Airports as Critical Transportation Infrastructures Increasingly Impacted by Cyberattacks: A Case Study

Alessandro Pollini[1(✉)], Alessandra Tedeschi[1], and Lorenzo Falciani[2]

[1] Deep Blue, Piazza Buenos Aires 20, 00198 Rome, Italy
{alessandro.pollini,alessandra.tedeschi}@dblue.it
[2] George Washington University, 2121 St NW, Washington, DC, USA
Lorenzo@alumni.gwu.edu

Abstract. The current state of cyber security in today's critical infrastructures reveals that there have been a limited but growing number of incidents in which the defences of safety-critical applications have been penetrated. In this work we concentrate on airports' infrastructures and investigate how airport authorities are concerned with emerging terrorist threats, such as cyber threats, against airport installations and systems, and security gain and risk perception of passengers. A review of actual attacks and real issues in the airport infrastructures allowed us to build projections or potential future scenarios. In the context of the present research, we analyzed in a deeper detail these factors, developed an emerging threat scenario, and calibrated a prediction model on our findings.

Keywords: Airport · Security · Cyberthreat · Transport · Infrastructure

1 Introduction[1]

The current state of cyber security in today's critical infrastructures reveals that there have been a limited but growing number of incidents in which the defences of safety-critical applications have been penetrated, including Air Traffic Management infrastructures, Airport infrastructures, Fire and Rescue dispatch systems and Maritime monitoring applications. The first step is to identify what the new and emerging threats are. Despite the reluctance of private and public companies to report cyber attacks, especially those that have been successful, a number of precedents can be found in both old and recent media reports. Old reports show that the cyber security problem is not a novelty and can be rooted back to the very introduction of analogue remote access methods. New media reports help characterize the current state of cyber security identifying existing threats and attack vectors. In this work we concentrate on airports' infrastructures and investigate how the airport authorities are concerned with emerging terrorist threats, such as cyber threats, against airport installations and systems, and security gain and risk perception of passengers. As a way to mitigate the impact of such new menace, some technical, procedural and organizational countermeasures are being

[1] The views expressed in this article are those of the authors and do not necessarily represent the views of, and should not be attributed to, their respective companies and organizations.

F. Cleary and M. Felici (Eds.): CSP Forum 2014, CCIS 470, pp. 37–48, 2014.
DOI: 10.1007/978-3-319-12574-9_4

implemented. Even though it is hard to assess the risks posed by cyberattacks, the impact of the attacks is also captured in this study, both in terms of the probability of an attack and the consequences for safety and security [1]. The review of actual attacks and real issues in the airport infrastructures allowed us to build projections or potential future scenarios. The identified scenario is representative of the airport environment, and the risks are representative of emerging threats.

Cyber security emerging threats for airports are those threats that have already been identified, at least in one instance, as feasible on information systems, and are poised to become more impactful, or more widespread, or to migrate in the airport infrastructure, contributing to the overall risk of the airport's assets, operations or users. The threat and the threat agents vectors included in the selected scenario are identified as part of the list of 10 emerging threats for Critical Infrastructure [2], including the airport environment (i.e. includes aircraft, air traffic control systems, commercial and military airports, heliports, and landing strips) as officially appointed in the U.S. National Infrastructure Protection Plan (NIPP) [6]. While risks and impacts of a cyber attack are most intimately connected with the target environment, resources, and function; the motives, threat agents, and threats can be drawn back to reasonably small and consistent sets that span unaltered across sectors (public and private), industries (financial, manufacturing, transportation, etc.), and level of informatization of targets (low technology and low maturity to highly coupled technological infrastructures).

The socio-economic models are built on the basis of the developed scenarios. The intention of these models is not to accurately predict future modes of attack. In contrast, the aim is to advise airport security decision makers by providing them with an optimal portfolio of security investments. The Adversarial Risk Analysis (ARA) modeling approach [3] has been used to build the Cyberthreat model. According to the ARA approach, two intelligent adversaries' (the Defender and the Attacker) decisions and actions are modeled. The utility functions, aggregating all relevant information about costs, revenues, payoffs, etc., are used with the goal of modeling each adversary's preferences and utilities. Utility functions are built from the costs and revenues relevant for each actor. Non-monetary rewards can be included in the revenue function as well (e.g., the revenues in terms of fame, recognition among peers, etc. might be considered). Both adversaries are expected to be utility maximizers, i.e. they both will try to obtain the maximum profit from their actions, making the corresponding decisions. The final output of the model will be to give advice to airport authorities for devising a security plan, i.e. providing them with an optimal portfolio of defensive measures.

The research questions guiding the investigation of the airport security scenarios are:

- Do the current security regulations adequately and appropriately ensure that airports mitigate the risks and optimize resource allocation?
- Different sized airports: what is the difference from security cost and decision perspective?
- What is the impact related to the risk perception of passengers, of airport operators, or the social acceptance of security measures; and how can it be modeled?
- What is the balance between new security measures and emerging threats, in terms of cost and technology, security gain and risk perception of passengers?

These questions form the key requirements of this work. By utilizing the threats and the scenarios identified in the present report we aim to answer the questions presented above and build socio-economic models based upon those answers.

This paper presents a literature of recent cyber disruptions of critical infrastructures (Sect. 1) and airports' attacks (Sect. 2). Cyberthreat scenarios are then described in detail (Sect. 3) and the selection and validation processes that they underwent is addressed (Sect. 4). As concluding section, the modeling approach and the future steps are also presented (Sect. 5).

2 Recent Cyber Disruptions of Critical Infrastructures

The first step in the identification of the relevant scenarios has been to identify what is the current state of cyber security in today's airports' infrastructures, and to identify emerging threats. Despite the reluctance of private and public companies to report cyber attacks, especially those that have been successful, a number of precedents can be found in both old and recent media reports. Old reports show that the cyber security problem is not a novelty and can be rooted back to the very introduction of analog remote access methods. New media reports help characterizing the current state of cyber security identifying current threats and attack vectors.

Rationale for selecting the following references is:

(1) The problem that they present is not new, it is connected to the very presence of the IT infrastructure,
(2) Successful attacks inflicted large consequences even in a less interconnected (and slower) world.

Table 1. Cyberattack

Year	Description	Reference
1982	Devastating Explosion in Siberian Gas Pipeline Caused by Logic Bomb – The result was *the most monumental non-nuclear explosion and fire ever seen from space* (Thomas Reed, Former AF Secretary)	http://en.wikipedia.org/wiki/Siberian_pipeline_sabotage
1997	Hacker launched a cyber attack that resulted in the disruption of all local police and fire 911 services as well as the ability of incoming aircraft to activate the runway lights at the Worcester, MA airport. The telephone service was out at the airport tower for six hours	http://www.gpo.gov/fdsys/pkg/CHRG-106shrg68563/html/CHRG-106shrg68563.htm

(*Continued*)

Table 1. (*Continued*)

Year	Description	Reference
2000	264,000 gallons of sewage intentionally released by the "insider" Vitek Boden who gained access into the controls of the sewer system of Australia's Maroochy Shire Council	http://www.aci-na.org/sites/default/files/larry_jaffe.pdf
2003	Slammer worm intrusion into Davis-Besse Ohio Nuclear Plant network. It rendered the network useless	http://www.aci-na.org/sites/default/files/larry_jaffe.pdf
2003	Worm infects CSX telecommunications network that supported both their signal system and dispatch system. Passenger and freight train traffic halted in 23 US states	http://www.aci-na.org/sites/default/files/larry_jaffe.pdf
2009–2010	StuxNet Worm Attack Targets Iranian Nuclear Program. Also, Infects India and Pakistan affecting SCADA targeting capability. Stuxnet uses two compromised security certificates (stolen from firms in Taiwan) and a previously unknown security hole in Windows to launch itself automatically from a memory stick. Targets particular Siemens controllers and a specific configuration of devices	http://www.theguardian.com/world/2012/jun/01/obama-sped-up-cyberattack-iran
2012	An unidentified group of hackers targeted various natural gas pipeline companies gained access to and exfiltrated data on how their control systems work	http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/

From the analysis of the cases reported in Table 1 it is possible to conclude that:

(1) Critical infrastructures can be and are attacked with success,
(2) Threat agents are various and diverse,
(3) Resources needed to successfully attack the CIs can be significant, but not always.

2.1 Airports Have Suffered Too

Selected incident reports of cyberattacks targeting Airports are:

2012	The National Technical Research Organisation (NTRO) officials alerted the Airports Authority of India (AAI) to serious vulnerabilities in its cargo management system at Chennai, Coimbatore, Kolkata, Amritsar, Lucknow and Guwahati airports. Weak passwords and outdated operating systems were the main problems. These six airports handled 311,000 metric tonne of international cargo in 2010/11. A single day's disruption would have sent 853 tonnes of cargo to the wrong destinations. "The economic impact would have been immense had the systems been penetrated by unscrupulous elements," says P.K. Kapoor, Executive Director (Information Technology), AAI.
2013	CBI believes a cyberattack led to IGI airport's technical problems, provoking the failure of the passenger processing system and impacting 50 flights delayed and their passengers had to be manually checked in.
2013	Boston digital security firm Trusteer says it uncovered malware hidden in the private network of a major non-U.S. international airport. The company says "the threat could have compromised everything from employees' personal information to the safety of passengers. […] The attack used Citadel Trojan malware—which computer users can unknowingly install simply by clicking on a Web link—to read the screens of employees who logged in remotely to the airport's virtual private network (VPN). It also allowed the cybercriminals to capture the username, password, and one-time passcode of the victims with a form-grabbing technology".

The following conclusions may be drawn:

- Despite the secrecy around security breaches and especially on their impacts, we know that airports have been breached,
- Again, as for the Critical Infrastructures (CIs), resources needed to accomplish the breaches vary greatly, as well as the skill level of the attackers, The news contains often only partial impact assessments.

2.2 Cutting Edge Cyber Security

A search on academic resources and research products related to the field of airports' cyber security did not return many results. Much research and literature has been produced on airport security as a whole socio-technical system, considering cyber security as a single high level item, but without ascertaining in depth its contribution as a single point of failure for the airport infrastructure, neither in terms of direct impact nor economic risk, for both the operator and the users [4].

However, this should not be seen as a lack of research or attention to the problem. Information security includes the major families: people, processes and technology. In the context of airports, the people and processes will vary because of the specific context; however the technological family will mirror other industries, and is consistent with general IT security research, as IT systems and concepts are transversal. It is this connection that allows us to understand the IT security problem in airport, and allows us to use general IT references and studies.

3 Airport Security Cyberattack Scenarios

The information presented above identifies a number of current cyber security threats already 'in the wild', and then a subset of those attacks that previously hit airport infrastructures. The reported events are all actual attacks and real issues, not projections or potential scenarios. Considering that the trend of cyber threats, with respect to their targets and their frequency, has been found to be consistent across many sectors, on the basis of past events it's possible to argue that such attacks will increase and target also airports.

In the context of the SECONOMICS research project [5], it is inevitable to analyze in a deeper detail exactly these factors. For this purpose, three scenarios will be identified, and a prediction model will be developed, calibrated, and run on them.

The identified scenarios aim to be representative of the airport environment, and the risks should be representative of emerging threats. The present paper doesn't attempt to identify new and innovative way to perpetrate cyber attacks. While such an exercise may have a great value in developing a long term strategic view, such an approach lacks the evidence and hard reference data needed to plan actual defence and security measures. Cyber security emerging threats for airports are those threats that have already been identified, at least in one instance, as feasible on information systems, and are poised to have a significant impact, to become more widespread, or to migrate in the airport infrastructure, contributing to the overall risk of the airport's assets, operations or users.

The following scenarios fit the requirements set forth above and relate to the airport context. Within the context of the present research the following three scenarios will be deepened into details, validated through the involvement of the stakeholders and used to leverage the socioeconomic models building.

3.1 Scenario 1: Targeted Cyber Attack

This first scenario is an example of how technology can be used to create damage even where it is minimally used and by an attacker with a limited IT and/or security knowledge.

Scenario: An example in today's Europe would be a hacktivist group wishing to stop pollution by airplanes in a particular zone. It may be also a foreign state or terrorist group trying to disrupt commercial flight operations. The important thing to consider is that the technological knowledge required to successfully perpetrate a targeted cyber attack is limited and, if successful the attack can have the most extensive impact on the IT infrastructure. An iteration of this scenario can see a green hacktivist group gathering intelligence on two sets of airport employees, managing directors and IT system administrators. When enough intelligence has been gathered, they proceed to forge ad hoc emails to those people. The probability that those emails containing links or documents are opened by the receivers is relatively high. The infected attached documents or links then give a backdoor in the systems to the attacker, possibly with the target access privileges. The attacker then gains a foothold in the system with limited

chances to be discovered by eventual Intrusion Detection Systems (IDS)/Intrusion Protection Systems IPSs placed in the network.

Threat agent: Since the complexity of the attack is terms of IT knowledge is limited, virtually any group with sufficient motive can enact it. Intelligence gathering can take some time, which is why this attack is usually perpetrated by groups that can count on more elements to collect data effectively in s short amount of time.

Threat: The name for this type of threat has already been coded with "spear phishing attack". It is a targeted attack to a specific person. It usually involves a phone call to a subordinate or an email sent from a person in the circle of trust of the receiver. Intelligence gathered in advance serves the purpose of avoiding rendering the email suspicious to the eyes of the receiver.

Threat vector: The threat vector is usually a specifically crafted email. It may contain malware, a link to an infected site, or an infected documented. If the target doesn't recognize the attack in time, the system and/or the network used to open the email are at risk. If the target is a system administrator or a manager with extensive access capabilities, the attacker may not even need to escalate privileges or to attack other systems in the network. However, if technical knowledge is available to the group, and the target is not just data, but airport sensitive systems, the intrusion can be used as starting point to launch internal attacks and reach other parts of the network. Even if disconnected from internet access, segregated network segments can be reached.

Vulnerability: The major vulnerabilities for this type of attack are lack of awareness and lack of training for the subject being targeted. However, a well forged email is almost undistinguishable from a legitimate one, and other measures need to be in place to keep this risk at bay. Networks should implement the principle of defence in depth to limit the damage a targeted attack can do to the infrastructure.

Impact: Switch back to manual procedures, loss of control or reliability of information systems.

3.2 Scenario 2: Operation Payback

Disgruntled employees are harmful to any organization and they do exist is a quote from a recent article in Forbes magazine (7/23/2012, The Power Of The Disgruntled Employee). There are many security controls that deal directly with this problem, starting from preventive controls like background checks, to monitoring and deterring controls like auditing and fully integrated Identity Management (IdM) solutions, to emergency and physical controls like fast user de-provisioning and escorting out of the premises in case of termination. This scenario is based on events that happen daily at any type of business and across all industries.

Scenario: The airport is in the need to scale down personnel and terminates a number of employees. One of these employees decides to make its former employer to pay for this decision and s/he is also knowledgeable about IT. S/he knows decides that stealing

personal data would be the perfect punishment for the former employer, as that would result in a big lawsuit, damaging the airport reputation, and it will be expensive to settle against the strict European rules regarding the protection of personal data. The disgruntled employee doesn't even need physical access to the premise, because the airport implements remote access capabilities. The day after the termination s/he unlawfully connects to the airport systems from a coffee shop, finds out that the account is still active, authenticates to the system, escalates the user privileges, and exfiltrates the personal data of all the airport personnel.

Threat agent: A disgruntled employee. The scenario described above assumes the termination, but it is worth noting that many occurrences of disgruntled employees still employed with the target firm have been recorded, and with much more serious impacts.

Threat: unauthorized access to systems and data or illicit use of company property. A disgruntled employee can act on a multitude of assets: recently an Italian disgruntled employee destroyed the complete Brunello wine production of his employer of the last 4 years for a total damage worth millions of Euros, another one, in Poland, continuously damaged computers and servers for 3 years with chemical cleaning products, until he was caught by surveillance cameras. In this scenario we focus on those that directly exploit the IT systems of the airport. It is important to note that the scenario can be construed with a threat that can be either internal, if still employed, or external, if already terminated.

Threat vector: Internet facing systems and especially remote access systems in case of the external threat, otherwise any type of IT internal system, since the threat vector is actually authorized to access those systems. Where the actor doesn't have all the necessary privileges to access its target, but enough to log into a system, the required privileges can easily be escalated if a thorough, efficient, and consistent patch management and change management program are not in place.

Vulnerability: In the case of the internal threat, any vulnerability in any system can be exploited to the advantage of the attacker. If a monitoring and auditing system is not in place, it may be impossible to identify and track down the perpetrator of an internal attack. In the case of an external threat, i.e. a former employee, there range of system that can be used is more limited but not necessarily better protected. For example, a slow user de-provisioning system can allow the terminated employee to access company resources after termination. The same can happen if group accounts are in place.

Impact: Loss of personal data, identity theft, legal risks.

3.3 Scenario 3: Dark Night

Attacks to SCADA networks and engineering systems are occurring in all major critical infrastructures. There is consensus that soon they will multiply also at airports, and small to medium airports should be on the watch. This scenario ultimately means that automated SCADA exploits are more common, available to a broader public, and can

be weaponized more easily. This scenario is based on events that already took place in a different industry, and that can be transposed in an airport context due to the identified cyber trends and evolution.

Scenario: The attacker crafts a piece of malware that is then used to infiltrate the internal IT system of the airport without affecting its operations or tripping monitoring devices. This is considered feasible for various classes of attackers. The malware is delivered and is not discovered by the security staff as it doesn't affect the internal network or its systems. The malware payload contains one or more specific exploits for the airport ground support lights system, which is necessary for safely landing airplanes and is connected with the internal network. It may use an Out of Band (OOB) channel or a maintenance monitoring port. From this moment on, an undetected unauthorized external entity has the capability to command those lights.

Threat agent: A possible attacker is an adversary nation state trying to deny airspace access to commercial flights, to inflict harm to the target country commercial interests, or a terrorist group trying to crash planes or disrupt airport operations to gain media attention.

Threat: The scenario can be set on by various cyber attack threats. A specifically crafted malware would be the threat of choice by the identified threat agent. The sophistication required for this type of threat is quite high, and the resources needed to implement it are medium, making it an affordable attack also for groups, should not be considered a prerogative of nation states.

Threat vector: The attack works on two different steps, infection of the internal network and infection of the SCADA/engineering system. The vector for the first step is any external connection to the internal network, whereas the vector for the second step is the connection between the two systems. The network and SCADA malware can be built upon a number of different issues and can target other systems as well.

Vulnerability: To be successful this attack will need to exploit multiple vulnerabilities, however these are not necessarily high risk vulnerabilities per se, and can be often found in most networks. Furthermore, different attack vectors can be used depending on which vulnerability can actually be identified in the target airport. Vulnerabilities allowing the first step of the attack could be an un-patched endpoint, the lack of defence in depth measures, untrained staff, improperly configured IDSs, etc. While vulnerabilities allowing the second step may include a poor network design, lack of structured processes for maintenance, etc. Vulnerabilities in engineering systems and SCADA are not uncommon.

Impact: Diversion of flights, critical services outage, physical damage/incident.

4 Selection and Validation Process

Section 4 describes the process of selection that the scenarios underwent and the validation according to stakeholders' judgement and contribution. One scenario has

been selected to ground the development of socioeconomic models to support decision-making in airport security.

4.1 Scenario Selection

Airport security stakeholders initially reviewed and evaluated the early formulation of scenarios, and later validated and selected the revised version of the scenarios. Figure 1 summarizes the two phases.

Fig. 1. Scenario selection process

In order to select proper scenarios to steer the modelling and development of a socio-economics security framework and tools, this study focuses on low level Airport Security scenarios that describe how local decisions are affected by the implementation of single security measures by decision makers at the airport. The picture below shows the scenarios' development and selection process (Fig. 2).

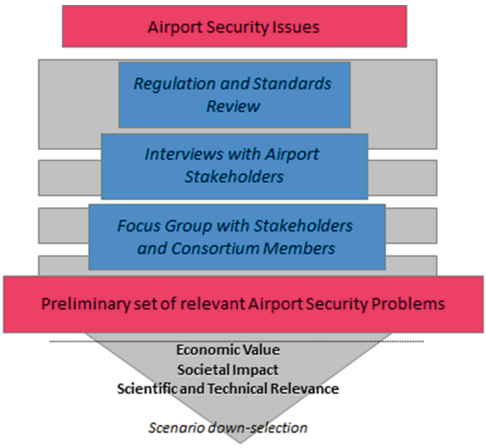

Fig. 2. Process of scenarios development and selection

The Scenario 1: Targeted cyber attack was selected among the three scenarios since it was evaluated to have the greatest impact in the Airport Security domain since it envisions an information security attack that is widespread in many critical infrastructures and that could easily affect airport security in the near future.

4.2 Scenarios Validation

Scenario 1, as well as other Airport Security scenarios (i.e. development of security regulation and physical attack to the control tower) has been presented and discussed with relevant stakeholders in the Airport Security domain, then refined iteratively by consortium partners.

Iterative meetings with two Security Instructors certified by the International Air Transport Association (IATA) have been organized to collect information to feed preliminary models versions, to steer and review the intermediate models, and to evaluate final versions of the models and discuss the results provided. A number of conference calls and phone interviews have been carried out with Operational and Security experts from Esjberg (DK), Brno (CZ) and Pescara (IT) Airports. Policy makers and decision makers at national (i.e. Ente Nazionale per l'Aviazione Civile – ENAC, the Italian CAA) and international levels (i.e. Eurocontrol and the Airport Council International - ACI Europe) have been involved as well.

A cyber-security expert has been involved in the refinement and assessment of Scenario 1.

The following activities have been carried out in order to evaluate and evolve the whole set of operational Airport Security scenarios developed:

- Interview with one Civil Aviation Authority Security Instructors,
- Informal contact with ICT Airport Security Solution Industry,
- Questionnaires for Airport Security Managers (total of 22 Questionnaires sent, 10 Questionnaires back),
- Skype Interviews with Airport Security Managers (3 Interviews done).

Different techniques, like informal contacts, structured and focused interviews as well as multiple choice questionnaires are some of the techniques used to support the stakeholders' engagement in the validation process. The results of these activities have been analyzed and elaborated as input into the socio-economics models.

In particular, Scenario 1 has been evaluated towards the actual collaborative decision making in airport security. 76 % respondents of the Questionnaire thought that the scenario is well structured with respect to both content and completeness of information. In particular, the scenario, originated as an United States specific case, is currently applicable and valuable in Europe as well, since the member states still lack ad hoc regulations on cybersecurity.

Scenario 1 is very innovative and interesting for the involved Policy Makers. ACI Europe is carrying out an in-depth research about cyber-security in Airport and comparing IT security level of different airports (linked to their size and to the national regulations on the topic) and they are studying the European Cyber-Security Strategy to understand how to apply it to the Airport domain to further inform relevant Policy

Makers in the Aviation domain for future Regulations on the topic (currently almost uncovered).

The impact of this scenario needs to be better specified since it could be even worse than the ones currently foreseen. According to the expert judges, the impact of an IT attack needs to put safety and security into relation.

A prologue describing the overall context of emerging threats could be useful. The major need is to prevent the eventual impact of a future threat (like biothreats and powder and chemical substances attacks). In order to reach this aim, the definition of the security scenario may need to be specified through a live example taking into account new security measures and future emerging threats.

5 Conclusions

In this report, the operational airport security cyberattack scenarios developed in this research are described. Through the participatory approach adopted, Airport security stakeholders have been involved in presentation, discussion and iterative refinement of working and final versions of the models and the scenarios.

Possible risks and limitations of the study have been highlighted, and the most appreciated and valuable results of the project are described. The complexity and the innovation of the proposed scenarios make the process of validating them a challenging task. The security, social and economic issues addressed by this project are heterogeneous, and the results of the research will be likewise heterogeneous, ranging from theoretical models to policy guidelines and software toolkit for decision support. The full coverage of security, social and economic issues will be assured by the data collection phase that will inform the development of model. In particular costs related to social issues (e.g. image cost, acceptance of security measures, etc.) will be included in the model aiming at explicitly integrating social and economic issues and developing a socio-economical understanding of the airport security.

References

1. Johnson, C.W.: Preparing for cyber-attacks on air traffic management infrastructures: Cyber-safety scenario generation. In: Proceedings of the 7th IET Conference on Systems Safety and Cyber-Security, Edinburgh, Scotland, 15–18 October 2012. IET, Savoy Place (2012)
2. ENISA Threat Landscape - Responding to the Evolving Threat Environment (2013). http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
3. Rios Insua, D., Rios, J., Banks, D.: Adversarial risk analysis. J. Am. Stat. Assoc. **104**(486), 841–854 (2009)
4. Foster, C.E., Hoey, J.: Airport security complexity: Problems with the information security components. In: Van de Walle, B., Carle, B. (eds.) 2nd International ISCRAM Conference, pp. 61–66. LeMoyne College Business Department, Brussels (2005). ISBN: 9076971099
5. SECONOMICS website. http://www.seconomicsproject.eu
6. United States National Infrastructure Protection Plan (NIPP). http://www.dhs.gov/transportation-systems-sector