SCADA system running on IPv6 network, the threats (as well as their propagations and consequences) resulting from these IPv6 vulnerabilities need to be clearly identified. Such an understanding is crucial because *risk* by definition is a function of both the probability and the consequences of identified threats to the system examined [13]. Therefore, the ability to detect and thus identify these threats is a precursor to risk analysis.

There are several techniques that can be used to study how IPv6 vulnerabilities can manifest themselves as threats to a SCADA system. These include:

1. use the presence of IPv6 in current COTS (commercial-off-the-shelf) network products to deploy a prototype SCADA over an working IPv6 system thereby allowing threats resulting from IPv6 vulnerabilities to be identified directly,

2. use formal analysis techniques to model a SCADA over IPv6 system and identify the vulnerabilities, and
3. use informal analysis of how IPv6 vulnerabilities can lead to threats to SCADA over IPv6 by studying the existing literature [6, 14] and drawing upon past experience.

Obviously, the first approach provides the most authoritative detection and identification of threats. However, at the moment the absence of an accessible real-world deployment of SCADA over IPv6 renders the option somewhat problematic. It would also be costly and time consuming.

On the other hand, the last approach (informal analysis) is comparatively cheap and not as time consuming. Provided there exists a detailed documentation of a SCADA system and IPv6 technologies (and their vulnerabilities), it is feasible to predict how a SCADA system will react when vulnerabilities are exploited. In fact, this is the approach that has been used in many of existing publications of security analysis of IPv6 such as RFC 3756 and RFC 3964 [8, 11]. However, while informal analysis is less costly and less time-consuming than using a 'live system', such an approach is not exhaustive. It also suffers from having too many variables to consider thereby rendering the approach incomplete and prone to errors.

The second approach (using formal methods) is arguably the best approach of the three techniques. It is comparatively cheaper and less time consuming than deploying a real SCADA system and the mathematical nature of formal modelling and analysis delivers a precise system modelling and potentially complete threat analysis depending on the validity and the details of the model of the system.

In this paper, we use both the formal analysis (Coloured Petri Nets (CPN) [4] along with the supported simulation and state space analysis) and informal analysis. In particular we show how CPN can be used to detect and identity threats manifested from IPv6 vulnerabilities and how the identified threats can then be documented and used as inputs to the ISM Tool for risk analysis. Alternatively, when a threat analysis has been performed informally, the results can be verified using the formal methods just mentioned in the future.

In the remainder of this section, we explain the result of our formal and informal analysis on how IPv6 vulnerabilities can manifest themselves as threats to a SCADA system over IPv6. We present the resulting threats from the three IPv6 vulnerabilities explained in Section 2: (1) NA/NS spoofing vulnerability (RFC 3756 [8]), (2) remote injection of ND messages vulnerability (RFC 3964 [11]) , and (3) reflection of traffic to 6to4 relay vulnerability (RFC 3964 [11]).

We have developed a proof-of-concept CPN model to detect threats resulting from the first vulnerability. The threats from the other two vulnerabilities have been informally analysed. From our analysis, we have managed to detect how the IPv6 vulnerabilities studied can become threats to SCADA over IPv6, and how those threats can propagate concluding in the SCADA system reaching a potentially undesirable state. The results of our formal and informal analysis are summarized in Table 1 and Table 2, and are fed into the ISM Tool for risk analysis (details are in the remainder of this paper).

3.1 Threats Resulting from NA/NS Spoofing Vulnerability

The immediate threat posed by NA/NS spoofing is that a legitimate node (such as a Master controller node – see Fig. 1) obtains an incorrect link layer address of its neighbours. This situation may lead to control messages being delivered to an incorrect RTU2 resulting in RTU2 executing the control messages intended for RTU1 and hence contributing to system instability and potential failure.

A brief description of the proof-of-concept CPN model for NA spoofing vulnerability, and how the model can tell us the threats manifested from this vulnerability, is provided. A simple SCADA system is studied (see Fig. 1). The `Industrial Control Network' part of the overall SCADA (see top right corner of Fig. 1) has been modelled using CPN. This network consists of one master controller with two RTUs, along with other supporting equipment.

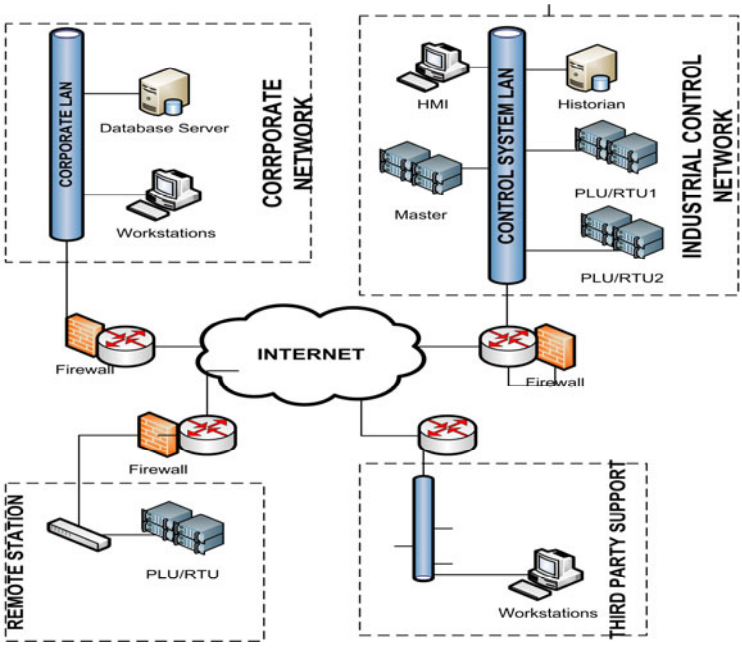


Fig. 1. A Simple SCADA system. The 'Industrial Control Network' is modelled using CPN.

Fig. 2 shows a snippet of the industrial control network modelled in CPN. It depicts a subset of RTU2 operations. Firstly, we model the sending of a Neighbour Advertisement (NA) message (see the `Sending NA' transition inside a rectangle box on the top left corner of Fig. 2). We also model the receiving of an NA message (and the updating of the Neighbour Cache Table) at each node, and the operations that RTU2 execute when a control message is received (see the lower part of Fig. 2).

As this is a proof-of-concept model, we abstract the NA packet and the control message packet to filter out information that is not relevant for our purpose. Similarly, we also do not model how RTU2 exactly processes a received control message;

rather, we are more interested in how RTU2 can reach an unstable/undesirable state. In the model, we assume that RTU2 has almost reached its `maximum capacity' (in a real world system, imagine RTU2 as a controller of an actuator, such as a pump, that pumps oil into an almost-full tank). Using the above analogy, we model RTU2 such that it can only handle additional 3 `pump' control messages before the tank is full.

Overall, we model the system such that RTU2 will send an NA message to be processed by both RTU1 and Master controller. After a successful processing of the NA messages by all nodes, the Master controller sends 5 control messages to RTU1.

Through the simulation of the CPN model, we have verified that the modelled SCADA system behaves correctly in the generation and processing of both NA and control messages.

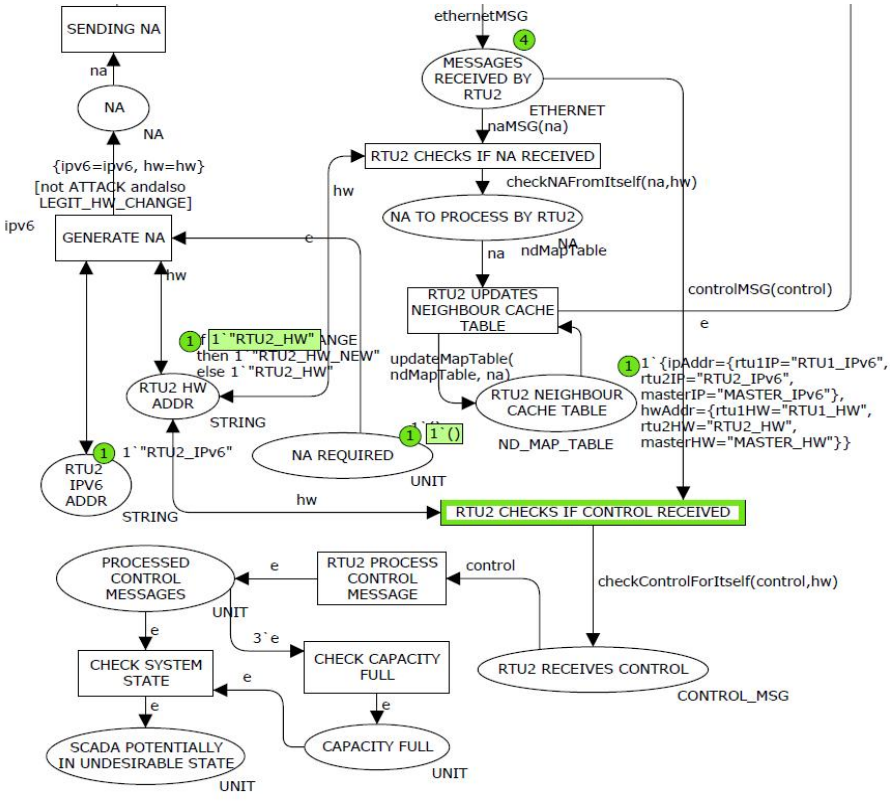


Fig. 2. A CPN Model of select RTU2 operations

The next step is to model the exploitation of the spoofed NA vulnerability. We do so by adding an attacker model as shown in Fig. 3. We model the attacker to inject a spoofed NA message claiming that the corresponding hardware address of an IPv6 address (which actually belongs to RTU1) is the attacker's hardware address. Then, we model the attacker modifying any control messages it receives so that they are

directed to the low-capacity RTU2 with the aim of causing instability in the system controlled by RTU2.

Leaving the rest of the model intact, we then run a simulation to study what happens to the SCADA system when the attacker injects the spoofed NA message followed by the Master controller sending a series of 5 control messages to RTU1. From the simulation of the model, we note that the control message is mistakenly delivered to RTU2 who then executes the control messages. As a result, the SCADA system may reach a potentially undesirable state (see Table 1 and 2 for summary).

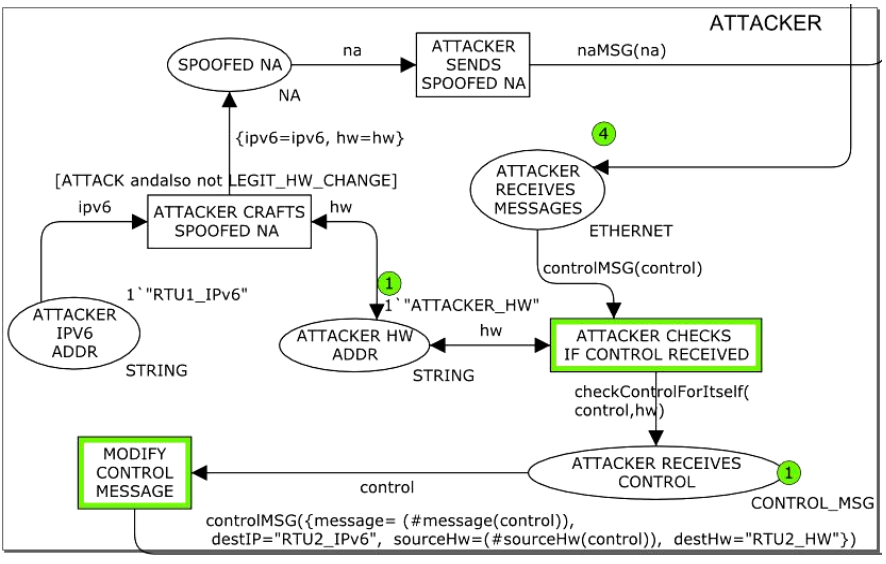


Fig. 3. A CPN Model Depicting an Attacker Exploiting IPv6 Spoofed NA Vulnerability

3.2 Threats Resulting from Remote Injection of ND Messages Vulnerability

The use of tunnelling mechanism could allow a compromised external node (such as a third-party support workstation) to inject a spoofed RA (or NA) messages. This may result in a successful exploitation of ND vulnerabilities, such as the modification of default router information. The consequence of such an attack is that control messages sent to a remote station RTU can be modified by an attacker, resulting in incorrect control messages received by the remote RTU. This may result to an unstable SCADA system at the remote location which could lead to the system being in an undesirable state (see Table 1 and 2).

3.3 Threats Resulting from Reflection of Traffic to 6to4 Relay Vulnerability

The use of tunnelling mechanism could allow a compromised external node (such as a third-party support workstation) to reflect traffic to a 6to4 relay router (such as the one at the Industrial Network). This may result in the router being overwhelmed with

too many packets causing legitimate control messages to be dropped, leading to instability and an undesirable state (see Table 1 and 2).

4 The ISM Risk Modelling Tool

In Section 3, we have described how we can identify threats to a SCADA system based on known IPv6 vulnerabilities. However, at least from a management point of view, the ultimate goal from this exercise is to be able to proportionately allocate resources to mitigate the identified threats according to their risks. To this end, we need a mechanism to study how 'risky' the identified threats are.

The ISM Risk Modelling tool [13, 15] has been developed for this purpose. This tool is developed based on the *information security management and modelling* approach proposed by Longley et al and has been developed over more than 15 years [15-17]. This tool can be used for several purposes, including: (1) as a tool to aid threat documentation, (2) as a risk modelling tool: by reading the threat documentation that has been fed into the ISM Tool, and (3) as a tool to analyse the effectiveness of threat countermeasures.

Threat Documentation: Depending on the system being studied, organizations may already have such threat documentation, or, threats can be identified and documented using the approach explained in Section 3. The ISM Tool allows these threats to be properly documented in a form that can be readily used for risk analysis. In Section 5, we provide an example of how threat documentation and threat propagation are documented using ISM Tool.

Risk Simulation and Analysis: Once threats are documented into the ISM Tool, they can be automatically scanned to generate a risk simulation by creating a threat network diagram [15] which shows both the risk measurement of a threat and the propagation of threat. The risk measurement is derived based on the consequences of a threat documented (catastrophic, major, moderate, minor, or insignificant) as well as the probability of the threat happening [13]. In Section 5, we demonstrate how we can derive a risk simulation on a SCADA system over IPv6 network using the ISM Tool.

Threat Countermeasures Analysis: The ISM tool also captures the set of mitigation techniques that have been (or planned to be) applied. Similar to threat documentation, such information may already be well-documented in an organization, or, a further study (using methods described in Section 3) is needed to verify the effectiveness of a countermeasure technique. An analysis of the effectiveness of countermeasure techniques to mitigate IPv6 threats to SCADA systems is part of the future work.

5 A Case Study Using the ISM Tool

In this section, we demonstrate how we can use the ISM Tool to (1) document detected threats and threats propagation, and (2) generate a simulation of risk which shows the risk level of documented threats.

The risk simulation can be performed in two styles: 'forward' and 'backward'. In the 'forward' style, a user chooses the starting threats that are assumed to have happened, and then either (a) uses the tool to show the ensuing chains of threats (as well as the risk level for the ensuing threats), or, (b) chooses the causal threats so that ISM Tool can show how the starting threats may lead to the chosen causal threats as well as the risk level associated with the starting threats, the propagated threats, and the causal threats. In the 'backward' style, a user simply chooses the causal threat. From there, the ISM Tool will do a 'backward' analysis to show the threats that may lead to the chosen causal threat [15], their propagation, and their risk levels.

5.1 Threat Documentation Using ISM Tool

To document threats, some key information is required, including (1) the entities of the system (such as platforms, hardware, softwares, networks, information assets, and so on) which may become the victims of some threats, (2) the relationships between those entities (for example, a master controller and an RTU may have a communication relationship), and (3) the detected threats and their propagations.

The first two pieces of information (entities involved and their relationships) can be easily documented based on the simple SCADA system shown in Fig. 1. Furthermore, information about the detected threats and their propagations is obtained from the results of both the formal and informal analysis of IPv6 threat detection explained in Section 3. These results are summarized in Table 1 and Table 2.

5.2 Risk Simulation and Analysis Using ISM Tool

Once the threats are documented, it is simple to obtain the risk simulation. Fig. 4 shows a threat network generated using a `forward' risk simulation whereby we determine the set of initiating threats ('Incorrect Link Address', 'Packets Reflected to IPv6 Relay Router', and 'Local Nodes Subjected to Remote ND Attacks') and use the ISM Tool to identify how the SCADA system can reach an undesirable state. The colour of each of the node in Fig. 4 is used to convey the risk level of each of the threat (green colour denotes the initiating threats, grey colour denotes a low risk level, yellow colour denotes a high risk level, and red colour denotes an extreme risk level). The ISM Tool can also generate a risk measurement report (see Table 3) which summarizes the resulting threats (including the initiative threats, the intermediary threats, and the resulting threats) and their risk level. From Fig. 4 and Table 3, we can conclude that there is an extreme risk of a seemingly-minor threat (e.g. a node obtains incorrect link layer address) leading to a major threat whereby a SCADA system becomes unstable. A `backward' style analysis can also be performed to determine the threats that could cause the SCADA system reach an undesirable state.

Table 1. A Summary of Detected Threat Entities

Threat Name	Threat Entity	Consequences
Incorrect Link Address	• RTU/Master/HMI/Historian at Industrial Control Network (ICN) • RTU at Remote Station	Minor
Internal Control Messages Communication Errors	• Communication between Master Controller and RTU1/RTU2 at ICN	Moderate
HMI Provides Inaccurate Feedback	• HMI at ICN	Moderate
Incorrect Control Message Sent	• Master Controller at ICN	Moderate
Packets Reflected to IPv6 Relay Router	• Router/Firewall at ICN	Moderate
IPv6 Hosts Receive Too Many Illegitimate Packets	• Industrial Control Network Remote Station	Moderate
Valid Control Messages Dropped	• Industrial Control Network • Remote Station	Moderate
Local Nodes Subjected to Remote ND Attacks	• RTU1/RTU2/Master at ICN	Moderate

Table 2. A Summary Threat Propagation

Incident Threat Entity	Target Threat Entity
Incorrect Link Address	Internal Messages Communication Errors
Incorrect Link Address	Internet Messages Communication Errors
Internal Messages Communication Errors	HMI Provides Inaccurate Feedback
Internet Messages Communication Errors	HMI Provides Inaccurate Feedback
HMI Provides Inaccurate Feedback	Incorrect Control Message Sent
Poorly Secured Host	Compromised Host
Compromised Host	Incorrect Control Message Sent
Compromised Host	Packets Reflected to IPv6 Relay Router
Packets Reflected to IPv6 Relay Router	Valid Control Messages Dropped
Valid Control Messages Dropped	HMI Provides Inaccurate Feedback
Local Nodes Subjected to Remote ND Attacks	Incorrect Control Message Sent
Incorrect Control Message Sent	SCADA Reaches Undesirable State

Table 3. An Example of Risk Measurement Summary for Fig. 4

Threat	Risk
Incorrect Link Address	High
Internal Control Messages Communication Errors	Extreme
Internet Control Messages Communication Errors	Extreme
Local Nodes Subjected to Remote ND Attacks	Extreme
Packets Reflected to IPv6 Relay Router	Extreme
HMI Provides Inaccurate Feedback	Extreme
Valid Control Messages Dropped	Extreme
Incorrect Control Message Sent	Extreme
SCADA Reaches Undesirable State	Extreme

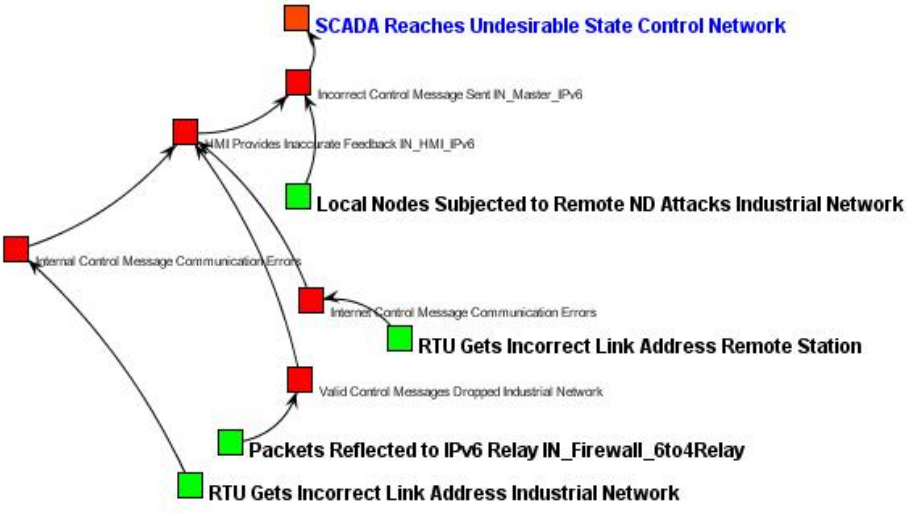


Fig. 4. Risk Simulation using the ISM Tool – 'forward' risk simulation

6 Conclusion

We have shown tools and techniques that can be used to perform a risk analysis of a SCADA system running on IPv6 network. In particular, we have shown how a formal technique, such as Coloured Petri Net, can complement the use of ISM Tool: as a technique to detect and identify threats manifested from IPv6 vulnerabilities which are subsequently fed to the ISM tool for risk analysis. We have also shown how the ISM Tool can be used to simulate and analyse risks in a SCADA system. An interesting future work will be to develop a detailed CPN model of a representative SCADA system running on IPv6 to allow threats manifested from IPv6 vulnerabilities to be comprehensively detected and documented.

Acknowledgment. This work was supported by the Australia-India Strategic Research Fund 2008-2011.

References

1. Wiles, J., Drake, P., Claypoole, T.: Techno Security's Guide to Securing SCADA: A Comprehensive Handbook on Protecting The Critical Infrastructure. Syngress, Rockland, Mass. (2007)
2. United States Government Accountability Office, Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks (2005)
3. United States Department of Commerce, The Evolving Internet: A Technical and Economic Assessment of Internet Protocol, Version 6, IPv6 (2006)
4. Jensen, K.: A Brief Introduction to Coloured Petri Nets. In: Brinksma, E. (ed.) TACAS 1997. LNCS, vol. 1217, pp. 203–208. Springer, Heidelberg (1997)

5. Branagan, M., Dawson, R., Longley, D.: User Documentation - ISM (Information Security Management) Risk Management Tool (2006)
6. Leeuwen, B.V.: Impacts of IPv6 on Infrastructure Control Systems. Sandia Report SAND2007-0383P. Sandia National Laboratories (2007), http://www.sandia.gov/scada/documents/VanLeeuwen-2007-0383P.pdf
7. Narten, T., Nordmark, E., Simpson, W.: Neighbor: Discovery for IPVersion 6 (IPv6), RFC 2461. The Internet Society (1998), http://www.ietf.org/rfc/rfc2461.txt
8. Nikander, P., Kempf, J., Nordmark, E.: IPv6 Neighbor Discovery (ND) Trust Models and Threats, RFC 3756. The Internet Society (2004), http://www.ietf.org/rfc/rfc2461.txt
9. Johnson, D., Perkins, C., Arkko, J.: Mobility Support in IPv6. RFC 3775. The Internet Society (2004), http://www.ietf.org/rfc/rfc3775.txt
10. Davies, E., Krishnan, S., Savola, P.: IPv6 Transition/Co-existence Security Considerations, RFC 4942. The Internet Society (2007), http://www.ietf.org/rfc/rfc4942.txt
11. Savola, P., Patel, C.: Security Considerations for 6to4, RFC 3964, Informational (2004)
12. Convery, S., Miller, D.: IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation. Cisco Systems White Paper (2004)
13. Dawson, R.E.: Secure communications for critical infrastructure control systems. Queensland University of Technology, Brisbane, QLD (2008)
14. Stouffer, K., Falco, J., Kent, K.: Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. In: Recommendations of the National Institute of Standards and Technology (2006)
15. Branagan, M., Dawson, R., Longley, D.: Security Risk Analysis for Complex Systems. In: Proceedings of the Information Security for South Africa 2006 from Insight to Foresight Conference, ISSA, Pretoria, South Africa (2006)
16. Caelli, W.J., Longley, D., Tickle, A.B.: A Methodology for Describing Information and Physical Security Architectures. In: Eight International Conference on Information Security (SEC) 1992. IFIP Transactions, Singapore (1992)
17. Kwok, L.F., Longley, D.: Information security management and modeling. Information Management and Computer Security 7(1), 30–39 (1999)

Author Index