Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Cyber situational awareness – A systematic review of the literature

Ulrik Franke[*], *Joel Brynielsson*

FOI Swedish Defence Research Agency, SE-164 90 Stockholm, Sweden

ARTICLE INFO

Article history:
Received 5 February 2014
Received in revised form
17 April 2014
Accepted 23 June 2014
Available online 3 July 2014

Keywords:
Situational awareness
Cyber security
National cyber strategies
Research strategy
Literature review

ABSTRACT

Cyber situational awareness is attracting much attention. It features prominently in the national cyber strategies of many countries, and there is a considerable body of research dealing with it. However, until now, there has been no systematic and up-to-date review of the scientific literature on cyber situational awareness.

This article presents a review of cyber situational awareness, based on systematic queries in four leading scientific databases. 102 articles were read, clustered, and are succinctly described in the paper. The findings are discussed from the perspective of both national cyber strategies and science, and some directions for future research are examined.

1. Introduction

"Cyber" issues are attracting evermore attention, worldwide. For example, renowned analysis firm Gartner explains how in 2013 awareness about gaps in cyber security defenses was heightened, and predicts that in 2014, governments will expand cyber security regulations (Walls, 2014). Cyber security strategies – government (Nissenbaum, 2005; Lynn III, 2010), private sector (Rowe and Gallaher, 2006) and power grid (Ericsson, 2010) – are subject to well-cited scholarly research. An increasing number of countries including the UK (Government of the UK, the Cabinet Office, 2011), the US (The White House (signed by President Barack Obama), 2011), Canada (Government of Canada, Public Safety Canada, 2010), Australia (Australian Government, Attorney-General's Department, 2009), Estonia (Cyber Security Strategy Committee, Ministry of Defence, 2008), Japan (National Information Security Center, 2013), France (Agence nationale de la sécurité des systèmes d'information (ANSS), 2011), Germany (Federal Ministry of the Interior, 2011), Finland (Secretariat of the Security Committee, 2013), the Netherlands (National Coordinator for Security and Counterterrorism, 2013) and Russia (The Federation Council, 2014) have adopted or are in the process of adopting cyber or cyber security strategies. Although these strategies are not always in agreement – as shown e.g. by Giles and Hagestad (2013) – they do have substantial priorities in common, e.g. the need to protect critical information infrastructures and the need to develop or enhance "situational awareness".

Situational (or situation) awareness is traditionally defined following the seminal work of Endsley (1988). The situational awareness underpinnings will be further discussed in the next section in order to put the study into context. It is, however, clear that this is a kind of capability that is sought by governments, enterprises and other stakeholders with respect to

* *Corresponding author*. Tel.: +46 855503504.
E-mail addresses: ulrik.franke@foi.se (U. Franke), joel.brynielsson@foi.se (J. Brynielsson).
http://dx.doi.org/10.1016/j.cose.2014.06.008

their information and control systems. Quoting examples from the strategies mentioned above, the Australian Cyber Security Operations Centre (CSOC) "provides the Australian Government with all-source cyber situational awareness and an enhanced ability to facilitate operational responses to cyber security events of national importance" (Australian Government, Attorney-General's Department, 2009). The US claims to be "making steady progress towards shared situational awareness of network vulnerabilities and risks among public and private sector networks" (The White House (signed by President Barack Obama), 2011). The most important service of the Finnish Cyber Security Centre is "to compile, maintain and distribute the cyber security situation picture to those who need it" (Secretariat of the Security Committee, 2013). To ensure security in cyberspace, France wishes to "[e]ffectively anticipate and analyse the environment in order to make appropriate decisions" (Agence nationale de la sécurité des systèmes d'information (ANSS), 2011). To identify and manage cyber attacks, Estonia concludes that "the efficiency of network traffic monitoring and the ability to perform strategic and tactical analyses should also be improved" (Cyber Security Strategy Committee, Ministry of Defence, 2008). The German National Cyber Response Centre is tasked to alert the federal authorities whenever "the cyber security situation reaches the level of an imminent or already occurred crisis" (Federal Ministry of the Interior, 2011). The Canadian Cyber Incident Response Centre is tasked "to monitor and provide mitigation advice on cyber threats, and coordinate the national response to any cyber security incident" (Government of Canada, Public Safety Canada, 2010). The UK Cyber Security Strategy makes it a priority for action both to "continue to improve our detection and analysis of sophisticated cyber threats" and to "pool knowledge and situational awareness as appropriate with partners across business to build a genuinely national response" (Government of the UK, the Cabinet Office, 2011). In the Netherlands, the same trend is visible as the National Cyber Security Centre develops a "stronger structure for confidential information-sharing and analysis" and develops from a CERT "into a Security Operations Centre" (National Coordinator for Security and Counterterrorism, 2013). In the Japanese strategy, "improving the recognition and analysis functions for incidents related to cyber attacks, integrating these functions, advancing threat analysis capabilities by promoting information sharing, strengthening of cooperation between CSIRT for each actor and between international CSIRT" are listed as critical actions (National Information Security Center, 2013). The Russian draft strategy calls for "the development of a government system for detection, warning and mitigation of cyber attacks on the information resources of the Russian Federation" (The Federation Council, 2014, our translation). It is clear that cyber situational awareness is very much in demand at the top strategic level.

However, despite this surge in attention, there is no good systematic review of the scientific literature when it comes to cyber situational awareness. The best overview of the subject is Jajodia et al. (2010), an edited volume. While a good introduction, it does not address all issues, and a large body of research has been produced since its publication. There are also a few more narrow literature reviews focusing e.g. on information fusion using the JDL model (Schreiber-Ehle and Koch, 2012) or visualization for computer security (Goodall, 2008). Clearly, these specialized reviews do not fully cover the whole cyber situational awareness field. This article aims to set this straight.

More specifically, this article was written as part of an effort to create a research agenda in the area of cyber situational awareness. The idea is that a good review of the existing literature makes it easier for researchers and decision-makers to get an overview of which areas are well-researched, are researched but could become more mature, or remain more or less unexplored. Such information is valuable input to anyone who wishes to create a research agenda.

1.1. *Outline*

This article unfolds as follows. Section 2 defines the term "cyber situational awareness" for the purposes of this article and places it in context. Section 3 outlines the method used in the literature review. Section 4 contains the main contribution: a survey of published scientific articles on cyber situational awareness, organized in eleven thematic clusters. The findings are discussed in Section 5, and Section 6 concludes the article.

2. Situational awareness and its relation to cyber security

In this section we elaborate on the notion of "cyber situational awareness", and describe the perspective taken in the article. The purpose of the section is to provide a theoretical framework, and to narrow down the target of the literature study.

Situational awareness is a multifaceted and well-studied phenomenon, which can be looked upon from several different perspectives (Brynielsson, 2006, pp. 15–17). From a technical viewpoint, situational awareness comes down to compiling, processing, and fusing data. Such data processing includes the need to be able to assess data fragments as well as fused information and provide a rational estimate of its information quality (Arnborg et al., 2000). This, in turn, makes it possible to technically relate and evaluate pieces of information relative to each other. In contrast, the cognitive side of situational awareness concerns the human capacity of being able to comprehend the technical implications and draw conclusions in order to come up with informed decisions. Cognitively it is therefore interesting to measure to what extent a human decision-maker is aware of the situation, i.e., has reached a certain level of situational awareness, and how well he/she manages to maintain and develop this awareness as time progresses. The widely applicable situational awareness definition given by Endsley (1988) can be used as a basis for such measurement. This definition describes situational awareness cognitively as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future". As suggested by Endsley (1995), the words "perception", "comprehension", and "projection" can be taken to denote progressively increasing awareness levels ranging from (i) basic perception of important data, (ii) interpretation and combination of data into knowledge, and (iii) ability to predict future events and their implications. Studies

have shown that the ability to develop and maintain a high level of situational awareness vary significantly between people and tasks (Endsley, 2000).

Situational awareness by necessity involves both technical and cognitive challenges in that the basic data used for developing situational awareness consists of some kind of underlying estimate of the state of the world which, in turn, is the result of some kind of data processing. In command and control applications for crisis management, military planning, etc., the data used to develop situational awareness is the result of data fusion, i.e., "the process of combining data to refine state estimates and predictions" (Steinberg et al., 1999). Put simple, data fusion is the core technology for fusing large amounts of data into comprehensible information, and a requirement for developing the technical decision support systems that ultimately serve to help a decision-maker gain and further develop a high degree of situational awareness. Hence, for the command and control case it follows that the technical and cognitive sides of situational awareness are closely related and somewhat intertwined.

As described in the preceding paragraphs, we think of situational awareness primarily as a mental state that can be reached to a varying degree. Within the scope of this article, this is the foundation for how we define and interpret *cyber situational awareness*. We take cyber situational awareness to be a subset of situational awareness, i.e., cyber situational awareness is the part of situational awareness which concerns the "cyber" environment. Such situational awareness can be reached, e.g., by the use of data from IT sensors (intrusion detection systems, etc.) that can be fed to a data fusion process or be interpreted directly by the decision-maker. Such situational awareness can also be reached by more traditional sensors, such as an insider informant leaking information about an imminent cyber attack. It is important to note that cyber situational awareness cannot be treated in isolation, but is intertwined with and a part of the overall situational awareness. Although cyber situational awareness indeed concerns awareness regarding cyber issues, these cyber issues need to be combined with other information to obtain full understanding regarding the situation. Hence, cyber events offer additional insight about the overall situation, not about a disjoint cyber situation. Indeed, events in the physical world offer additional sensors providing insight regarding the cyber situation. That is, the combination of information from different arenas makes way for insight regarding the cyber situation so that, e.g., the combination of a cyber sensor (such as an IDS alarm) and an ordinary sensor (such as a human intelligence report) contribute to enhancing the overall cyber situational awareness.

It follows that cyber situational awareness includes awareness of, e.g., any kind of suspicious/interesting activity taking place in cyberspace, where cyberspace includes any kind of computer network-related activity. Such suspicious/interesting activity can take place at all levels in the TCP/IP stack and might range from low-level network sniffing to suspicious linguistic content on social media. The detected network activity provides insight in its own right, and also serves as additional information to be fused along with ordinary state parameters in order to provide basic data for obtaining overall situational awareness.

In this literature study, cyber situational awareness is studied from the perspective that situational awareness serves to enhance sensemaking, i.e., the perspective taken is that new cyber sensors can contribute to situational awareness for the purpose of understanding what needs to be done in terms of the desired effects and the actions that ought to be undertaken to achieve these effects (Weick et al., 2005). Taking this perspective, the information infrastructures that cyber situational awareness targets can be related to two distinguishing contexts, namely routine operational work in an organization (e.g., everyday production), and command and control work related to a specific situation (e.g., crisis management).

3. Method

In order to capture a reasonably full range of the literature on cyber situational awareness, literature searches were conducted in July 2013 using four scientific databases. In each case, the search query "cyber situational awareness" was entered, with no temporal limitation. Such a query (without quotation marks) typically also returns some variations, where the search engine allows for permutations and inflections. The initial results were as follows:

IEEE Xplore returned 53 results. The database covers electrical engineering, computer science and electronics, and indexes more than 160 journals and 1 200 conference proceedings.

Scopus returned 97 results. The database claims to be "the largest abstract and citation database of peer-reviewed literature", indexing 20 000 peer-reviewed journals and 5.5 million conference papers.

Springer link returned 298 results. The database contains journals and conference proceedings published by the Springer publishing house, and indexes over 8.3 million scientific documents.

Web of Science returned 44 results. The database covers over 12 000 of the high impact journals and over 150 000 conference proceedings.

As an initial screening, titles and abstracts were read and a number of clusters were manually identified. The list of these clusters can be seen as a very general description of the research area, and comprises the following:

- General cyber situational awareness
- Cyber situational awareness for industrial control systems (mostly the power grid)
- Cyber situational awareness for emergency management
- Tools, architectures, and algorithms for cyber situational awareness
- Information fusion
- Visualization for cyber situational awareness
- Human-computer interaction, design specifications and work flows for cyber situational awareness
- Nation-wide, large scale cyber situational awareness
- Exercises relating to cyber situational awareness
- Information exchange for cyber situational awareness
- Military cyber situational awareness

Following this initial analysis, a review form was iteratively constructed by the authors. The aim was to cover the most

relevant aspects of the research. Apart from title, authors, and a free text field for additional comments, the following 21 questions were used:

Application area of results

1. Does the work assume one or more specific application areas for the network?
2. Is the resulting application aimed at cyber situational awareness in control systems (SCADA)?
3. Is the resulting application aimed at cyber situational awareness in civilian or military command and control networks (crisis management, operational or tactical command)?
4. Is the resulting application aimed at cyber situational awareness in organizational operations management networks (e.g. intranets)?

The application area questions were inspired by the most prominent areas featured in the initial screening.

Threat description

5. Is there a threat description (an attack purpose) described or discussed in greater detail than just general remarks in the introduction?
6. Is the threat description mostly about espionage – i.e. covert copying and reading information?
7. Is the threat description mostly about dissemination of information – i.e. copying and making information public?
8. Is the threat description mostly about degrading information availability – i.e. DoS attacks or obscure networking errors?
9. Is the threat description mostly about degrading information integrity – i.e. to change or destroy application information?

The threat description is inspired by the traditional confidentiality – integrity – availability model of information security, breaking confidentiality into two versions: the narrow (e.g. espionage) and the broad (e.g. whistleblowing). Overall, questions 1 through 9 relate to the research areas and can thus be compared to the areas prioritized in the national strategies.

Proposals and experiments – methodology and technology

10. Is the report based on a design (or idea for a design) pertaining to method, technology etc. to achieve cyber situational awareness or for part of a system to achieve cyber situational awareness?
11. Is the report based on an implementation of a method, technology etc. to achieve cyber situational awareness or for part of a system to achieve cyber situational awareness?
12. Does the report contain a non-trivial empirical contribution?
13. Is the article about methodology or technology for visualization (what and/or how), user interaction and/or usability?
14. Is the article about methodology for a cyber situational awareness workflow?
15. Is the article about methodology or technology for detection/analysis of adversarial network activity?
16. Is the article about methodology or technology for battle damage assessment?
17. Is the article about methodology or technology for identifying the adversary and the purpose of his actions?
18. Is the article about using current cyber situational awareness to project a situation into the future?

The final question is inspired by Endsley's definition. Overall, questions 10 through 18 relate to methods and level of maturity of the research studied.

Other

19. Is the article about training operator or analyst training?
20. Is the article a review article?
21. Is the article written on a "meta" level (e.g. strategies, what should be researched)?

The resulting odd 500 articles, however, were not without overlap. Many articles were found several times in different databases. Furthermore, a number of articles were deemed irrelevant in light of the delimitation made in Section 2 when manually screened. These typically addressed situational awareness *aided* by computers, e.g. geospatial sensors for environmental decision-support, but not situational awareness *about* computer network systems. As a consequence, these works were removed from further consideration. All in all, 102 articles were subject to analysis in terms of the 21 questions. The results of this review are detailed in the next section.

4. Results

Some quantitative measures of the articles reviewed are presented in Table 1. It should be noted that the categorizations used are not mutually exclusive: e.g. there are a few articles that address both threats to confidentiality and availability, and indeed every article addressing integrity also addresses availability. Most articles, however, belong to single application and threat categories.

Regarding threats, it is worth observing that there is a marked tilt favoring availability (17 articles) over confidentiality (5 + 3 articles) and integrity (7 articles). Further investigation reveals that this is related to the ICS application area: the overlap between the 17 articles that focus on ICSs and the 17 articles that focus on threats to availability is 10 articles. This is a marked contrast to the other application areas, where just a single article (command & control) or no articles at all (operations management) also offer a clear threat description. The articles addressing the different facets are listed in Table 2.

It is not surprising to see that the number of design concepts is greater than the number of actually implemented designs, which is again greater than the number of articles that actually contains a non-trivial empirical contribution. However, it should be noted that empirical contribution has been interpreted in a rather inclusive way, so that it includes not only results based on data from experiments or archival studies, but also e.g. mathematical proofs, results from

Table 1 – Characteristics of the 102 articles reviewed. Note that the categorizations used are not mutually exclusive.

	Number of articles
Application area	
Industrial control systems (ICS)	17
Command & Control	15
Operations management	7
Threat description	
Threat: Confidentiality, narrow	5
Threat: Confidentiality, broad	3
Threat: Availability	17
Threat: Integrity	7
Experiments, methodology, technology	
Design	76
Implementation	56
Empirics	45
Visualization	24
Workflow	28
Attack detection & analysis	60
BDA	16
Attacker ID & purpose	12
Project into the future	15
Other	
Training	7
Review	8
"Meta"	2

simulations, informed reasoning about computational complexity etc. Thus, while having a design idea and an implementation of it is not strictly a precondition to having a non-trivial empirical contribution, in fact 33 out of 45 articles with empirical contribution also do have a design idea and an implementation.

The three categories Battle Damage Assessment, Attacker ID & purpose, and Project into the future are particularly interesting, as in a sense they reflect the most refined version of cyber situational awareness: knowing what is happening, who is doing it, and what will happen next. (The fact that these are the smallest categories in the Experiments, methodology, technology section also suggests that they might be non-trivial to achieve.) The articles addressing these issues are listed in Table 3.

As stated in the introduction, there is no existing review article with the same coverage as ours. However, our literature search certainly found review articles for related areas. These are listed in Table 4.

In the following, each of the 11 cluster categories (cf. Section 3) is presented in greater detail along with a few remarks regarding implications for situational awareness and/or national cyber strategies. While all of the 102 articles reviewed are not cited below, the aim has been to include a reasonably representative sample of articles in each category.

4.1. *General cyber situational awareness*

This category includes much of the introductory literature on cyber situational awareness, e.g. chapters from the edited volume by Jajodia et al. (2010) on definitions and concepts (Barford et al., 2010b), risk assessment (Liu et al., 2010), human cognition (Yen et al., 2010), and analysis methods for finding software vulnerabilities (Sezer et al., 2010).

Apart from these texts, there is also a number of works concerned with network traffic scanning, focusing on the

Table 2 – Articles addressing the different threat facets. C = confidentiality, A = availability, I = integrity.

Article	C, narrow	C, broad	A	I
King et al. (2012)	X			
Greitzer and Frincke (2010)	X		X	
Brunner et al. (2011)	X	X		
Mahoney et al. (2010)	X	X		
D'Amico et al. (2007)	X	X	X	X
Alcaraz and Lopez (2013)			X	X
Sheldon et al. (2013)			X	
Ross et al. (2013)			X	
Mavridou and Papa (2012)			X	
Garlapati and Shukla (2012)			X	
Valdes and Cheung (2009)			X	X
Ten et al. (2008)			X	X
Alcaraz and Lopez (2012)			X	
Hennin (2008)			X	
Ghanea-Hercock et al. (2007)			X	
Rice et al. (2011)			X	
Gagnon et al. (2010)			X	
Michel et al. (2011)			X	X
Kopylec et al. (2007)			X	X
D'Amico and Salas (2003)			X	X

Table 3 – Articles addressing the issues Battle Damage Assessment, Attacker ID & purpose, and Project into the future.

Article	BDA	Attacker	Future
Cheng et al. (2012)		X	
Morris et al. (2011)		X	X
Ke et al. (2009)		X	X
Yang et al. (2008)			X
Zakrzewska and Ferragut (2011)			X
Dietterich et al. (2010)			X
Yu et al. (2008)	X		
Schreiber-Ehle and Koch (2012)			X
Giacobe (2010)			X
Shen et al. (2007b)			X
Shen et al. (2007a)			X
Greitzer and Frincke (2010)			X
Skopik et al. (2012b)		X	X
Skopik et al. (2012a)		X	X
Lee et al. (2006)		X	X
Doup et al. (2011)	X		
Klump and Kwiatkowski (2010)		X	
Grimaila et al. (2008)	X		
Grimaila and Fortson (2007)	X		
Sorrels et al. (2008)	X		
Fortson and Grimaila (2007)	X		
Haas et al. (2011)	X		
Robinson and Cybenko (2012)	X	X	X
Klein et al. (2011)	X	X	
Beaver et al. (2011)	X		
Wu et al. (2009)	X		
D'Amico et al. (2007)	X	X	
Kopylec et al. (2007)	X		X
Pike et al. (2008)	X	X	
O'Hare et al. (2008)	X		
D'Amico and Salas (2003)	X		

Table 4 – Review articles.

Article
Tadda and Salerno (2010)
Schreiber-Ehle and Koch (2012)
Giacobe (2010)
Li et al. (2010)
Klein et al. (2011)
D'Amico et al. (2007)
Goodall (2008)
Tamassia et al. (2009)

technical aspects of cyber situational awareness. Thus Harmer et al. (2011) propose metrics for how to analyze wireless network traffic in order to detect attacks, McHugh et al. (2005) deal with analyzing traffic on high speed networks and King et al. (2012) show how deep packet inspection (DPI) can provide insight and situational awareness within classified proprietary networks.

Game-theoretic models can be used to understand strategic behavior in cyberspace and enable more informed decision-making. For instance, Hu et al. (2009) model attacker intent and strategies based on the incentives of the situation using the Bayesian Nash equilibrium concepts, as do He et al. (2009).

More conceptual contributions include the ideas for a common operational picture presented by Cheng et al. (2012), the discussion by Preden et al. (2011) on achieving situation awareness for networked systems and the discussion by Lacey et al. (2007) on philosophical aspects of cyber situational awareness.

Rather than addressing the full complexity of situational awareness, most of the literature is concentrated on cyber issues, i.e., how cyber sensors can contribute to the overall understanding of the situation, or being more specific with regard to particular cyber sensors. Hence, the relationship between cyber sensors and their contribution to overall situational awareness is covered to some extent, but the opposite relationship where ordinary sensors have the potential to contribute to the cyber situation is not covered much.

Being aware of strategic situations where, e.g., willful-thinking opponents use deception and try to conceal their actual intentions is an important part of situational awareness. Such awareness can be related to obtaining a higher level understanding of the situation as described in Section 2. Hence, it is not surprising to see game-theoretic techniques appearing among the search results when it comes to, e.g., modeling attacker intent.

4.2. *Cyber situational awareness for industrial control systems*

Cyber security in industrial control systems (ICS) has received much attention lately, not least in the wake of the Stuxnet malware. ICSs are used to control facilities such as water plants, industrial production, electrical power distribution, and oil refineries. The complexity of these systems makes testbeds and simulations attractive for cyber situational awareness. For instance, Adhikari et al. (2012) describe a testbed where power systems (particularly synchrophasor data, i.e. synchronized measurements of voltage and current waveforms on multiple locations within the grid) can be simulated for research purposes, and Berman and Butts (2012) have built an ICS emulator in order to better be able to investigate cyber attacks. Similarly, Ross et al. (2013) demonstrate their proposed agent-based protection system for the power grid using a federated simulation platform.

Another direction in ICS cyber situational awareness is frameworks such as the one proposed by Mavridou and Papa (2012). The architecture describes how to collect and analyze traffic from field sensors, using threat modeling to assess the potential impact on operations (cf. also Mavridou et al., 2012). Alcaraz and Lopez (2013) propose a set of protection services for the smart grid, based on different technologies such as cloud computing and wireless sensors. Dean III (2009) explores the use of enterprise architecture models to gain appropriate awareness of the National Airspace System surveillance, automation, and weather systems.

More traditional intrusion detection has also been explored, e.g. how to integrate existing intrusion detection systems (IDSs) into architectures that allow monitoring of control systems (D'Antonio et al., 2006), use system characteristics such as regularity of network traffic to spot attacks (Valdes and Cheung, 2009), or simply use general anomaly detection for attack identification (Ten et al., 2008).

The threats to ICS and SCADA features prominently in many national strategies. As pointed out in the German strategy, this is probably largely due to the Stuxnet incident, that "shows that important industrial infrastructures are no longer exempted from targeted IT attacks" (Federal Ministry of the Interior, 2011). The Australian government works within the Trusted Information Sharing Network for Critical Infrastructure Protection to provide guidance on control systems security and to disseminate alerts on vulnerabilities. Australia has also established a SCADA Community of Interest to raise awareness among stakeholders (Australian Government, Attorney-General's Department, 2009). The Canadian strategy foresees similar Joint public/private sector initiatives (Government of Canada, Public Safety Canada, 2010). Increasing the security of control systems is one of the measures defined in the Estonian strategy (Cyber Security Strategy Committee, Ministry of Defence, 2008).

4.3. *Cyber situational awareness for emergency management*

In emergency and crisis management, cyber situational awareness can play an important role. However, most work is still on a conceptual level, including general discussions of the topic (Walker et al., 2010), a metamodel of shared situation awareness (Kirillov et al., 2012) and an architecture for achieving situational awareness and interoperability (Adams et al., 2011).

Some national strategies note the connection between cyber situational awareness and emergency management, e.g. the Canadian: "Cyber attacks that disrupt emergency response and public health systems would put lives in danger" (Government of Canada, Public Safety Canada, 2010).

From a situational awareness perspective, it is worth noting that the term cyber situational awareness is largely discussed in terms of IT security when addressed in the

context of applied areas such as emergency management. From an overall situational awareness perspective, it is worth noting that many other kinds of cyber sensors, such as web crawlers, also have the potential to provide insight and enhance situational awareness with regard to a crisis and the further development of the crisis situation.

4.4. *Tools, architectures, and algorithms*

Tools, architectures, and algorithms constitute a large and diverse part of the literature. Almost all of these contributions are based on actual implementations, and most of them make a non-trivial empirical contribution.

For obvious reasons, much work has been dedicated to the question of how to turn large amounts of data into useful cyber situational awareness. Aspects include visualization of "big data" (Jonker et al., 2012), anomaly detection made to detect low probability events (Harrison et al., 2012), fusion of RSS feeds, SIGINT data etc. to gain increased appreciation of cyber threats (Morris et al., 2011), fast calculations of important statistical properties of high speed and high volume data (Streilein et al., 2011) as well as investigations of visualization (Jajodia et al., 2011) and scalability (Albanese et al., 2011) of large attack graphs. Sudit et al. (2005) apply fusion algorithms to IDS data, achieving high speed fusion and presentation as well as a relatively high level of abstraction in the user interaction (cf. also Stotz and Sudit, 2007).

Another interesting class of work has to do with behavioral modeling. Ke et al. (2009) use dynamic Bayesian networks and hidden Markov models to model insider threats, aiming to foresee future behavior. Zakrzewska and Ferragut (2011) employ Petri Nets to model real-time cyber conflicts. Dietterich et al. (2010) use machine learning methods to capture the behavior of ordinary desktop computer users. Dutt et al. (2011) use cognitive instance-based learning (IBL) to formalize how a security analyst works. Barford et al. (2010a) explore the use of honeynets to map the behavior of adversaries, characterizing it largely in terms of traffic distributions over time. Cai et al. (2011) apply game theory to the problem of defending a honeynet from systematic mapping by an attacker. Robinson and Cybenko (2012) create a formal behavioral model based on activities performed by a user when on the Internet, and test it using browser history data collected from consenting individuals.

Another topic that has received much attention is the issue of attack attribution. Dacier et al. (2009) present an attribution method based on aggregating small attack traces into larger and more meaningful patterns. The method has been tested on honeypot data, collected over two years time.

Yang et al. (2008) represent a relatively rare example of projection of the current situation into the future. The authors use IDS data to build attack tracks, and then employ variable length Markov models (VLMM) to model attacker behavior and project ongoing attacks into the future. They also offer some encouraging experimental results.

4.5. *Information fusion*

Fusion of information from different sources is an important technology for maintaining cyber situational awareness. Several papers discuss the application of the well established JDL data fusion model to the cyber area (Schreiber-Ehle and Koch, 2012; Giacobe, 2010). Li et al. (2010) explores the important conceptual issue of how to manage uncertainty and risk in cyber situational awareness. Paffenroth et al. (2012) demonstrate how to detect network data patterns not discernible on individual nodes and Mathews et al. (2012) propose a system for collaboratively combining data from sensors using ontology methods. Greitzer and Frincke (2010) who fuse security audit data with data from a psychological model in order to mitigate insider threats is an example of less traditional fusion.

Insight from game theory can be used to improve the effectiveness of fusion systems with regard to situational awareness, in effect viewing sensor data through the lens of Markov game models that help estimate the probabilities of different cyber attack patterns (Shen et al., 2007a, 2007b).

4.6. *Visualization for cyber situational awareness*

Visualization is generally believed to be very important to attain cyber situational awareness. Tamassia et al. (2009) offer a survey of approaches. Some work is closely connected to human-computer interaction, e.g. Erbacher (2012) who uses a human in the loop design to find appropriate visualizations or D'Amico et al. (2007) who employ cognitive task analysis to create a visualization framework to support the work of analysts. Other work focuses more on using machine learning methods such as artificial neural networks and self-organizing maps (Wu et al., 2009) or swarm analysis (Beaver et al., 2011) to sift through IDS data and present relevant information to the human user. There is also work on the visualization of attack graphs (O'Hare et al., 2008), and cascading threats in critical infrastructures (Kopylec et al., 2007).

Michel et al. (2011) investigate the use of virtual worlds to better convey the large amounts of data involved in real-time cyber situational awareness. Somewhat in a similar fashion, D'Amico and Salas (2003) explore the use of 3D models to visualize the impact of information security events on military missions. Klein et al. (2012) address the cyber situational awareness problem in two stages: first data is collected into a comprehensive model, then this data is visualized in a way that supports human understanding. Phan et al. (2008) present a system that focuses on making temporal relationships apparent and allows users to interactively classify events, work iteratively and themselves create a visual structure. Williams et al. (2012) also focus on dynamic and interactive exploration of network security data. Pike et al. (2008) goes beyond the computer network and describe a visualization tool that captures the larger threat landscape – organizational, social, and geopolitical events.

Visualization techniques are seldom mentioned in national strategies, but there are exceptions. In Japan, "frameworks will be examined for visualizing the degree of vulnerability of Japan's cyberspace, degree of malware infections and other overall trends" (National Information Security Center, 2013).

The studied articles target visualization from a technical perspective, i.e., focusing on the actual implementation of the

visualizations. Although information visualization must be considered a vital component when it comes to obtaining situational awareness, the actual visualization is in itself, however, not directly related to the mental state that the notion of situational awareness refers to. Hence, it would be interesting to perform further studies with regard to measuring the extent of situational awareness that is reached using different visualizations. This will differ between people, but it would still be interesting to study what kind of cyber visualizations that make a difference when it comes to obtaining and further developing situational awareness.

4.7. *Human-computer interaction, design specifications and work flows for cyber situational awareness*

Clearly, human-computer interaction is essential for achieving cyber situational awareness. Erbacher et al. (2010b) has collected feedback from network analysts in order to understand the actual needs of the personnel involved. Based on such user information about processes, goals and concerns, they present a task-flow diagram (cf. also Erbacher et al., 2010a). Along similar lines, Mahoney et al. (2010) present findings from a cognitive task analysis with a subject matter expert, indicating requirements for the design of a cyber situational awareness tool. Another set of cognitive task analyses is provided by D'Amico et al. (2005) who have looked at the work of information assurance and computer network defense analysts. Findings include analytical process workflows, definitions of analyst roles, and discussions on proper visual representations (cf. also D'Amico and Whitley, 2008).

Klein et al. (2011) argue that cyber defense needs to be seen as an integrated activity, where all the stages in the OODA (observe, orient, decide, act) loop are considered holistically.

Stevens-Adams et al. (2013) report on an experiment where different teams received different training – tool-based or narrative-based or a combination thereof – before being subjected to network security analysis tasks. The team receiving narrative-based training achieved the highest level of situational awareness.

The human-computer interaction area include a rich body of techniques for modeling and understanding the target domain, i.e., the user, the group of users, or the organization, from a design perspective. From a situational awareness perspective it would be interesting to turn this view around and try to understand, e.g., the attacker, the organization, etc., for the purpose of understanding the situation in more depth. None of the articles seem to be addressing this perspective, though, which might call for future research initiatives.

4.8. *Nation-wide, large scale cyber situational awareness*

The idea of establishing cyber situational awareness on a national scale, while popular with policy-makers, does not appear to have received very much scholarly attention. Lee et al. (2006) offer an early attempt to design a real time cyber early warning system, including an efficiency validation experiment. More recently, some work has been published within the Austrian national research project CAIS (Cyber Attack Information System), where design requirements for national incident response have been elicited (Skopik et al., 2012b) and a prototype architecture for distributed anomaly detection has been implemented (Skopik et al., 2012a). However, this work has yet to undergo empirical evaluation.

As mentioned in Section 1, all the national strategies include wordings that call for nation-wide cyber situational awareness.

4.9. *Exercises relating to cyber situational awareness*

One way to empirically investigate cyber situational awareness is by studying different kinds of exercises. Doup et al. (2011) describe a security competition held in 2010 with almost a thousand participants, specifically aiming to create a cyber situational awareness dataset. The participating teams were looking for a set of vulnerable services to attack, thereby gaining points. The authors introduce two new measures of cyber situational awareness, and share some experiences.

Malviya et al. (2010) use data from an exercise held among the U.S. service academies to see whether team situational awareness correlates with team success as measured by score. They conclude that there is indeed such a weak correlation. In later work, the authors collect data on team collaboration, including scoring data, interview data on situational awareness, network packets and logs and video/audio of the competition (Fink et al., 2013).

One reason to believe that research based on exercises has a promising future is that many countries seem committed to conducting exercises, as is evident in the strategies of Australia, Estonia, Germany, Canada, the UK, the US, Japan, the Netherlands, and Finland.

4.10. *Information exchange for cyber situational awareness*

One way of gaining increased cyber situational awareness is to exchange information with others. Thus Klump and Kwiatkowski (2010) propose an architecture for information exchange about incidents in the power system, and Hennin (2008) proposes one for sharing information about suspicious IP addresses. Brunner et al. (2011) address more principled problems as they ponder the trade-off between the increased awareness gained by sharing data and the loss of privacy entailed. Combining peer-to-peer networking and traceable anonymous certificates, they propose a collaborative and decentralized concept for an exchange platform.

Information exchange receives much attention in the national strategies. The Netherlands find "information-exchange between the various players" to be "of the utmost importance" for fighting cyber crime (National Coordinator for Security and Counterterrorism, 2013). The Australian government strives to foster "more intensive trusted information exchanges with high risk sectors to share information on sophisticated threats", aiming primarily at telecommunications, banking and finance, and owners of industrial control systems (Australian Government, Attorney-General's Department, 2009). Estonia highlights the importance of exchanging expert information within the frameworks of the international network of national CERTs, the network of government CERTs, Interpol, Europol and organizations dealing with

critical information infrastructure protection (Cyber Security Strategy Committee, Ministry of Defence, 2008).

4.11. Military cyber situational awareness

Cyber situational awareness is important for military operations, whether defensive or offensive. In particular the issue of damage assessment is pressing. Grimaila and Fortson (2007) critically review the state of defensive information risk management within the U.S. Air Force, and recommends an information asset focused risk assessment. In another paper, the authors prescribe a roadmap in order to reach real-time situational awareness that bridges the gap between technical impact and impact on operations (Fortson and Grimaila, 2007). They go on to recommend an operational process and an architecture for what they call Cyber Incident Mission Impact Assessment (CIMIA) (Sorrels et al., 2008). Gagnon et al. (2010) introduce a Cyber OODA loop in a study focusing on maintaining availability and robustness of a Ballistic-Missile-Defense system in the face of cyber attack.

Yu et al. (2008) present a testbed for developing and testing information operations (focusing on the cyber aspect) using simulations. The tool includes a graphical user interface to design and monitor the tests implemented. Haas et al. (2011) present ideas and concepts for how simulations can aid the planning and conduct of information operations.

Rice et al. (2011) call attention to the idea of systematically using deception in cyber sensor placement to shield them from an adversary. The idea is to introduce uncertainty in the adversary's beliefs about sensors. The paper describes a number of sensor shielding tactics.

Most strategies mention military in general terms to illustrate that cyber threats cut across organizational boundaries, necessitating civil-military cooperation. Many also mention international cooperation within the NATO framework. The UK is probably the most explicit when it comes to expressing the *situational awareness* aspect: "The intelligence agencies and Ministry of Defence have a strong role in improving our understanding of – and reducing – the vulnerabilities and threats that the UK faces in cyberspace" (Government of the UK, the Cabinet Office, 2011). Finland also explicitly mentions the intelligence aspects – the need to know what is going on: "A military cyber defence capacity encompasses intelligence as well as cyber attack and cyber defence capabilities" (Secretariat of the Security Committee, 2013).

5. Discussion

Given the characterization of the state of research, a few observations can be made. In the following, these observations are summarized and discussed from the initially laid out perspectives: (i) national cyber (security) strategies, and (ii) situational awareness for the purpose of understanding an overall situation. Also, some additional remarks conclude the section.

5.1. National cyber strategies

When it comes to national cyber (security) strategies, it is clear that the emphasis on protecting critical information infrastructures, evident in all of the national strategies cited in the introduction, is also reflected in the literature. Cyber situational awareness in industrial control systems – arguably a cornerstone of critical information infrastructures – is frequently addressed. Furthermore, as noted above, this focus probably also has an impact on the kinds of threats addressed, viz. the focus on availability over confidentiality and integrity. As a consequence, there is an uneven characterization of threats in the literature – confidentiality and integrity being somewhat underdeveloped.

A second feature that the national strategies have in common is that they stress the importance of international partnerships and allies. Given this, it is somewhat surprising to find that the scientific research dedicated to exploring information exchange for cyber situational awareness is relatively scarce – as is the research on nation-wide, large scale cyber situational awareness. One noteworthy topic that is completely absent is the role and effectiveness of national strategies – apparently very popular – in achieving increased cyber situational awareness.

The national strategies also stress the need for training of IT specialists. This priority seems to be synchronized with the relatively well-developed body of research on human-computer interaction, work flows and visualization for cyber situational awareness.

These days, various kinds of electronic deception is receiving much attention. For instance, in the *Global risks report* (Howell, (ed.), 2013) released in conjunction with the 2013 World Economic Forum in Davos, "massive digital misinformation" features prominently (for a more in-depth analysis, cf. Franke (2013)). However, the vulnerability of cyber situational awareness to deception is virtually absent from the literature, save the low-level race between exploits and intrusion detection systems. Given the prominent place of high-level cyber situational awareness in national cyber strategies, it seems that more attention should be directed to the risk of deception.

5.2. Situational awareness

As discussed in Section 2, the sought for overall situational awareness according to Endsley (1995) serves to help a decision-maker to make sense of a situation in order to make the right decisions. Taking this overall perspective, however, we note that a majority of the literature concerns specific aspects that are indeed *related* to situational awareness, but whether the overall situational awareness is actually improved is seldom measured. Examples of such specific research results concern sensor solutions, awareness regarding the cyber situation alone, awareness related to the understanding of the strategic component of the situation, etc. Hence, we note that there are many solutions that can potentially contribute to the overall understanding of the situation according to Section 2, but that it remains uncertain to what extent the situational awareness actually improves. Here we see opportunities for performing experiments to measure how particular solutions contribute to the overall understanding of a situation by, e.g., combining cyber defense exercises and large-scale command and control exercises. Doing so, it will be interesting to investigate the participants'

understanding of both the specific cyber events, and how the overall understanding of the situation is or is not improved when the physical events and the cyber events are taken together. From a sensor perspective, it will for the same reason be necessary to investigate how physical sensors contribute to the cyber situational awareness and vice versa.

A parallel dimension that was found in several of the 11 cluster categories presented in Section 4 relates to game theory and the need to reason about uncertain situations where the true intent of an attacker is uncertain. This is hardly surprising since much of the cyber security landscape concerns deception, concealed actions, etc. Rather, such strategic considerations should probably be taken to be the norm where, e.g., one can not be sure whether an IT attack is performed in isolation or has been undertaken for a higher-order purpose, etc. In our previous work, we have taken a top-down perspective on the game-theoretic part of situational awareness which is an inherent ingredient in large-scale command and control situations where decisions need to be taken based on one's understanding of the intent of opposing leaders (Brynielsson and Arnborg, 2004; Brynielsson, 2004; Brynielsson and Arnborg, 2005, 2006; Brynielsson, 2007). Here we see the opportunity to investigate further how these two game-theoretic perspectives can be combined to obtain a further understanding of the situation. To advance the game-theoretic paradigm in cyber situational awareness, it would be useful to structure the literature. One interesting dimension is the above distinction between large-scale strategic understanding in command and control (e.g. on a national level) and small-scale tactical understanding (e.g. in an IDS). Another interesting dimension is between game-theory as a vehicle for reflecting and understanding a situation (e.g. whether a situation is a positive sum or a zero sum game, whether there are multiple equilibria, mixed strategies etc.) or as a vehicle for tactical decision-making (e.g. given this complex sensor input, we close down port 80).

From a sensor point of view, we recognize that IT sensors come in many shapes, ranging from network sniffing tools to web crawlers. In the former case, the sensors consist of a range of network monitoring tools. In the latter case, tools for monitoring and analysis of large amounts of online user generated content hold the potential to provide insight with regard to crisis communication (Brynielsson et al., 2013b, 2013c) as well as intelligence (Brynielsson et al., 2013a). Here, the challenge is to automatically combine two kinds of information arising from automatic data processing, namely low-level numeric sensor input and information that can be extracted through data mining and natural language processing. These two kinds of cyber data have the potential to contribute to one and the same cyber situation in real-time, which calls for development of new fusion algorithms where high-level data obtained from, e.g., hacker discussion boards can be automatically fused with readings from, e.g., IDSs. In the end, the information must also be further combined with physical sensors in order to be able to understand the full situation, but the cyber part of the situation is complex in its own right since very different technologies and disciplines need to be combined in order to develop the sought for fusion algorithms. A way to inform such development could be to design and setup specific cyber defense exercises where the incentive structure is specifically designed to target these aspects.

5.3. *Some additional remarks*

From a scientific perspective, it is somewhat disappointing that not more of the research is empirically based. On the rather liberal interpretation of a non-trivial empirical contribution (cf. Section 3) slightly below 45% of the articles reviewed were classified into this category, but it is noteworthy that only three articles were found where exercises were used as vehicles to gather empirical data on cyber situational awareness. The potential of using exercises as an experimental platform is probably much greater (Sommestad and Hallberg, 2012).

Last, it is evident that the research on military aspects of cyber situational awareness does not match the level of attention given to "cyber war" neither in the media nor in other academic disciplines (Libicki, 2007; Rid, 2012). Indeed, the crucial aspect of battle damage assessment (i.e. how to know whether actions taken have an effect) is completely missing in the literature found. (Though there are examples not covered by our choice of databases and keywords in the systematic review, e.g. Gallagher and Horta (2013).) Of course, it might be that the issue of cyber battle damage assessment is deemed too sensitive to publish openly at all.

6. Conclusions

This article has presented a review of the scientific literature on cyber situational awareness. Based on systematic queries in four leading scientific databases, 102 articles were read, clustered, and succinctly described.

It is evident that some aspects of the cyber situational awareness area are more mature than others. For example, there is plenty of work dedicated to cyber situational awareness in industrial control systems, or general work on algorithms and information fusion in intrusion detection systems (IDSs). The challenges in these areas are to mature as a field by, e.g., finding good measures for the usability of IDSs (Werlinger et al., 2008), defining granular and relevant measures of service availability in control systems (Franke, 2012) or compiling appropriate data sets on which to test new IDS algorithms and architectures (Tjhai et al., 2008).

In contrast, less research has been devoted to areas such as information exchange for cyber situational awareness, the risks of deception, or the issue of cyber battle damage assessment in military operations. In these areas, the challenge is rather to establish research agendas, and start thinking about methods, data, and experiments.

Overall, it seems that there is a potential for making more empirically based research. Cyber security exercises of various kinds offer a particularly interesting source of data on cyber situational awareness. While it can be difficult to get the most qualified people to participate in purely research-oriented experiments, exercises can be adapted to answer research questions, while still offering more tangible benefits to the participants.

Acknowledgments

This work has been supported by Security Link, in the Strategic Area for security and crisis management research, funded by the Swedish Government. The authors wish to thank Anders Törne, Pontus Svenson and Teodor Sommestad for their support and constructive comments, and Ingolf Berg for useful discussions on national cyber strategies.

REFERENCES

Adams K, Wassell A, Ceruti M, Castro E, Lehan S, Mitchell J. Emergency-management situational-awareness prototype (EMSAP). In: 2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2011; 2011. pp. 110–4.

Adhikari U, Morris T, Dahal N, Pan S, King R, Younan N, et al. Development of power system test bed for data mining of synchrophasors data, cyber-attack and relay testing in RTDS. In: IEEE Power and Energy Society General Meeting; 2012.

Agence nationale de la sécurité des systèmes d'information (ANSS). Information systems defence and security – France's strategy; Feb. 2011. http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf. Accessed 20.01.14.

Albanese M, Jajodia S, Pugliese A, Subrahmanian V. Scalable detection of cyber attacks. In: Computer Information Systems–Analysis and Technologies. Springer; 2011. pp. 9–18.

Alcaraz C, Lopez J. Addressing situational awareness in critical domains of a smart grid. In: Network and System Security. Springer; 2012. pp. 58–71.

Alcaraz C, Lopez J. Wide-area situational awareness for critical infrastructure protection. Computer 2013;46(4):30–7.

Arnborg S, Artman H, Brynielsson J, Wallenius K. Information awareness in command and control: precision, quality, utility. In: Proceedings of the Third International Conference on Information Fusion (FUSION 2000). Paris, France; Jul. 2000. ThB1/25–32. URL, http://www.csc.kth.se/~joel/iq.pdf.

Australian Government, Attorney-General's Department. Cyber Security Strategy; 2009. http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf. Accessed 20.01.14.

Barford P, Chen Y, Goyal A, Li Z, Paxson V, Yegneswaran V. Employing honeynets for network situational awareness. In: Cyber Situational Awareness. Springer; 2010a. pp. 71–102.

Barford P, Dacier M, Dietterich TG, Fredrikson M, Giffin J, Jajodia S, et al. Cyber SA: situational awareness for cyber defense. In: Cyber Situational Awareness. Springer; 2010b. pp. 3–13.

Beaver J, Steed C, Patton R, Cui X, Schultz M. Visualization techniques for computer network defense. In: Proceedings of SPIE – The International Society for Optical Engineering, vol. 8019; 2011.

Berman D, Butts J. Towards characterization of cyber attacks on industrial control systems: emulating field devices using gumstix technology. In: Proceedings – 2012 5th International Symposium on Resilient Control Systems, ISRCS 2012; 2012. pp. 63–8.

Brunner M, Hofinger H, Roblee C, Schoo P, Todt S. Anonymity and privacy in distributed early warning systems. Lect Notes Comput Sci 2011;6712:81–92 [including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics], LNCS.

Brynielsson J. Game-theoretic reasoning in command and control. In: Proceedings of the 15th Mini-EURO Conference: Managing Uncertainty in Decision Support Models (MUDSM 2004). Coimbra, Portugal; Sep. 2004. URL, http://www.nada.kth.se/~joel/mudsm.pdf.

Brynielsson J. A gaming perspective on command and control [Ph.D. thesis]. Stockholm, Sweden: School of Computer Science and Communication, Royal Institute of Technology; Jun. 2006. URL, http://www.csc.kth.se/~joel/PhD.pdf.

Brynielsson J. Using AI and games for decision support in command and control. Decis Support Syst Aug. 2007;43(4):1454–63.

Brynielsson J, Arnborg S. Bayesian games for threat prediction and situation analysis. Stockholm, Sweden. In: Svensson P, Schubert J, editors. Proceedings of the Seventh International Conference on Information Fusion (FUSION 2004), vol. 2; Jun. 28–Jul. 1, 2004. pp. 1125–32. URL, http://www.nada.kth.se/~joel/IF04-1125.pdf.

Brynielsson J, Arnborg S. Refinements of the command and control game component. In: Proceedings of the Eighth International Conference on Information Fusion (FUSION 2005). Philadelphia, Pennsylvania; Jul. 2005. URL, http://www.csc.kth.se/~joel/refinements.pdf.

Brynielsson J, Arnborg S. An information fusion game component. J Adv Inf Fusion Dec. 2006;1(2):108–21.

Brynielsson J, Horndahl A, Johansson F, Kaati L, Mårtenson C, Svenson P. Harvesting and analysis of weak signals for detecting lone wolf terrorists. Secur Inf 2013a;2(11).

Brynielsson J, Johansson F, Lindquist S. Using video prototyping as a means to involving crisis communication personnel in the design process: innovating crisis management by creating a social media awareness tool. In: Proceedings of the 15th International Conference on Human-Computer Interaction. Las Vegas, Nevada; Jul. 2013. pp. 559–68.

Brynielsson J, Johansson F, Westling A. Learning to classify emotional content in crisis-related tweets. In: Proceedings of the 2013 IEEE International Conference on Intelligence and Security Informatics (ISI 2013). Seattle, Washington; Jun. 2013. pp. 33–8.

Cai J-Y, Yegneswaran V, Alfeld C, Barford P. Honeynet games: a game theoretic approach to defending network monitors. J Comb Optim 2011;22(3):305–24.

Cheng Y, Sagduyu Y, Deng J, Li J, Liu P. Integrated situational awareness for cyber attack detection, analysis, and mitigation. In: Proceedings of SPIE - The International Society for Optical Engineering, vol. 8385; 2012.

Cyber Security Strategy Committee, Ministry of Defence. Cyber Security Strategy; 2008. http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf. Accessed 20.01.14.

Dacier M, Pham V-H, Thonnard O. The WOMBAT attack attribution method: some results. In: Information Systems Security. Springer; 2009. pp. 19–37.

D'Amico A, Salas S. Visualization as an aid for assessing the mission impact of information security breaches. In: DARPA Information Survivability Conference and Exposition, 2003. Proceedings, vol. 2; 2003. pp. 18–20.

D'Amico A, Whitley K. The real work of computer network defense analysts. In: VizSEC 2007. Springer; 2008. pp. 19–37.

D'Amico A, Whitley K, Tesone D, O'Brien B, Roth E. Achieving cyber defense situational awareness: a cognitive task analysis of information assurance analysts. In: Proceedings of the Human Factors and Ergonomics Society; 2005. pp. 229–33.

D'Amico AD, Goodall JR, Tesone DR, Kopylec JK. Visual discovery in computer network defense. Comput Graph Appl IEEE 2007;27(5):20–7.

D'Antonio S, Oliviero F, Setola R. High-speed intrusion detection in support of critical infrastructure protection. In: Lopez J,

editor. Critical Information Infrastructures Security. Lecture Notes in Computer Science, vol. 4347. Berlin Heidelberg: Springer; 2006. pp. 222–34.
Dean III N. Improving NAS (national airspace system) cyber security detection and response utilizing enterprise system architectures. In: Air Traffic Control Association – 54th Air Traffic Control Association Annual Conference 2009; 2009. pp. 45–9.
Dietterich TG, Bao X, Keiser V, Shen J. Machine learning methods for high level cyber situation awareness. In: Cyber Situational Awareness. Springer; 2010. pp. 227–47.
Doup A, Egele M, Caillat B, Stringhini G, Yakin G, Zand A, et al. Hit 'em where it hurts: a live security exercise on cyber situational awareness. In: ACM International Conference Proceeding Series; 2011. pp. 51–61.
Dutt V, Ahn Y-S, Gonzalez C. Cyber situation awareness: modeling the security analyst in a cyber-attack scenario through instance-based learning. In: Data and Applications Security and Privacy XXV. Springer; 2011. pp. 280–92.
Endsley MR. Design and evaluation for situation awareness enhancement. In: Proceedings of the Human Factors Society 32nd Annual Meeting. Santa Monica, California; 1988. pp. 97–101.
Endsley MR. Toward a theory of situation awareness in dynamic systems. Hum Factors Mar. 1995;37(1):32–64.
Endsley MR. Theoretical underpinnings of situation awareness: a critical review. In: Endsley MR, Garland DJ, editors. Situation Awareness Analysis and Measurement. Mahwah, New Jersey: Lawrence Erlbaum Associates, Inc; 2000. pp. 3–32.
Erbacher R. Visualization design for immediate high-level situational assessment. In: ACM International Conference Proceeding Series; 2012. pp. 17–24.
Erbacher R, Frincke D, Chung Wong P, Moody S, Fink G. A multi-phase network situational awareness cognitive task analysis. Inf Vis 2010a;9(3):204–19.
Erbacher R, Frincke D, Wong P, Moody S, Fink G. Cognitive task analysis of network analysts and managers for network situational awareness. In: Proceedings of SPIE – The International Society for Optical Engineering, vol. 7530; 2010.
Ericsson GN. Cyber security and power system communicationessential parts of a smart grid infrastructure. Power Deliv IEEE Transactions 2010;25(3):1501–7.
Federal Ministry of the Interior. Cyber Security Strategy for Germany; Feb. 2011. http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile. Accessed 20.01.14.
Fink G, Best D, Manz D, Popovsky V, Endicott-Popovsky B. Gamification for measuring cyber security situational awareness. In: Foundations of Augmented Cognition. Springer; 2013. pp. 656–65.
Fortson L, Grimaila M. Development of a defensive cyber damage assessment framework. In: Armistead L, editor. ICIW 2007: Proceedings of the 2nd International Conference on Information Warfare and Security. pp. 69–76, 2nd International Conference on Information Warfare and Security, Naval Postgrad Sch, Monterey, CA, MAR 08–09, 2007; 2007.
Franke U. Optimal IT service availability: shorter outages, or fewer? Netw Serv Manag IEEE Transactions March 2012;9(1):22–33.
Franke U. Information operations on the Internet: a catalog of modi operandi. FOI, the Swedish Defence Research Agency; 2013. FOI-R–3658–SE.
Gagnon MN, Truelove J, Kapadia A, Haines J, Huang O. Towards net-centric cyber survivability for ballistic missile defense. In: Architecting Critical Systems. Springer; 2010. pp. 125–41.
Gallagher MA, Horta M. Cyber joint munitions effectiveness manual (JMEM). M&S J 2013;8:5–14.
Garlapati S, Shukla S. Formal verification of hierarchically distributed agent based protection scheme in smart grid. Lect Notes Comput Sci 2012;7385:137–54 [including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics], LNCS.
Ghanea-Hercock R, Gelenbe E, Jennings N, Smith O, Allsopp D, Healing A, et al. Hyperion - next-generation battlespace information services. Comput J 2007;50(6):632–45.
Giacobe N. Application of the JDL data fusion process model for cyber security. In: Proceedings of SPIE - The International Society for Optical Engineering, vol. 7710; 2010.
Giles K, Hagestad W. Divided by a common language: cyber definitions in Chinese, Russian and English. In: Cyber Conflict (CyCon), 2013 5th International Conference on; 2013. pp. 413–29.
Goodall JR. Introduction to visualization for computer security. In: VizSEC 2007. Springer; 2008. pp. 1–17.
Government of Canada, Public Safety Canada. Canada's Cyber Security Strategy; 2010. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf. Accessed 20.01.14.
Government of the UK, the Cabinet Office. The UK Cyber Security Strategy; Nov. 2011. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf. Accessed 20.01.14.
Greitzer FL, Frincke DA. Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In: Insider Threats in Cyber Security. Springer; 2010. pp. 85–113.
Grimaila M, Fortson L. Towards an information asset-based defensive cyber damage assessment process. In: Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications, CISDA 2007; 2007. pp. 206–12.
Grimaila M, Mills R, Fortson L. Improving the cyber incident mission impact assessment (cimia) process. In: CSIIRW'08 – 4th Annual Cyber Security and Information Intelligence Research Workshop: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead; 2008.
Haas MW, Mills RF, Grimaila MR. Aiding understanding of a contested information environments effect on operations. In: Human-in-the-Loop Simulations. Springer; 2011. pp. 175–202.
Harmer P, Thomas R, Christel B, Martin R, Watson C. Wireless security situation awareness with attack identification decision support. In: Computational Intelligence in Cyber Security (CICS), 2011 IEEE Symposium on; 2011. pp. 144–51.
Harrison L, Laska J, Spahn R, Iannacone M, Downing E, Ferragut E, et al. Situ: situational understanding and discovery for cyber attacks. In: IEEE Conference on Visual Analytics Science and Technology 2012, VAST 2012-Proceedings; 2012. pp. 307–8.
He H, Shuping Y, Wu P. Security decision making based on domain partitional markov decision process. In: Proceedings – 2009 International Conference on Information Engineering and Computer Science, ICIECS 2009; 2009.
Hennin S. Control system cyber incident reporting protocol. In: 2008 IEEE International Conference on Technologies for Homeland Security, HST'08; 2008. pp. 463–8.
Howell L, editor. Global risks report 2013. World Economic Forum; 2013.
Hu H, Wang X, Yang X. A decision-support model for information systems based on situational awareness. In: 1st International Conference on Multimedia Information Networking and Security, MINES 2009, vol. 2; 2009. pp. 405–8.
Jajodia S, Liu P, Swarup V, Wang C, editors. Cyber situational awareness: Issues and Research. Springer Publishing Company; 2010 [Incorporated].
Jajodia S, Noel S, Kalapa P, Albanese M, Williams J. Cauldron: Mission-centric cyber situational awareness with defense in

depth. In: Proceedings – IEEE Military Communications Conference MILCOM; 2011. pp. 1339–44.
Jonker D, Langevin S, Schretlen P, Canfield C. Agile visual analytics for banking cyber "big data". In: IEEE Conference on Visual Analytics Science and Technology 2012, VAST 2012-Proceedings; 2012. pp. 299–300.
Ke T, Zhou M-T, Wang W-Y. Insider cyber threat situational awareness framwork using dynamic bayesian networks. In: Proceedings of 2009 4th International Conference on Computer Science and Education, ICCSE 2009; 2009. pp. 1146–50.
King D, Orlando G, Kohler J. A case for trusted sensors: encryptors with deep packet inspection capabilities. In: Proceedings - IEEE Military Communications Conference MILCOM; 2012.
Kirillov I, Metcherin S, Klimenko S. Metamodel of shared situation awareness for resilience management of built environment. In: Proceedings of the 2012 International Conference on Cyberworlds, Cyberworlds 2012; 2012. pp. 137–43.
Klein G, Gnther H, Trber S. Modularizing cyber defense situational awareness – technical integration before human understanding. Commun Comput Inf Sci 2012;318:307–10. CCIS.
Klein G, Tlle J, Martini P. From detection to reaction – a holistic approach to cyber defense. In: 2011 Defense Science Research Conference and Expo, DSR 2011; 2011.
Klump R, Kwiatkowski M. Distributed ip watchlist generation for intrusion detection in the electrical smart grid. In: Critical Infrastructure Protection IV. Springer; 2010. pp. 113–26.
Kopylec J, D'Amico A, Goodall J. Visualizing cascading failures in critical cyber infrastructures. In: Critical Infrastructure Protection V, vol. 253; 2007. pp. 351–64.
Lacey T, Mills R, Raines R, Williams P, Rogers S. A qualia framework for awareness in cyberspace. In: Proceedings – IEEE Military Communications Conference MILCOM; 2007.
Lee S, Lee DH, Kim KJ. A conceptual design of knowledge-based real-time cyber-threat early warning system. In: Frontiers of High Performance Computing and Networking–ISPA 2006 Workshops. Springer; 2006. pp. 1006–17.
Li J, Ou X, Rajagopalan R. Uncertainty and risk management in cyber situational awareness. In: Cyber Situational Awareness. Springer; 2010. pp. 51–68.
Libicki MC. Conquest in cyberspace: national security and information warfare. Cambridge University Press; 2007.
Liu P, Jia X, Zhang S, Xiong X, Jhi Y-C, Bai K, et al. Cross-layer damage assessment for cyber situational awareness. In: Cyber Situational Awareness. Springer; 2010. pp. 155–76.
Lynn III WF. Defending a new domain-the Pentagon's cyberstrategy. Foreign Aff 2010;89:97.
Mahoney S, Roth E, Steinke K, Pfautz J, Wu C, Farry M. A cognitive task analysis for cyber situational awareness. In: Proceedings of the Human Factors and Ergonomics Society, vol. 1; 2010. pp. 279–83.
Malviya A, Fink G, Sego L, Endicott-Popovsky B. Situational awareness as a measure of performance in cyber security collaborative work. In: Proceedings – 2011 8th International Conference on Information Technology: New Generations, ITNG 2011; 2010. pp. 937–42.
Mathews M, Halvorsen P, Joshi A, Finin T. A collaborative approach to situational awareness for cybersecurity. In: CollaborateCom 2012-Proceedings of the 8th International Conference on Collaborative Computing: Networking, Applications and Worksharing; 2012. pp. 216–22.
Mavridou A, Papa M. A situational awareness architecture for the smart grid. Lect Notes Inst Comput Sci Social-Inf Telecommun Eng 2012;99:229–36. LNICST.
Mavridou A, Zhou V, Dawkins J, Papa M. A situational awareness framework for securing the smart grid using monitoring sensors and threat models. Int J Electron Secur Digital Forensics 2012;4(2–3):138–53.
McHugh J, Gates C, Becknel D. Situational awareness and network traffic analysis. In: Cyberspace Security and Defense: Research Issues. Springer; 2005. pp. 209–28.
Michel M, Helmick N, Mayron L. Cognitive cyber situational awareness using virtual worlds. In: 2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2011; 2011. pp. 179–82.
Morris T, Mayron L, Smith W, Knepper M, Ita R, Fox K. A perceptually-relevant model-based cyber threat prediction method for enterprise mission assurance. In: 2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2011; 2011. pp. 60–5.
National Coordinator for Security and Counterterrorism. National Cyber Security Strategy 2; 2013. http://english.nctv.nl/Images/national-cyber-security-strategy-2_tcm92-520278.pdf. Accessed 20.01.14.
National Information Security Center. National cyber security strategy; Jun. 2013. http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf. Accessed 20.01.14.
Nissenbaum H. Where computer security meets national security. Ethics Inf Technol 2005;7(2):61–73.
O'Hare S, Noel S, Prole K. A graph-theoretic visualization approach to network risk analysis. Lect Notes Comput Sci 2008;5210:60–7 [including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics],LNCS.
Paffenroth R, Du Toit P, Scharf L, Jayasumana A, Bandara V, Nong R. Space-time signal processing for distributed pattern detection in sensor networks. In: Proceedings of SPIE - The International Society for Optical Engineering, vol. 8393; 2012.
Phan D, Gerth J, Lee M, Paepcke A, Winograd T. Visual analysis of network flow data with timelines and event plots. In: VizSEC 2007. Springer; 2008. pp. 85–99.
Pike WA, Scherrer C, Zabriskie S. Putting security in context: visual correlation of network activity with real-world information. In: Goodall JR, editor. VIZSEC 2007. Mathematics and Visualization, 4th International Workshop on Computer Security, Sacramento, CA, OCT 29, 2007; 2008. pp. 203–20.
Preden J, Motus L, Meriste M, Riid A. Situation awareness for networked systems. In: 2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2011; 2011. pp. 123–30.
Rice M, Guernsey D, Shenoi S. Using deception to shield cyberspace sensors. In: Critical Infrastructure Protection V. Springer; 2011. pp. 3–18.
Rid T. Cyber war will not take place. J Strategic Stud 2012;35(1):5–32.
Robinson D, Cybenko G. A cyber-based behavioral model. J Def Model Simul 2012;9(3):195–203.
Ross K, Hopkinson K, Pachter M. Using a distributed agent-based communication enabled special protection system to enhance smart grid security. IEEE Transactions Smart Grid 2013;4(2):1216–24.
Rowe BR, Gallaher MP. Private sector cyber security investment strategies: an empirical analysis. In: The fifth workshop on the economics of information security (WEIS06); 2006.
Schreiber-Ehle S, Koch W. The JDL model of data fusion applied to cyber-defence - a review paper. In: 2012 Workshop on Sensor Data Fusion: Trends, Solutions, Applications, SDF 2012; 2012. pp. 116–9.
Secretariat of the Security Committee. Finland's Cyber Security Strategy; 2013. http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf. Accessed 20.01.14.

Sezer EC, Kil C, Ning P. Automated software vulnerability analysis. In: Cyber Situational Awareness. Springer; 2010. pp. 201–23.
Sheldon F, Huang J, Dang J, Fetzer D, Goose S, Kirsch J, et al. Intrinsically resilient energy control systems. In: ACM International Conference Proceeding Series; 2013.
Shen D, Chen G, Cruz Jr J, Haynes L, Kruger M, Blasch E. A markov game theoretic data fusion approach for cyber situational awareness. In: Proceedings of SPIE – The International Society for Optical Engineering, vol. 6571; 2007.
Shen D, Chen G, Haynes L, Blasch E. Strategies comparison for game theoretic cyber situational awareness and impact assessment. In: FUSION 2007-2007 10th International Conference on Information Fusion; 2007.
Skopik F, Bleier T, Fiedler R. Information management and sharing for national cyber situational awareness. In: ISSE 2012 Securing Electronic Business Processes. Springer; 2012a. pp. 217–27.
Skopik F, Ma Z, Smith P, Bleier T. Designing a cyber attack information system for national situational awareness. Commun Comput Inf Sci 2012b;318:277–88. CCIS.
Sommestad T, Hallberg J. Cyber security exercises and competitions as a platform for cyber security experiments. In: Secure IT Systems, Proceedings of NordSec 2012, Karlskrona, Sweden. Berlin Heidelberg: Springer; 2012. pp. 47–60.
Sorrels D, Grimaila M, Fortson L, Mills R. An architecture for cyber incident mission impact assessment (CIMIA). In: Armistead L, editor. 3rd International Conference on Information Warfare and Security, Proceedings. pp. 335–344, 3rd International Conference on Information Warfare and Security, Univ Nebraska, Peter Kiewit Inst, Omaha, NE, APR 24-25, 2008; 2008.
Steinberg A, Bowman C, White Jr FE. Revisions to the JDL data fusion model. In: Proceedings of SPIE AeroSense (Sensor Fusion: Architectures, Algorithms, and Applications III), vol. 3719; Apr. 1999. pp. 430–41. Orlando, Florida.
Stevens-Adams S, Carbajal A, Silva A, Nauer K, Anderson B, Reed T, et al. Enhanced training for cyber situational awareness. In: Foundations of Augmented Cognition. Springer; 2013. pp. 90–9.
Stotz A, Sudit M. Information fusion engine for real-time decision-making (inferd): a perceptual system for cyber attack tracking. In: FUSION 2007-2007 10th International Conference on Information Fusion; 2007.
Streilein W, Truelove J, Meiners C, Eakman G. Cyber situational awareness through operational streaming analysis. In: Proceedings – IEEE Military Communications Conference MILCOM; 2011. pp. 1152–7.
Sudit M, Stotz A, Holender M. Situational awareness of a coordinated cyber attack. In: Proceedings of SPIE - The International Society for Optical Engineering, vol. 5812; 2005. pp. 114–29.
Tadda GP, Salerno JS. Overview of cyber situation awareness. In: Cyber Situational Awareness. Springer; 2010. pp. 15–35.
Tamassia R, Palazzi B, Papamanthou C. Graph drawing for security visualization. In: Graph Drawing. Springer; 2009. pp. 2–13.
Ten C-W, Liu C-C, Govindarasu M. Anomaly extraction and correlations for power infrastructure cyber systems. In: Conference Proceedings – IEEE International Conference on Systems, Man and Cybernetics; 2008. pp. 7–12.
The Federation Council. Kontseptiia strategii kiberbezopasnosti Rossiiskoi Federatsii [Concept for a Cyber Security Strategy for the Russian Federation]; 2014. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf. Accessed 20.01.14.
The White House (signed by President Barack Obama). International Strategy for Cyberspace; May 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Accessed 20.01.14.
Tjhai GC, Papadaki M, Furnell SM, Clarke NL. The problem of false alarms: evaluation with Snort and DARPA 1999 dataset. In: Trust, privacy and Security in digital business. Springer; 2008. pp. 139–50.
Valdes A, Cheung S. Intrusion monitoring in process control systems. In: Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS; 2009.
Walker J, Williams B, Skelton G. Cyber security for emergency management. In: 2010 IEEE International Conference on Technologies for Homeland Security, HST 2010; 2010. pp. 476–80.
Walls A. Agenda overview for information security technologies and services. Gartner; Jan. 2014. Tech. rep.
Weick KE, Sutcliffe KM, Obstfeld D. Organizing and the process of sensemaking. Organ Sci Jul.–Aug. 2005;16(4):409–21.
Werlinger R, Hawkey K, Muldner K, Jaferian P, Beznosov K. The challenges of using an intrusion detection system: is it worth the effort?. In: Proceedings of the 4th symposium on Usable privacy and security. ACM; 2008. pp. 107–18.
Williams F, Faithfull W, Roberts J. Sitavis - interactive situation awareness visualization of large datasets. In: IEEE Conference on Visual Analytics Science and Technology 2012, VAST 2012-Proceedings; 2012. pp. 273–4.
Wu Q, Ferebee D, Lin Y, Dasgupta D. Visualization of security events using an efficient correlation technique. In: 2009 IEEE Symposium on Computational Intelligence in Cyber Security, CICS 2009-Proceedings; 2009.
Yang S, Byers S, Holsopple J, Argauer B, Fava D. Intrusion activity projection for cyber situational awareness. In: IEEE International Conference on Intelligence and Security Informatics, 2008, IEEE ISI 2008; 2008. pp. 167–72.
Yen J, McNeese M, Mullen T, Hall D, Fan X, Liu P. RPD-based hypothesis reasoning for cyber situation awareness. In: Cyber Situational Awareness. Springer; 2010. pp. 39–49.
Yu T, Fuller B, Bannick J, Rossey LM, Cunningham RK. Integrated environment management for information operations testbeds. In: VizSEC 2007. Springer; 2008. pp. 67–83.
Zakrzewska A, Ferragut E. Modeling cyber conflicts using an extended Petri net formalism. In: Computational Intelligence in Cyber Security (CICS), 2011 IEEE Symposium on; 2011. pp. 60–7.

Ulrik Franke, Ph.D., is a senior scientist at the Swedish Defence Research Agency. His research interests include Enterprise Architecture, the theory and practice of decision-making, information fusion and the impact of ICT on politics and national security. He has published articles in e.g. IEEE Transactions on Network and Service Management, Software Quality Journal, and Enterprise Information Systems.

Joel Brynielsson is a senior scientist at the Swedish Defence Research Agency and an adjunct associate professor at the Royal Institute of Technology (KTH). Joel holds a Ph.D. in Computer Science and an M.Sc. in Computer Science and Engineering from KTH, and previously worked as an assistant professor at the Swedish National Defence College. His research interests include web mining, uncertainty management, information fusion, probabilistic expert systems, decision support, command and control, operations research, game theory, privacy-preserving data mining and computer security education.