Ten National Cyber Security Strategies: A Comparison

H.A.M. Luiijf[1], Kim Besseling[1], Maartje Spoelstra[1], and Patrick de Graaf[2]

[1] TNO, P.O. Box 96864, 2509 JG The Hague, The Netherlands
[2] Capgemini Netherlands BV, P.O. Box 2575, 3500 GN Utrecht, The Netherlands
{eric.luiijf,kim.vanbuul}@tno.nl, maartje.spoelstra@gmail.com, ap.degraaf@ziggo.nl

Abstract. A number of nations developed and published a national cyber security strategy (NCSS). Most of them were published in the period 2009 - 2011. Despite the fact that each of these NCSS intends to address the cyber security threat, large differences exist between the NCSS approaches. This paper analyses and compares the NCSS of Australia, Canada, Czech Republic, France, Germany, Japan, The Netherlands, New Zealand, the United Kingdom, and the United States. Thirteen observations lead to a set of conclusions which nations with an NCSS and developers of future NCSS may use to their advantage.

Keywords: cyber security, strategy, policy, critical infrastructure, national security.

1 Introduction

A number of nations have developed and published a National Cyber Security Strategy (NCSS) in the period 2009–2011. During the development of the Dutch NCSS, a short analysis was made of some of earlier published NCSS. During the first half of 2011, a wider set of NCSS became available. We extended our analysis to ten NCSS (Australia, Canada, Czech Republic, France, Germany, Japan, The Netherlands, New Zealand, the United Kingdom, and the United States). As each of these ten NCSS intends to address the same global cyber security threat, one would expect a major strategic drive for international collaboration and harmonisation in the various NCSS as well as a common set of national actions. Below, we will analyse whether that is the case or not, make comparisons, and analyse the differences between the NCSS. We will analyse the underlying reasons for the differences. We will use tables as a quick reference to the main elements of the ten NCSS as the NCSS vary in size from nine up to sixty pages. The analysis and final conclusions may be of help to current NCSS implementers and to the developers of future NCSS.

2 Analysis Framework

To analyse and compare the ten NCCS, we look at the following topics:

S. Bologna et al. (Eds.): CRITIS 2011, LNCS 6983, pp. 1–17, 2013.

1. What does the notion ‘Cyber Security’ mean to nations?
2. What are the perceived threats that the various NCSS address?
3. What is the scope of the various NCSS?
4. Is there a relationship with other national strategies?
5. What are the strategic objectives and guiding principles of the NCSS?
6. Which stakeholders are addressed and how are they addressed?
7. What are the key action lines and planned actions?
8. Are emerging threats covered?
9. How are national functions institutionalised by the various NCSS?

3 Cyber Security: A Gamut of Definitions

Table 1 presents an overview of the various definitions and descriptive understandings of the notion ‘Cyber Security’ in the various NCSS.

Only five nations provide a definition for ‘Cyber Security’. Canada and the UK use a descriptive text to indicate what cyber security means to them. The Czech Republic, Japan and the USA do not provide a definition or description. It can be observed that some nations focus on the information security aspects whereas other nations consider Cyber Security as a property to address and counter threats from cyberspace.

From the table above, it is clear that there is no harmonised understanding of the notion ‘Cyber Security’ by the ten nations; three nations even fail to present a definition or a description of the notion in their NCSS.

Observation 1. An internationally accepted and harmonized definition of ‘Cyber Security’ is lacking.

All ten nations consider the cyber threat as an international threat. All NCSS plan activities for international collaboration to secure cyberspace. This requires a common understanding of notions like ‘cyber crime’, ‘cyber security’, etceteras. Recently, a joint Russian-U.S. bilateral working group of the EastWest Institute (EWI) and Moscow University has suggested a terminology framework [1] which may be a starter for harmonisation although some of the proposed cyber terminology requires more debate. According to them cyber security is “*a property of cyberspace that is an ability to resist intentional and unintentional threats and respond and recover*”. Compared to the Table 1 definitions, this definition may replace most of the current national notions and definitions when accompanying semantics clarify whether the set of threats include or exclude threats like physical and electromagnetic disruptions of cyberspace. Moreover, the risk acceptance aspect in the German definition has to be covered in some way or another.

Observation 2. A global harmonised definition and understanding of ‘cyber security’ (and related terminology framework) would be beneficial to all nations.

Table 1. NCSS definitions of Cyber Security

	Definition?	*Cyber Security is …*
AUS	definition	Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.
CR	no definition	
CAN	descriptive	An appropriate level of response and/or mitigation to cyber attacks – the intentional or unauthorised access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information.
FRA	definition	An information system allowing to resist likely events resulting from cyber space which may compromise the availability, the integrity or confidentiality of data stored, processed or transmitted and of the related services that Information and Communication (ICT) systems offer.
GER	definition	(Global) cyber security is the desired objective of the IT security situation, in which the risk of (global) cyberspace has been reduced to an acceptable minimum. *German, civil, and military cyber security are defined in similar wordings.*
JPN	no definition	
NLD	definition	Cyber security is to be free from danger or damage due to the disruption or destruction of ICT, or due to the abuse of ICT.
NZ	definition	The practice of making the networks that constitute cyber space as secure as possible against intrusions, maintaining confidentiality, availability, and integrity of information, detecting intrusions and incidents that occur, and responding and recovering from them.
UK	descriptive	Cyber security embraces both the protection of UK interests in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers.
USA	implicit	References to 'information security'.

4 Ten National Cyber Security Strategies

Table 2 below contains base information for the NCSS of Australia (AUS), Canada (CAN), Czech Republic (CR), France (FRA), Germany (GER), Japan (JPN), The Netherlands (NLD), New Zealand (NZ), the United Kingdom (UK), and the United States (USA) such as the publication date and language(s), reference(s), and scope.

4.1 The NCSS – General Remarks

It is interesting to note that four of the five non-native English speaking countries have published an English translation of their NCSS simultaneously with their native language version. Most of the ten NCSS have been published for the first time. Note that an updated version of UK's 2009 NCSS is expected to appear in the Autumn of 2011. The USA strategy was published in 2003 when the notion 'cyber security' was less in use. In 2010, the Obama Administration undertook a Cyberspace Policy Review which resulted in a set of new national cyber security activities [2].

4.2 Scope of the NCSS

Most NCSS relate their cyber security activities to cyberspace in their descriptive texts. The German NCSS states that it considers 'only information and communication technology (ICT) connected in a certain way to Internet. The Australian and the Canadian NCSS suggest that these national strategies focus on internet connected ICT only. The Dutch NCSS explicitly states that it addresses the full range of ICT which apart from Internet-connected ICT comprises e.g., chip cards, in-car systems, and information transferral media. The other NCSS are less outspoken about this topic but do not restrict their focus.

Observation 3. Some NCSS are restricted to Internet-connected ICT only leaving the protection of other ICT that might very well be hampered out-of-scope.

4.3 Relationship with Other National Strategies

Most of the ten NCSS relate to the nations' National Security Strategies (Table 2). Most often, an earlier national threat and risk assessment is the main instigator of the NCSS development. The Dutch take a different approach. One of their NCSS actions is to deliver a national cyber threat and risk assessment for inclusion in the national risk assessment register (NRB) on a yearly basis. As a result, the NRB process may trigger the need for an update of the Dutch NCSS.

Although the cyber security threat to Critical Infrastructure (CI) is explicitly discussed by most NCSS, the relationship of NCSS with existing Critical Infrastructure Protection (CIP) strategies is less explicit. Critical (Information) Infrastructure (C(I)I) operators may become confused. Moreover, none of the European NCSS refers to the European program on CIP (EPCIP).

Observation 4. Most of the ten nations mention the cyber threat to their CI. Their NCSS, however, lack to clarify the relationship of existing national and international CIP strategies and the national cyber security strategy.

Most of the ten NCSS address the economical aspects of the cyberspace realm. Cyber security is considered as a minimal requirement to enhance the prosperity of the population and to foster economic welfare. The EU Digital Agenda [3] should be a driver for cyber security activities of the 28 European member countries, but only the German and Dutch NCSS refer to the Digital Agenda in their NCSS.

In most of the ten nations a discussion takes place about which governmental department or agency is the leading agency when a major cyber attack or disruption affects the nation. As part of their cyber defence strategy, nations may develop military cyber operations/ cyber defence capabilities as outlined in the British NCSS, the French NCSS reference to the French national security and defence strategy, and references in the German and Dutch NCSS to strategic Cyber Operations plans.

4.4 Perceived Threats

Risk

With respect to the perceived cyber threats, most of the ten nations explicitly mention the threats to their C(I)I and their national security. Only Australia and Canada explicitly state the cyber security risk to their defence abilities. France, despite its national defence driven NCSS and the Netherlands implicitly address this last threat.

From an economic point of view, both Germany and Japan mention the risk of stagnation of globalisation when the cyber security risk is insufficiently addressed. Related to this threat is the threat of disruption of the societal and social ICT-life of citizens. Most nations, with exception of France, Germany and the USA mention this threat. The Netherlands is the only nation which formulates the threat of loss of public confidence in the use of ICT.

Observation 5. Most NCSS address the general cyber crime and e-spionage type of threats. Only a small set of nations consider threats to their national defence, economy, and public confidence.

Threat Actors

All nations except Japan and the USA pinpoint individuals, criminals, and organised crime as threat actors. Cyber espionage (e-spionage) is mentioned by all nations but the Czech Republic and Japan. All nations but Australia and New Zealand mention the threat of hostile activities by foreign nations (e.g., cyber warfare). Despite the 2011 set of attacks in cyberspace by groups like Anonymous and LulzSec, only the Dutch and New Zealand's NCSS mention (h)activists as threat actors.

The terrorist threat to cyberspace is mentioned by all nations but Japan. There are however large differences. Some nations fear (potential) cyber attacks by terrorists on their C(I)I, something which has not occurred so far. Other nations consider information published in cyber space by terrorists, the ability for terrorists to communicate using ICT, and the gathering of intelligence on terrorists as topics that belong to their national cyber security approach.

Observation 6. The NCSS do not show a common understanding of the terrorist threat in cyberspace.

Both the Germany and Japanese NCSS explicitly address the threat of large-scale cyber attacks to their C(I)I. For Japan, this is not surprising as Japan has experienced several large-scale cyber attacks to its governmental and business systems in the recent past. Germany, however, has not yet experienced large-scale cyber attacks.

Both the German and Japanese NCSS mention the threat of mismatches between functional ICT developments (in other words: ICT innovation) and an appropriate level of cyber security related to those developments as a threat to be addressed. Interestingly, none of the other nations address this important topic.

The UK NCSS comprises jamming and signal modification (e.g., of GPS signals) and high-power radio frequency transmission (e.g., High Power Microwave) damaging unprotected electronics to be part of set of cyber security threats they intend to addressed. None of the other NCSS publically refer to these specific threats which are often only dealt with by the military despite growing concerns about criminal use.

Table 2. National Cyber Security Strategies (NCSS) ■ = explicitly described, □ = implicitly referenced

	AUS	*CAN*	*CR*	*FRA*	*GER*
Reference to NCSS document Other language(s)	English [4] n/a	English [5] French [6]	Czech English [7]	French [8] n/a	German [10] English [11]
Issued	2009	10.2010	15.07.2011	15.02.2011	23.02.2011
First NCSS version?	yes	yes	yes [1]	yes	yes
All Cyber threats to ICT?	only Internet connected systems	only Internet connected systems	yes	yes	only Internet connected systems
Relates to:					
- National Security Strategy	■	■	■	■	■
- Critical Infrastructure Protection Strategy		■			■
- National Digital Agenda	■	no	no	no	no
- EU Digital Agenda [17]	n/a	n/a	no	no [2]	■
- National Defence Strategy				■ [9]	□
Addresses cyber threats to:					
- Critical infrastructure	■	■	■	■	■
- Defence abilities	■	■		□	
- Economic prosperity	■	■	■		■
- Globalisation					■
- National Security	■	■	■	■	□
- Public Confidence in ICT					
- Social Life of Citizens	■	■	□		
Addresses cyber threats from:					
- Activism					
- Criminals/Organised crime	■	■	■	■	■
- Espionage	■	■		■	■
- Foreign nations/ cyber warfare		■	■	■	■
- Terrorists	■	■	■	■	■
- Large-scale attacks		□			■
- Mismatch technology development and security					□

[1] The Czech NCSS has been issued as a draft document awaiting discussion, first in the Czech National Security Council, next by the Government of the Czech Republic.

[2] The EU Digital Agenda was published after the publication of UK's NCSS.

Table 2. (*continued*)

	JPN	*NLD*	*NZ*	*UK*	*USA*
Reference to NCSS document	Japanese	Dutch [14]	English [16]	English [17]	English [20]
Other language(s)	English [12]	English [15]	n/a	n/a	n/a
Issued	03.02.2009	22.02.2011	07.06.2011	25.06.2009	2003
First NCSS version?	no: 2006 [13]	yes	yes	yes	yes
All Cyber threats to ICT?	implicitly	yes	networked systems only	yes	implicitly
Relates to:					
- National Security Strategy		□		■ [18-19]	■
- Critical Infrastructure Protection Strategy		□		□	
- National Digital Agenda	no	■	no	■	no
- EU Digital Agenda [17]	n/a	■	n/a	no	n/a
- National Defence Strategy		□		□	
Addresses cyber threats to:					
- Critical infrastructure	□	■	■	■	□
- Defence abilities		□			
- Economic prosperity	■	■	■	■	■
- Globalisation	■				
- National Security	■	□	■	■	■
- Public Confidence in ICT		■	□		
- Social Life of Citizens	■	■		■	
Addresses cyber threats from:					
- Activism		■	■		
- Criminals/Organised crime	□	■	■	■	□
- Espionage	□	■	■	■	■
- Foreign nations / cyber warfare	■	■		■	■
- Terrorists		■	■	■	■
- Large-scale attacks	■				□
- Mismatch technology development and security	■				

Observation 7. Only the UK addresses the jamming, signal modification and high-power transmission threats in its national cyber security approach.

5 Strategic Level Topics of the NCSS

5.1 Strategic Objectives

Table 3 outlines the strategic objectives in the ten NCSS. Major differences in the national strategic approaches are found depending on the differences in starting points: economic prosperity, national security, or (military) defence. Apart from that, the German NCSS does not clearly state strategic objectives. It mentions a set of strategic priority areas which other NCSS present as action line. The Australian, Canadian and New Zealand's NCSS structure their strategies along an alike three-fold approach: government, critical businesses, and citizens/individuals.

Table 3. Strategic objectives of the ten NCSS

AUS	The maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy: 1. All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online; 2. Australian businesses operate secure and resilient ICT to protect the integrity of their own operations and the identity and privacy of their customers; 3. The Australian government ensures its own operations and the identity and privacy of their customers.
CAN	Meeting the Cyber Security threat by: 1. Securing government systems; 2. Partnering to secure vital cyber systems outside the federal government; 3. Helping the Canadians to be secure online.
CR	To maintain a safe, secure, resistant and credible environment that makes use of available opportunities offered by the digital age.
FRA	1. To be a world power in cyber defence; 2. To guarantee the French national freedom to decide by protecting national information; 3. To reinforce the cyber security of critical infrastructures; 4. To ensure the safety in the cyberspace.
GER	Strategic security areas rather than objectives are presented: 1. Protection of Critical Infrastructures; 2. Secure IT systems in Germany; 3. Strengthening IT security in the public administration; 4. National Cyber Response Centre; 5. National Cyber Security Council; 6. Effective crime control in cyberspace; 7. Effective coordinated action to ensure cyber security in Europe and worldwide; 8. Use of reliable and trustworthy IT; 9. Personnel development in federal authorities; 10. Tools to respond to cyber attack.
JPN	1. Reinforced policy to counter cyber attacks; 2. Policies to adapt to changes in cyber security environment; 3. Active/dynamic cyber security measures (see [12]).
NLD	To reinforce the security of the digital society, in order to increase confidence in the use of ICT by citizens, business and government in order to stimulate the Dutch economy and to increase prosperity and well-being of its citizens. Proper legal protection in the digital domain is guaranteed and societal disruption is prevented. Adequate action will be taken if things were to go wrong.
NZ	1. Raise awareness and on-line security of individuals and small businesses; 2. Protecting government systems; 3. Build strategic relationships to improve cyber security for critical infrastructure and other businesses.
UK	Citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space. The government will secure UK's advantage in cyberspace by reducing risk, and exploiting opportunities in cyber space by improving knowledge, capabilities and decision-making.
USA	1. Prevent cyber attacks against America's critical infrastructure; 2. Reduce national vulnerability to cyber attacks; 3. Minimize damage and recovery time from cyber attacks that do occur.

Table 4. Guiding principles of the ten NCSS

AUS	1. National leadership. 2. Shared responsibilities. 3. Partnerships. 4. Active international engagement. 5. Risk management. 6. Protecting Australian values.
CAN	See remark in text.
CR	1. Abide the principles of a democratic society and duly consider legitimate interests of its citizens, business sector and public administrations and agencies in relation to citizens. 2. Adequate cyber security measures to protect and guarantee national security will respect privacy, fundamental rights and liberties, free access to information, and other democratic principles. 3. National cyber security measures balance the need to guarantee security with the respect for fundamental rights and liberties.
FRA	None.
GER	All stakeholders have to act as partners and fulfil protection tasks together. Enforcement of international rules of conduct, standards and norms.
JPN	None.
NLD	1. Linking and reinforcing existing cyber security initiatives. 2. Public-private Partnership and clear responsibilities, powers & safeguards. 3. Individual responsibility to secure cyberspace (citizens, businesses, the public administration and its agencies). 4. Active international collaboration. 5. Security measures are balanced and proportional with respect to public and national security versus safeguarding of fundamental human rights. 6. Self-regulation if possible, legislation and regulation when required.
NZ	None.
UK	1. Set of core values: human rights, rule of law, legitimate and accountable government, justice, freedom, tolerance, and opportunity for all. 2. Hard-headed about risk, aims, and capabilities. 3. Tackle security challenges early. 4. Nationally, partnership approach; internationally a multilateral approach; internal government an integrated approach. 5. Retain strong, balanced and flexible capabilities. 6. Continue to invest, learn and improve to strengthen UK's security.
USA	Privacy and civil liberties need to be protected.

The French NCSS strategic objectives stem from a national power projection point of view. France is the only of the ten nations which takes that approach, although some other NCSS support power projection. The UK, for instance, makes clear that it wants to gather and use intelligence on criminals, terrorists, and other adverse actors in cyberspace. Explicitly, their NCSS mentions the exploitation of such information and the disruption of adversary activities. Recently, it was published that MI6 hacked into Al Qaeda's on-line magazine Inspire and replaced an article on 'Make a bomb in the Kitchen of your Mom' with a page of recipes for 'The Best Cupcakes in America' [21].

Despite the differences in wording, most NCSS aim for a safe, secure and resilient ICT environment for the citizens, society, and economic prosperity. As only nation, Japan recognises the need for agile adaption to new and upcoming cyber security threats in their set of strategic objectives.

Observation 8. All but one NCSS lack a strategic objective which reflects the need for agile adaption to emerging cyber security threats.

5.2 Guiding Principles and Framework Conditions

Seven of the ten nations relate the content of their NCSS to guiding principles or framework conditions (see Table 4 above). Although Canada does not explicitly list any guiding principle in their NCSS, they consider most of the guiding principles of the USA, UK and Australia to resemble their own. Each of the seven nations considers the protection of civil liberties and other (inter)national democratic core values as guiding principles to their NCSS. UK's guiding principles are by far the most outspoken reassuring their citizens about the basics of its national cyber security approach.

Observation 9. The NCSS of France, Japan and New Zealand lack guiding principles/ framework conditions for their cyber security actions and activities.

Table 5. The NCSS directly addresses the following types of stakeholders with respect to threats, vulnerabilities and measures (□ when discussed in NCSS but limited set of actions/activities)

	Citizens	*SME*	*ISP*	*Large organisations*	*CI Operators*	*The State / national security*	*Global infrastructure & issues*
AUS	■	■	■	■	■	■	□
CAN	■	□	□	■	■	■	□
CR	■	■	■	■	■	■	
FRA	■	■	□	■	■	■	□
GER	■	■	■	□	■	■	■
JPN	□	□		□	■	■	□
NLD	■	■	□	■	■	■	□
NZ	■	■	■	■	■	■	
UK	■	■	□	■	■	■	■
USA	■	■	□	■	■	■	■

5.3 Stakeholders

With respect to stakeholders, the Japanese NCSS limits itself to the government and the critical sectors (see Table 5). Internet Service Providers (ISP) are only explicitly addressed by the Australian, Czech, German and New Zealand's NCSS. Australia's ISP, supported by the Australian government, undertake a set of joint activities to raise the cyber security of their operations and their customers. An ISP Code of Practice and identifying compromised customer systems are part of that approach (see [1]). Germany, the UK and the USA NCSS explicitly consider the global cyber infrastructures as stakeholders despite that it will be hard to pinpoint who is responsible.

6 Tactical/Operational Level Topics of the NCSS

6.1 Key Action Lines and Planned Actions

As Table 6 shows, most of the NCSS present a limited set of planned action lines and related sets of, often operational, subsidiary actions. Where feasible, we directly refer to numbering in the specific NCSS.

Both Japan and the USA are the only nations explicitly addressing the dynamics of the cyber security threat. Japan sees the agile adaption to emerging cyber security threats even as a strategic objective. Japan approaches the cyber security issues more from a wider (holistic) security perspective than the other nations. Some nations mention specific emerging cyber threats in their NCSS such as France and Japan which plan to address the cyber security of cloud computing. Japan also plans to address the security of IP version 6 and of home appliances taking part in smart grids.

All nations address the protection of their critical infrastructures and their critical information infrastructures including the government's own ICT. Some nations refer in their NCSS to already existing activities rather than starting new ones. Only some of the ten nations refer to their military cyber security capabilities and plans. The Dutch NCSS points to cyber operations structures and activities planned by the Ministry of Defence which were published as part of the Defence reform plans shortly after the Dutch NCSS was published. In a similar way, the German NCSS points to cyber operations plans of the German Armed Forces (Bundeswehr).

Most nations have cyber security awareness programs and plans for cyber security education. Apart from community-wide programs, some nations (e.g., Germany, the Netherlands, UK and USA) develop high-priority programs to educate and train a large number of cyber defence and law enforcement experts. Apart of New Zealand and the UK, all nations work on specific ICT crisis management measures to address major cyber-related disruptions. National and sector-specific exercises are often related to these activities. At the same time, most NCSS refer to the development of national detection capabilities and national response capabilities.

Most NCSS mention international collaboration as an action line or high priority topic. However, only a few specific actions are mentioned in the various NCSS. This despite the fact that the majority of the cyber threats require swift collaborative international action as adversaries and cyber criminals will not wait until multiple national authorities finally agree to act. Germany, The Netherlands and USA expressed that they intend to promote the Cybercrime Convention to other nations [22]. Canada intends to ratify the Cybercrime Convention treaty; the UK did that recently. The Czech Republic intends to update their legislation and to mandate a set of cyber security standards to protect their government systems and their C(I)I.

Table 6. Key action lines and planned actions ■ = specific activities; □ implicitly indicated

Key action lines	*AUS*	*CAN*	*CR*	*FRA*	*GER*
Active/dynamic security measures					
Awareness & training/ Information Security Campaign	■	■ (objective 3)	■	action 7	action 2
Adaptable policy to new ICT risk					
Continuity & contingency plans					
Critical Infrastructure Protection	■	■	■	action 4 (objective 3)	action 1
Cryptographic Protection				■	(action 8)
Defence Cyber Operations/ intervention, training & exercises		■		□	■
Economic growth	■	■	■		
Education	■	■	■	■	(action 9)
Exercises	■	■			■
Explicit holistic view					
Exploitation to combat threats					
ICT crisis management	■	■	■	■	action 4
Improved security of ICT products					
Information Exchange (PPP)	■				
Information Sharing	■	■	■		action 4
Intelligence gathering on threat actors	■	■			
International collaboration	■	■	■	action 6	action 7
Knowledge development					
Legislation			■		
Mandating security standards			■		
National Detection Capability	■	■	■	action 2	
National Response Capability	■	■	■	action 2	action 4
Privacy protection	■	■		□	
Promote Cyber Crime Convention		□			action 6
Protection of non-critical infra	■	■	■		
Public-private Partnership	■	(objective 2)	■		
Reducing adversary's motivation & capabilities					
Research & development	■	■	■	action 3	
Resilience against disturbances/ threat & vulnerability reduction	■			action 4	
Secure protocols and software				■	action 2
Secure sourcing of products				■	action 8
Self Protection of the Government	■	(objective 1)	■	■ (objective 2)	action 3
Strategic Cyber Security Council			ICBCS		action 5
Threat & vulnerability analysis	■	■	■	action 1	action 4
Tracing criminals & Prosecution	■	■		action 5	action 6
Actions defined in SMART way?	no	no	no	no	no

Table 6. (*continued*)

Key actions and action lines	*JPN*	*NLD*	*NZ*	*UK*	*USA*
Active/dynamic security measures	■ (objective 3)				■
Awareness & training/ Information Security Campaign	■	on-going; intensify	■	■	priority 3
Adaptable policy to new ICT risk	■ (objective 2)				
Continuity & contingency plans	■	telecom law		telecom law	□
Critical Infrastructure Protection	action line 1	on-going	■	■	on-going
Cryptographic Protection	■				
Defence Cyber Operations/ intervention, training & exercises		■		■	■
Economic growth	action line 4 (objective)	□ (objective)		□ (objective)	□
Education		action line 6		■	□
Exercises		■	■	□	□
Explicit holistic view	action line 3				priority 5
Exploitation to combat threats				■	
ICT Crisis Management	action line 2	■			■
Improved security of ICT products		■			
Information Exchange (PPP)		■		■	
Information Sharing		■			■
Intelligence gathering on threat actors		■		■	
International collaboration	action line 5	■		■	priority 5
Knowledge development		■		■	
Legislation			review		
Mandating standards					
National Response Capability		action line 4	■		priority 1
Privacy protection	■	■			
Promote Cyber Crime Convention		■	considering	[3]	■
Protection of non-critical infra	□	□		□	
Public-Private Partnership	■	action line 1		■	
Reducing adversary's motivation & capabilities				■	
Research & development		action line 6	■	■	■
Resilience against disturbances/ threat & vulnerability reduction	action line 1	action line 3	■	■	priority 2
Secure protocols and software					■
Secure sourcing of products				□	
Self Protection of the Government	■	■	■	■	priority 4
Strategic Cyber Security Council		all actors		only gov.	
Threat & vulnerability analysis		action line 2			■
Tracing criminals & Prosecution	■	action line 5			■
Actions defined in SMART way?	yes	no	no	no	no

[3] The UK ratified the Cyber Crime Convention In May 2011.

The Netherlands NCSS intends to put the software security quality issue on the international agenda. Software liability may reduce the amount of insecure software being delivered to the market.

As discussed before, the UK plans to gather intelligence and use that to reduce the motivation and capabilities of adversaries operating in cyberspace as part of the exploitation objective in their NCSS.

Only the French and German NCSS explicitly refer to secure sourcing and own development of so-called government-off-the-shelf (GOTS) hardware and software to be used as part of the critical and sensitive government infrastructures and sometimes in national critical infrastructure. The UK implicitly mentions its information assurance agencies. The other NCSS do not make clear whether GOTS hardware and software is a high priority issue or not.

Germany, Japan and the Netherlands plan a cyber security council (CSC) at the strategic level. The Japanese one is an intra-governmental board. The Dutch CSC will have members from public, private, and R&D institutions/academic organizations. The German CSC will be a council in which private stakeholders may participate as observers.

Because of the sense of urgency expressed by most NCSS, one would expect that most actions would be defined in a SMART way: Specific, Measurable, Achievable, Realistic and Timely. Apart from the Japanese NCSS and some minor actions mentioned in other NCSS that is not the case.

Observation 10. The NCSS lack a notion of collaborative international detection and response capabilities.

Observation 11. The Japanese NCSS takes a wide view to cyber security and includes an agile adaptation to emerging cyber security threats.

Observation 12. The Netherlands requests international action to enhance the software security quality globally by promoting software liability.

Observation 13. Only one of the ten NCSS defines its set of planned actions in a SMART way. Therefore, most nations are unable to measure and determine afterwards whether their strategy is a success and where strengthening is required by taking additional measures.

6.2 NCSS Institutionalisation by the Various Nations

Table 7 shows that most nations plan to institutionalise by enlarging mandates and efforts of existing government organisations and agencies like The Netherlands and the UK. Australia, Czech Republic, and Germany create new cyber security operational centres. Germany, the Netherlands and the UK will establish cyber security councils at the strategic level. Germany and the Netherlands refer to new military operational cyber security capabilities; Canada will extend their existing defence capabilities.

Table 7. NCSS institutionalisation (CS = Cyber Security)

	AUS	*CAN*	*CR*	*FRA*	*GER*
Extends existing organisations		CSE; DND/CF			BSI
Establishes new organisations	CERT AUS; CS Operations Centre (CSOC)		Interdpt. Coordination Board for CS (ICBCS); CERT-CR		National CS Council; National Cyber Abwehrzentrum (NCAZ)

	JPN	*NLD*	*NZ*	*UK*	*USA*
Extends existing organisation(s)	National Information Security Center (NISC)	GovCERT.nl KLPD/THTC	National CS Centre (absorbs CCIP)		DHS as centre of excellence on cyber security
Establishes new organisation(s)		Nationale CS Raad (NCSR); National CS Centre (NCSS); Defence Cyber Expertise Centre		Office of CS (OSC) CS Operations Centre (CSOC)	

7 Conclusions

Only half of the ten NCSS are based on a strict definition of cyber security. The other nations either use descriptive text or a kind of ‘common understanding’. Because of the lack of a harmonized terminology set, nations will be hampered in collaboratively addressing threats to cyber space.

Comparing the ten NCSS, major differences in approaches stemming from the differences in starting points are found: economics, national security, or military defence. Another major difference is the scope of cyber security: internet connected systems only versus the whole of ICT. Most NCSS lack a holistic approach to the threats to cyberspace; only the UK explicitly mentions the electromagnetic spectrum threats to cyberspace. Emerging cyber security threats are only explicitly addressed by Japan in their NCSS.

Most NCSS recognise the need for a society-wide approach: citizens, businesses, the public sector, and the government. However, the set of actions specially aimed at citizens is most often limited to awareness campaigns and minor security education actions at schools. Only Australia has an outreach program which supports the citizens with national cyber security tools. This is also a demonstration that most nations underrate the (inter)national risk of loss of public confidence in ICT which may seriously hamper economic prosperity.

Most NCSS are developed without a clear descriptive section on how the NCSS relates to existing national and international strategies and policies, such as the protection of critical infrastructures.

All NCSS recognise the international cyber security threat and plan weakly described activities for international legal and operational collaboration. Given the threats and the cyber security trouble most nations experience on a daily basis, a more aggressive approach and leadership is expected, especially from the EU nations. In May 2011, the US issued their International Strategy for Cyberspace [23] and ask other nations to endorse the guiding principles, to harmonise legal approaches (with an explicit reference to the Council of Europe Cybercrime convention [20]), to build and enhance military alliances to 'confront potential threats in cyberspace', and to work on the governance issues.

Only one NCSS addresses the issue of insecure software and the need for software manufacturers to be held accountable.

Last but not least, all but one NCSS is developed with national political sensitivities and the departmental playing fields in mind. As a result, all activity lines and set of actions are far from being SMARTly defined. This may cause less progress to be made when the national political focus temporarily shifts. Given the sense-of-urgency expressed in almost all NCSS, this may result in a boomerang effect to nations when they are not properly prepared for dealing with the cyber security risk.

References

1. Rauscher, K.F., Yashenko, V. (eds.): Critical Technology Foundations. EastWest Institute, London (2011), http://www.ewi.info/system/files/reports/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20%282%29.pdf
2. The White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, Washington, DC, USA (2010), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
3. European Commission, A Digital Agenda for Europe – COM(2010) 245 final/2, Brussels, Belgium (2010), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R(01):EN:NOT
4. Attorney General, Cyber Security Strategy, Australia (2009), http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity#h2strategy
5. Public Safety Canada, Canada's Cyber Security Strategy: For a stronger and more prosperous Canada (2010), http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf
6. Sécurité publique Canada, Stratégie de cybersécurité du Canada: Renforcer le Canada et accroître sa prospérité, Ottawa, Canada (2010), http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-fra.pdf
7. Ministry of Interior, Cyber Security Strategy of the Czech Republic for the 2011-2015 period (Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011-2015), Prague, Czech Republic (2011), http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF
8. Secrétariat général de la défense et de la sécurité nationale, Défense et sécurité des systèmes d'information: Stratégie de la France (2011), http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

9. Secrétariat général de la défense et de la sécurité nationale, Défense et Sécurité nationale: Le Livre Blanc, Paris, France (2008), http://www.defense.gouv.fr/portail-defense/enjeux2/politique-de-defense/livre-blanc-2008
10. Bundesministerium des Innern, Cyber Sicherheitsstrategie für Deutschland (2011), http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile
11. Federal Ministry of the Interior, Cyber Security Strategy for Germany, Germany (2011), http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile
12. Information Security Strategy for Protecting the Nation, Information Security Policy Council, Tokyo, Japan (2010), http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf
13. The First National Strategy on Information Security: towards the realization of a trustworthy society, Information Security Policy Council, Tokyo, Japan (2006), http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf
14. Netherlands Ministry of Security and Justice, De Nationale Cyber Security Strategie: Slagkracht door samenwerking, The Hague, The Netherlands (2011), http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/02/22/nationale-cyber-security-strategie-slagkracht-door-samenwerking/de-nationale-cyber-security-strategie-definitief.pdf
15. Netherlands Ministry of Security and Justice, The National Cyber Security Strategy (NCSS): Success through Cooperation, The Hague, Netherlands (2011), http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011
16. Ministry of Economic Development, New Zealand's Cyber Security Strategy, New Zealand (2011), http://www.dpmc.govt.nz/dpmc/publications/nzcss
17. Cabinet Office, Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space, London, United Kingdom (2009), http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf
18. HM Government, The National Security Strategy Update 2009: Security for the Next Generation, London, United Kingdom (2009), http://www.official-documents.gov.uk/document/cm75/7590/7590.pdf
19. HM Government, A Strong Britain in an Age of Uncertainty: The National Security Strategy, London, United Kingdom (2010), http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy
20. The National Strategy to Secure Cyberspace, The White House, USA (2003), http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf
21. http://lafiga.firedoglake.com/2011/06/03/finally-an-intelligent-use-for-cupcakes-hacking-terrorist-sites (last visited June 30, 2013)
22. Council of Europe, Convention on Cybercrime, ETS No. 185 (2001), http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm
23. The White House, International Strategy for Cyberspace, Washington, DC, USA (2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf