Designing a Cyber Attack Information System for National Situational Awareness

Florian Skopik, Zhendong Ma, Paul Smith, and Thomas Bleier

AIT Austrian Institute of Technology
Safety and Security Department
2444 Seibersdorf, Austria
firstname.lastname@ait.ac.at
http://www.ait.ac.at/it-security

Abstract. Information and communication technology (ICT) systems underpin many of today's societal functions and economic development. Consequently, protecting a nation's ICT infrastructure from deliberate cyber attacks and unintentional disruptions is of paramount importance. Collaboration among all parties across all domains of cyberspace is the key to effective and coordinated effort to cope with cyber threats. This is particularly the case as cyber threats become increasingly sophisticated and distributed. In this paper, we introduce the foundational building blocks to realize an efficient incident response cycle on a national level, and propose the design of a conceptual framework – the Cyber Attack Information System (CAIS) – for establishing national cyber situational awareness.

Keywords: cyber attack information system, situational awareness, national incident response, collaborative detection and response

1 Introduction

Information and communication technology (ICT) is of fundamental importance for our society and economy. For example, in Europe the most important factor for growth in productivity is the application of modern ICT [8]. ICT offers unique opportunities, but introduces a significant new vulnerability to a society that increasingly relies on electronic services. A deliberate or unintentional disruption as a result of technical or human failure, or due to natural causes could lead to social destabilization. As a consequence, IT security measures are rapidly being adopted in almost all areas utilizing ICT. However, the complexity and interconnectedness of modern ICT facilities and the rise of mobile data traffic and cloud computing pose further challenges to securing today's infrastructures.

A number of recent high-profile incidents have shown the vulnerability of critical infrastructures, which depend on ICT, to sophisticated cyber attacks. For example, the Stuxnet virus [9], explicitly designed to attack industrial process automation facilities, impressively demonstrated the vulnerability of critical infrastructures. Thorough analysis revealed that due to its complexity it must

have been developed or at least financed by a state; created to be used against another state. Furthermore, highly distributed botnets can cause major problems for national organizations and private enterprises, in many cases via denial of essential services. Distributed Denial of Service (DDoS) attacks were the main tactic used in the cyberattacks on Estonia in 2007 [15] and Georgia in 2008 [19] to paralyze a nation's ICT infrastructure.

In order to cope with such threats, we argue that tight cooperation between all parties in the digital society is necessary. In some domains, such as the banking sector, strategic alliances and public information sharing are already commonplace (e.g., to deal with phishing attacks [3]). Furthermore, there exist adhoc relationships between organizations, such as national Computer Emergency Response Teams (CERTs), to support collaborative incident response activities. However, these tend to be informally arranged between individual groups and are largely focused on securing infrastructures in the same operational domain. Whilst these activities have proven useful, a more comprehensive and formal approach to ensuring the security of national critical infrastructures, which spans numerous operational domains, will become necessary with the increasing use of ICT in interdependent critical infrastructure provisioning, e.g., as with Smart Grids.

In this paper, we discuss a number of foundational building blocks that can be used to realize an effective cyber incident response cycle on a national level, and propose the design of a conceptual framework – the Cyber Attack Information System (CAIS). The ultimate goal of this framework is to strengthen the resilience of today's interdependent networked services, and increase their overall availability and trustworthiness. The rationale for our framework is as follows:

- *Linking and coordinating existing initiatives*: important work performed by CERTs and other agencies need to be coordinated on a national level to tackle current and future sophisticated highly-distributed cyber threats.
- *Establishing situational awareness on a national level*: developing situational awareness is important for determining effective responses to cyber attacks, this needs to be done on a national level to fully understand any risks to our society's interdependent infrastructure.
- *Facilitating public-private partnerships*: interconnected national infrastructures, which are operated using numerous public-private partnerships, require a suitable intermediary in order to facilitate a national cyber incident response strategy.
- *Maintaining organizational responsibility*: it is essential that participants in a national cyber incident response initiative clearly understand their role, including obligations, and the interfaces with other organizations; these are outlined in our framework.
- *Activating inter-organizational collaboration*: essential to improving national resilience to cyber attacks is inter-organizational collaboration – our framework aims to facilitate this. A further benefit of such collaboration is a

decreased dependency on a national coordination point, which may be necessary or desirable in some cases.

The remainder of the paper is organized as follows. Section 2 introduces the notion of situational awareness and essential methods for its establishment. As mentioned earlier, developing situational awareness is critical in order to define well-informed and effective national cyber incident response strategies. Furthermore, Sect. 2 introduces an extended incident response cycle, which underlies our CAIS framework and supports the development of situational awareness. Section 3 highlights the basic stakeholders in the framework and their associated responsibilities. Subsequently, Sect. 4 outlines the high-level CAIS architecture and a mapping to organizational roles in order to implement the framework. The purpose of the architecture is to inform potential participants in a future national CAIS of the activities they need to undertake, the interfaces they must support, and the kinds of data they need to maintain. Furthermore, the architecture can be used to understand the human resources necessary to support the CAIS framework. Related work and international initiatives are presented in Sect. 5. Section 6 concludes the paper.

2 Situational Awareness for Incident Response

Central to taking an informed and coordinated approach to cyber security incidents is determining Situational Awareness (SA). A number of models of SA exist [6][10][16], but arguably the most pervasive is that proposed by Endsley [6], which describes three increasing levels of awareness: *perception*, *comprehension*, and *projection*. As one advances through these levels, decision making capabilities are improved.

Previous work from the EU-funded ResumeNet project proposed a mapping of information sources and mechanisms to the first two levels of SA [17] for identifying *challenges*, e.g., attacks, to computer networks. It is proposed there are two key sources of information for situational perception: *(1) multilevel network measurement information* and *(2) context information*, which is external to the network under scrutiny, such as news items about an ongoing situation. These two forms of information – network and context – are used as inputs to various techniques that are used to build situational comprehension. There are three proposed main approaches to comprehension: *(1)* detection of the presence of a challenge, e.g., provided by anomaly and intrusion detection systems; *(2)* identification of the characteristics of the challenge, e.g., provided by classification [14] and data fusion [18] techniques; and *(3)* the impact an attack is having on the network and associated services. Situational projection, which was not addressed by the ResumeNet project, estimates possible future situations, such as the continued behaviour and impact of a cyber attack. A way to approach determining situational projection is via the continued simulation of an ongoing cyber security incident, using output (data and events) from perception and comprehension mechanisms to drive the simulation. To support this process, we propose the use of an extended incident response cycle.

In short, we distinguish a preventive (green) and reactive (red) phase in our extended incident response cycle, as depicted in Fig. 1. While the preventive phase focuses on identifying and characterising potential attacks and the deployment of sustainable defence mechanisms, the reactive phase deals with short-term counter measures to tackle those that are ongoing.

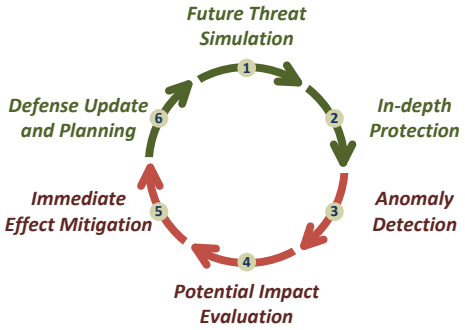

Fig. 1. Incident response cycle incorporating modeling and simulation phases.

The cycle starts with the creation of an infrastructure model and simulation of potential threats and future attacks (①). The infrastructure model is created with information collected from organizations that are participating in the proposed national CAIS framework – such information is typically maintained in asset management systems. The threats to be simulated are identified in a number of ways, such as from databases managed by CERTs and by using threat and vulnerability analysis techniques. The outcome of these simulations is an understanding of the potential impact of attacks and how they may manifest. Based on the simulation findings, which can form an input to a suitable risk assessment process, the deployment of mechanisms for an in-depth protection is performed in the next step (②). In particular, this should include mechanisms for enabling situational perception and comprehension, as discussed earlier. A key addition, in order to participate in the national CAIS, are interfaces to enable exporting of monitoring data and alarms generated by the various mechanisms used for situational comprehension. Once an anomaly, such as an attack, is detected (③), its potential impact on the whole infrastructure is evaluated using models and the simulation from the first step (④). The aim of these simulations is to *project* how an anomaly may continue to manifest across the institutions participating in the CAIS, and determine its potential impact. Studying potential effects allows for informed and targeted counter measures in order to mitigate negative effects (⑤). After a current attack has been successfully repelled, the basic security plans and measures must be updated (⑥) to ensure preparedness for future threats. This phase closes the cycle. Based on this extended incident response cycle, we can derive a number of responsibilities for the organizations that participate in the CAIS.

3 CAIS Stakeholder Responsibilities

The basic principle to establishing situational awareness on a national level, and consequently deriving a national cyber incident response strategy, relies on collecting information from single organizations that are involved in running critical infrastructures. Stakeholders, being *single organizations* or a *national cyber defence centre*, have numerous responsibilities, as discussed here.

3.1 Responsibilities of Single Organizations

A single organization in the CAIS framework can include entities such as banks, utility providers, telecommunication network providers, and so on. Collectively, they provide the ICT-coupled critical infrastructures our society depends on, and have a number of responsibilities in the CAIS:

1. *Asset Management*, i.e., knowing what hardware and software is deployed and the design of their own infrastructure, is essential since this is the basis for determining vulnerabilities of certain organizations.
2. *Infrastructure Monitoring* is about the thorough observation and logging of own network traffic reflected by e.g., firewall logs, proxy logs, DNS queries. This is the basis for discovering and tracking anomalies which can be potentially caused by ongoing attacks.
3. *Organization-wide Anomaly Detection* through aggregation, correlation, and analysis of distributed network logs from various devices, services, and components is required to respond on a local level to identified exploits.
4. *Local Incident Response* deals with the deployment of immediate counter measures once an attack has been detected in order to mitigate the effects as fast as possible.
5. *Reporting to the National Cyber Defence Centre* enables the establishment of situational awareness on a larger scale. Besides actually identified attacks and threats, also relevant asset configurations need to be reported so that the Cyber Defence Centre can estimate an organizations's vulnerability to identified attack vectors.

Complementary to organizations that provide critical national infrastructures are those that provide security-related tools and information, such as CERTs and security enterprises (antivirus software companies, for example). Their role within the CAIS is typically to fulfil responsibilities two to five in the list above. Furthermore, they can support critical infrastructure providers with their participation in the CAIS.

3.2 Responsibilities of the National Cyber Defence Centre

We propose that a national cyber defence centre should collate information from single organizations, develop country-wide situational awareness, and provide guidance on how to respond to incidents. The national cyber defence centre is

intended to act as a trusted third-party and coordinate activities between public-private organisations, for example. Correspondingly, the national cyber defence centre has a number of responsibilities:

1. *Collective Asset Management* aggregates asset information from all involved organizations. This is a vital aspect, e.g., for the estimation of the effects of spreading malware or for goal-oriented planning of counter measures.
2. *Centralized Report Collection and Evaluation* enables the cyber defence centre to be informed about the ICT states of single organizations and with what anomalies they have to deal with.
3. *Complex Attack Simulations* are used to evaluate the causes and effects of certain attacks. These simulations use infrastructure models created from asset management data and further account for the organizational states according to their most recent reports. This way, the impact of ongoing attacks can be identified on a national level (this is particularly important for dealing with coordinated attacks) as well as various scenarios for counter measures tested before they are even deployed.
4. *Establishing Situational Awareness* by combining (i) data sent from single organizations, (ii) intelligence data gathered from simulations, and (iii) coordination with international cyber centres (similar as CERTs do today)
5. *Planning Coordinated Counter Measures* deals with finding an effective way to mitigate the impact of ongoing attacks; and finally helps to re-establish a normal state of operation.
6. *Policy-based Advice and Recommendation* are the means to inform attacked organizations (and also potential future targets) how to reconfigure, update, or reshape their network and components in order to close open vulnerabilities, and thus, harden their infrastructure.

4 A Cyber Attack Information System Architecture

Building on the extended incident response cycle presented in Sect. 2 (which faciltitates the development of Endsley's three levels of SA), and the stakeholders and their roles that are identified in Sect. 3, we have developed a high-level architecture for a national cyber attack information system. The CAIS architecture, shown in Fig. 2, describes the flow of information and activities that are undertaken to implement two incident response cycles within a single organization and nationally within the cyber defence centre. Furthermore, the architecture identifies the necessary data repositories that are required to support the activities and information flow, along with the interfaces between the various stakeholders in the CAIS. Next, we briefly summarise the operation of the organizational and national aspects of the architecture, then we identify the necessary human resource roles, including the competencies and tasks, that must be filled to realise the architecture.

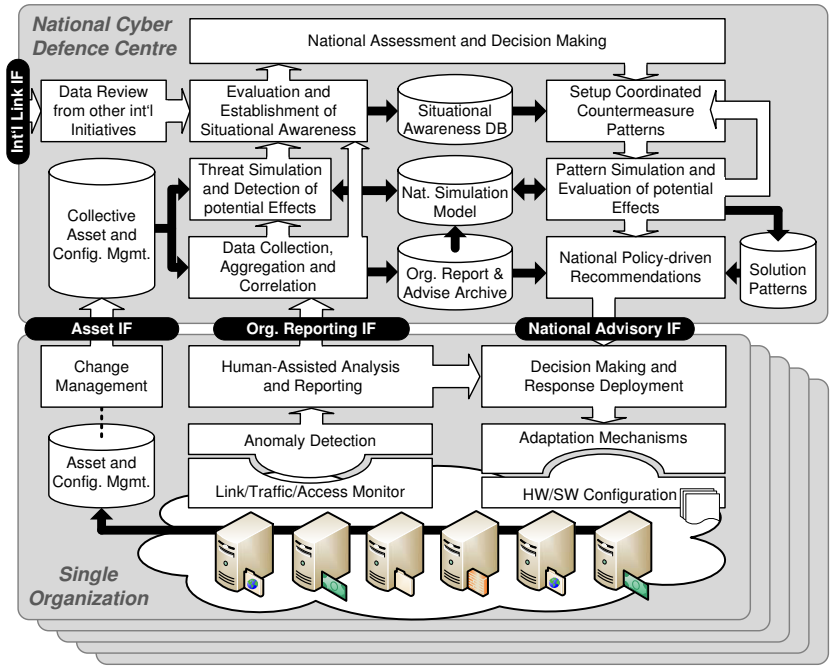

Fig. 2. High-level architecture for a national CAIS

4.1 CAIS Architecture – Organizational Level

Every organization essentially runs its own infrastructure to support their business processes. Monitoring links, traffic and service accesses is state-of-the-art of IT administration. In case of (mostly automatically) detected anomalies (e.g., a triggered alarm of an intrusion detection system), a human-assisted analysis is performed to, first, find out if an attack is going on at all, and second, which services are concerned. Based on these investigations, a decision for solving these issues is reached by a security manager and counter measures deployed by security administration staff. Here, hardware or software is adapted or reconfigured.

While such an incident response cycle in one form or another is usually applied today in every professional IT environment, we foresee an extension to integrate with our CAIS approach. Here the results of the human-assisted analysis need to be reported to the defence centre, where reports from participants all over the nation are collected. Additionally, to help address locally identified anomalies, feedback and advice from the defence centre is considered in the decision phase.

4.2 CAIS Architecture – National Level

The national cyber defence centre applies a higher-level version of the cycle introduced in Fig. 1 – in addition to the single-organization cycles. It collects

reports about detected anomalies and identified attacks from single organizations (via the `Org. Reporting IF`). Using this intelligence data, a nation-wide threat simulation (on an abstract level) is used to assess potential effects of ongoing attacks – not only for a single enterprise but spanning numerous interconnected organization and domains. An approach to realising the national simulation is to use an agent-based simulator [13], which can model autonomous, interacting agents, such as the organizations in our CAIS. The simulation model captures the rough organizational assets and their interdependencies (using the `Asset IF`) in order to enable the identification of cascading effects and estimation of rolling breakdowns. This is important input for the evaluation of situational awareness and ultimately, for national decision making. Decisions include, for instance, to extend/fund backup systems of a frequently attacked organization providing a critical service. Decision are evaluated by applying changes to the simulation model and running simulations from previous attacks. Therefore, the improved resilience of the whole infrastructure can be evaluated and finally, the

Table 1. Organizational and national roles in the framework.

Role	*Competencies and tasks*
Network Op. Centre (NoC)	Running the technical infrastructure; monitoring the operational state; anomaly detection; deploying counter measures on advise
Security Team	Human-assisted threat analysis; incident reporting to the Chief Security Officer and the Organizational Report PoC (see below)
Chief Security Officer	Decision making; keeping an overview of the operational status of the organization
Head of IT	Decision making together with Chief Security Officer; processing recommendations from the Advisory PoC from the National Defence Centre
Organizational Report PoC	Collecting reports from single organizations, maintaining a public-private partnership; optionally stay in touch with international initiatives
Data Analyst	Reviewing, aggregating and correlating reports; maintain an up-to-date data base of organizations' identified attacks
Simulation Task Force	Large-scale infrastructure simulation; making forecasts and predictions; feed the situational awareness model; evaluation of counter measures (solution patterns)
National Security Council	National decision making about the strategic evolution of the IT infrastructure on a higher level
Advisory Point of Contact	Advise heads of IT in single organizations in order to realize the evaluated counter strategy to an identified threat
National Asset Management	Requesting asset information from single organizations; keeping an overview about critical assets

strategy with the best value for money is propagated to concerned organizations (using the `National Advice IF`).

4.3 Roles, Interactions and Information Exchange

In order to implement the CAIS framework, we need to map tasks and responsibilities onto dedicated roles. For that purpose, Table 1 describes mandatory roles (i) to realize fast incident response within an organization, (ii) to enable long-term strategic evolution of the IT infrastructure from a national perspective, (iii) to manage national assets, which is an essential input for simulation and risk assessment.

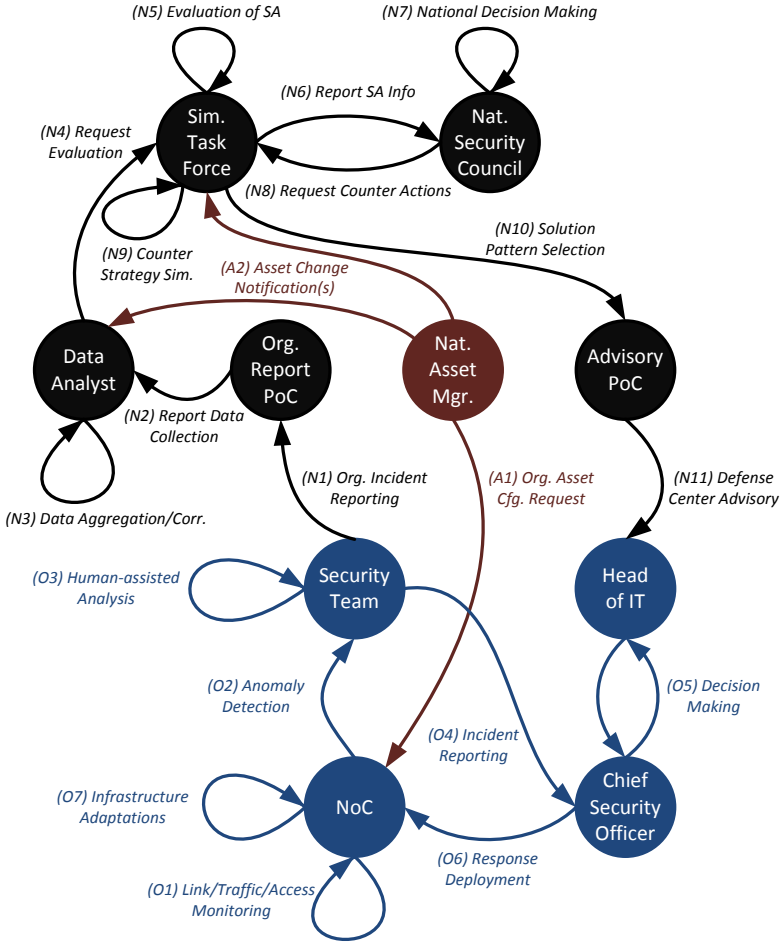

Fig. 3. Sequential steps for incident response: *(O)*rganizational level, *(N)*ational level, and *(A)*sset management.

Furthermore, Fig. 3 depicts the relationships between these roles and how a detected incident within an organization is propagated. The starting point is at the Network Operation Centre which monitors infrastructure links, traffic, and service accesses (*O1*). All blue elements represent actions within an organization (*O1* to *O7*), including monitoring, anomaly detection, incident reporting, decision making, response deployment and optional infrastructure adaptations. The black elements reflect roles and interactions in the cyber defence centre (*N1* to *N11*), such as the collection of reports from all single organizations, aggregation and correlation of data, evaluation of situational awareness, informing of decision makers and decision making itself, requesting counter actions, counter strategy simulation, solution pattern selection, and defense centre advisory provisioning. The National Asset Management (in red) is part of the defence centre, however it provides the Data Analyst and Simulation Task Force (*A1* to *A2*) with essential data about infrastructure assets (e.g., deployed hardware and software in the single organizations).

5 Related Work

As ICT systems are being applied in a greater number of critical areas, cyber attacks are becoming more frequent and have an increasing impact (see [12] for a list of reports on cyber security and cyber attacks). Situational awareness plays an important role in the defence and survival of ICT infrastructures amid a cyber attack. Attack detection relies on cyber sensors, such as intrusion detection systems (IDS), log file sensors, anti-virus systems, malware detectors, and firewalls [11]. Many of the sensor techniques used today are based on sophisticated anomaly detection techniques, i.e., finding non-conforming patterns in data [5]. The results from various research fields, such as data mining, statistical analysis, machine learning, as well as information theory are applied to anomaly detection.

Since many of the attack detection tasks are performed at a local level, within a single organization, such as an Internet Service Providers (ISP), cross-domain security information sharing is a crucial step to correctly understanding the situation for national cyber defence. However, in practice, security information sharing is usually accomplished via ad-hoc and informal relationships [20]. Often, national Computer Emergency Response Teams (CERTs) assume the role of national contact points for coordinating and aggregating security incidence reports via communication channels such as email, instant messaging, file exchange/storage, VoIP, IRC and the Web [7]. Other means exist for information sharing. Internet forums such as the Internet Storm Center from SANS [2] collect and provide data about malicious activities on the Internet. Commercial service providers, such as Arbor Networks [1], offer network-wide threat information updates and analysis services.

Although many of the existing efforts contribute to a better understanding and response in light of cyber attacks, many technical and organizational challenges remain for establishing a national situational awareness infrastruc-

ture. As situational awareness is multi-faceted and multi-disciplinary, a holistic framework is needed to ensure systematic development and cooperation. The architecture proposed in this paper provides such an overview on the building blocks which contribute to reaching this goal.

6 Conclusion and Future Work

Because of the increasingly sophisticated and distributed nature of cyber attacks, e.g., that use botnets as a platform, and our dependence on ICT-coupled critical infrastructures, a coordinated multi-domain approach to cyber incident response is required. This paper has introduced the building blocks in the form of a framework to realize an incident response cycle and a design of a cyber attack information system (CAIS) for establishing situational awareness to strengthen the resilience and trustworthiness of today's national ICT infrastructure. Our design aims at linking existing initiatives, maintaining organizational responsibility, and activating inter-organizational collaboration on a national level.

The cyber attack information system introduced in this paper is the first step towards establishing national cyber situational awareness. In order to reach this goal, the following major open research challenges need to be addressed: (i) secure and privacy-preserving data sharing across organizational boundaries (for example, building on secure multi-party computation (MPC) approaches [4]); (ii) methodologies and techniques for efficient and scalable data synthesis and processing, and information reasoning to generate full situational awareness; (iii) evaluation of proven techniques on hypothesis and reasoning for projection and decision making under high uncertainty.

Acknowledgments

This work was partly funded by the Austrian security-research programme KIRAS and by the Austrian Ministry for Transport, Innovation and Technology.

References

1. Arbor networks. `http://www.arbornetworks.com/`
2. Internet storm center. `http://isc.sans.org/`
3. Phishtank. `http://www.phishtank.com/`
4. Burkhart, M., Strasser, M., Many, D., Dimitropoulos, X.: SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics. In: USENIX Security Symposium. Washington, DC, USA (August 2010)
5. Chandola, V., Banerjee, A., Kumar, V.: Anomaly detection: A survey. ACM Comput. Surv. 41(3) (2009)
6. Endsley, M.: Toward a theory of situation awareness in dynamic systems. Human Factors 37(1), 32–64 (1995)
7. ENISA: Practical guide/roadmap for a suitable channel for secure communication: secure communicatio with the CERTs & other statkeholders (December 2011)

8. EU Press Release IP/07/453: ICT drives 50% of eu growth, says commission's annual report on the digital economy (2007)
9. Falliere, N., Murchu, L.O., Chien, E.: W32.Stuxnet Dossier. Tech. rep., Symantic Security Response (Oct 2010)
10. Fracker, M.: Measures of situation awareness: Review and future directions. Tech. Rep. AL-TR-1991-0128, Wright-Patterson Air Force Base, OH: Armstrong Laboratories (1991)
11. Jajodia, S., Liu, P., Swarup, V., Wang, C.: Cyber Situational Awareness: Issues and Research. Springer Publishing Company, Incorporated, 1st edn. (2009)
12. Lewis, J.A.: Selected bibliography for cyber security. `http://csis.org/publication/selected-bibliography-cyber-security`
13. Macal, C.M., North, M.J.: Tutorial on agent-based modelling and simulation. Journal of Simulation 4, 151–162 (2010)
14. Nguyen, T.T.T., Armitage, G.J.: A survey of techniques for internet traffic classification using machine learning. IEEE Communications Surveys and Tutorials 10(1–4), 56–76 (2008)
15. Ottis, R.: Analysis of the 2007 cyber attacks against estonia from the information warfare perspective. In: Proceedings of the 7th European Conference on Information Warfare. p. 163. Academic Conferences Limited (April 2008)
16. Sarter, N., Woods, D.: Situation awareness: A critical but ill-defined phenomenon. International Journal of Aviation Psychology 1, 45–57 (1991)
17. Smith, P., Hutchison, D., Sterbenz, J.P.G., Schöller, M., Fessi, A., Doerr, C., Lac, C.: D1.5c: Final strategy document for resilient networking. ResumeNet Project Deliverable (August 2011), `http://www.resumenet.eu`
18. Tadda, G., Salerno, J.J., Boulware, D., Hinman, M., Gorton, S.: Realizing situation awareness within a cyber environment. In: Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications. Orlando, FL, USA (April 2006)
19. Tikk, E., Kaska, K., Rnnimeri, K., Kert, M., Talihärm, A.M., Vihul, L.: Cyber attacks against georgia: Legal lessons identified (Novermber 2008), `http://www.carlisle.army.mil/dime/getDoc.cfm?fileID=167`
20. U.S. Homeland Security Cyber Security R&D Center: A roadmap for cybersecurity research (November 2009)