Information & Security

Published since 1998

J. Pöyhönen, V. Nuojua, M. Lehto &
J. Rajamäki, vol. 43, no. 2 (2019): 236-256
https://doi.org/10.11610/isij.4318

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations

Jouni Pöyhönen [a] (✉), *Viivi Nuojua* [a], *Martti Lehto* [a],
Jyri Rajamäki [a,b]

[a] *University of Jyväskylä, https://www.jyu.fi/en*

[b] *Laurea University of Applied Sciences, https://www.laurea.fi/en/*

Abstract:

Cybersecurity-related capabilities play an ever-growing role in national security, as well as securing the functions vital to society. The national cyber capability includes the resilience of companies running critical infrastructures, their cyber situational awareness (SA) and the sharing of cybersecurity information required for cyber SA. As critical infrastructures become more complex and interdependent, ramifications of incidents multiply. The EU Network and Information Security Directive calls for cybersecurity collaboration between EU member states regarding critical infrastructures and places the most crucial service providers and digital service providers under security-related obligations. Developing better SA requires information sharing between the different interest groups and enhances the preparation for and management of incidents. The arrangement is based on drawing correct situation-specific conclusions and, when needed, on sharing critical knowledge in the cyber networks. The target state is achieved with an efficient process that includes a three-level—strategic, operational and technical/tactical—operating model to support decision-making by utilizing national and international strengths. In the dynamic cyber environment strategic agility and speed are needed to prepare for incidents.

Article Info:

Received: 12 Jun 2019
Revised: 28 Aug 2019
Online: 22 Sep 2019

Keywords:

cybersecurity, situational awareness, information sharing, critical infrastructure, vital societal functions

✉ E-mail: jouni.a.poyhonen@jyu.fi

Introduction

The capability related to national cybersecurity plays an even more important role when it comes to the overall security and securing the crucial functions of society in the future. The national capability consists of most of the resilience of the critical infrastructure companies and the situational awareness of the cyber environment, they constantly maintain.

The critical infrastructures become more complex and their parts are even more strongly dependent on each other, and that way, the ramifications of the incidents can be multiple compared with the original impact. The operation of critical infrastructure and the threats having an impact on them are not limited to organizations or administrative borders.[18]

The EU Network and Information Security (NIS) Directive [4] increases the collaboration between the member states in the important field of cybersecurity. It puts the most crucial service providers (critical industries such as energy, transport, health, and financing) and digital service providers (online marketplaces, search engines, and cloud computing) of society under the security-related obligations. The application of the Directive results in imposing the security and information requirements concerning the aforementioned operators. The goal is to develop even better situational awareness and information sharing. The critical infrastructure consists especially of the crucial service providers defined by the NIS Directive. In Finland, the administrative sector coordinates the operations required by the Directive, when both monitoring and the duty to notify are decentralized. The National Cyber Security Centre Finland builds situational awareness.

Principally, the functional observation and analysing ability collected from the different trust circles gives a good basis for the development of Finland's national situational awareness, and information sharing.[9] Critical infrastructure can be described as a three-levelled system of systems (Fig. 1); efficient and appropriate operations can be targeted at its three levels, from bottom to the top: power grid, data transmission network, and services.[14]

The situational awareness of critical infrastructure is emphasized also in the Security Strategy for Society,[16] as part of maintaining vital national operations. Efficient incident management requires tight collaboration between the management, situation awareness and communication. Good management requires:

- unquestionable managerial responsibility, the casting of different operators and the decision-making ability of the ministerial authority

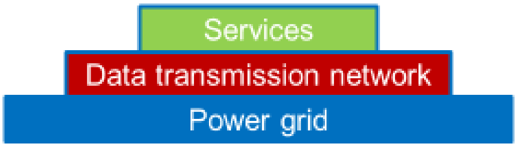

Figure 1: Plain structure of critical infrastructure.

- building of situation awareness (situational understanding, evaluation of situational development)
- crisis communication
- information sharing, and supporting technical solutions
- business continuity management
- co-operation.

Research Purpose, Research Questions, and Article Structure

The research questions deal with the situational awareness and understanding of an organization, as well as the data analysis and information sharing between the different interest groups. The aim is to develop the preparation for incidents and their management in the whole society. The arrangement is based on drawing correct situation-specific conclusions and, when needed, on sharing critical knowledge in the cyber networks of society.

The research questions are:

1. How the cyber situational awareness of an organization can be developed?
2. How do the organizations exchange their cybersecurity-related information?
3. Can an organization's cybersecurity capability be utilised more extensively?

This paper is a continuum of the research "Cyber strategic management in Finland,"[10] in which one task was to formulate management proposals for the management of nationally pervasive incidents concerning cyber environment. Good situational awareness and information sharing between the different interest groups have an essential impact on incident management. The research method was an open theme interview with material-based content analysis. All three levels of the critical infrastructure system of systems (see Figure 1) were represented. There were altogether 40 interviewees from 25 private or public organizations, which were leaders or persons responsible for the information/ cybersecurity of their organizations.

In Finland, the significance of the private businesses is emphasised in the operation of critical infrastructure, since approximately 80 % of the operations can be estimated to belong to their responsibility. Researchers interviewed six private businesses, as well as public authorities, such as the National Cyber Security Centre Finland and the National Emergency Supply Agency.

Section 2 deals with the need for situational awareness, and related decision-making levels and the theory of situational awareness. In Section 3, the information sharing needs of an organization are explored, ever since the national and European Union needs. Section 4 describes the formation of situational awareness into the different levels of an organization, and the information-sharing procedures at the national level. Finally, Section 5 concludes with the conclusion.

Situational Awareness

To function, every organization needs information about its environment and happenings, and also about its impact on its operation. An appropriate and fast situational awareness is based on correct information and evaluations, and it is emphasized in the case of incidents when very pervasive decisions must be made quickly. To make correct solutions, decision-makers have to know the base for their decisions, consequences how the others react to them and what risks the decisions include. For that reason, decision-makers must have sufficient situational awareness and understanding of all the operational levels, which enables timely decision-making and operation. Situational awareness and understanding require collaboration and expertise, which enables the comprehensive monitoring of the operational environment, data analysis, and aggregation, information sharing, recognition of the research needs and network management. The information systems must enable the systematic use of information sources and collaboration and the flexible sharing of situation information related to it.[11]

The organizations' and decision-makers' formation of situational awareness is supported by the situation awareness arrangements. In general, situation awareness means the description of the dominant circumstances and the operational preparedness of different operators aggregated by the specialists, the happenings caused by an incident, its background information and the evaluations concerning the development of a situation. In addition, data analysis based operational recommendations may be related to situation awareness. The general view is constituted by utilizing a networked operational model based on different sources. The process consists of data acquisition, information aggregation, classification and analysis, and of a timely and efficient sharing of the analysed information with those in need. The surrounding data space is organised such that the information is understood correctly, and that the operators have a chance to get the information important to their operation.[11]

The pervasive incidents targeting society are a challenging cyber environment when it comes to the critical reaction speed required by the situation management. Advanced Persistent Threats (APT) are unfamiliar attacks to the traditional protection ways and can proceed quickly when fast information sharing and good situational awareness play an important role in incident management. In a worst-case scenario, the delegation of responsibility should be able to make possible in a few minutes, the response evoked without delay, and the abilities and tools put to use.[12]

Decision-making levels

Organizations operate in very complex, interrelated cyber environments, in which the new and long used information technology system entities (e.g. a system of systems) are utilized. Organizations are depended on these systems and their apparatus to accomplish their missions. The management must recognize that clear, rational and risk-based decision are necessary for business continuity. The risk management at best combines the best collective risk assessments of the organization's individuals and different groups related to strategic planning, and also the operative and daily business management. The understanding and dealing of risks are an organization's strategic capabilities and key tasks when organizing the operations. This requires, for example, the continuous recognition and understanding of the security risks on the different levels of the management. The security risks may be targeted not only at the organization's operation but also at individuals, other organizations and the whole society.[8]

Joint Task Force Transformation Initiative recommends implementing the organization's cyber risk management as a comprehensive operation, in which the risks are dealt with from the strategic to tactical level.[8] That way, risk-based decision-making is integrated into all parts of an organization. In Joint Task Force Transformation Initiative's research, the follow-up operations of the risks are emphasised in every decision-making level. For example, in the tactical level, the follow-up operations may include constant threat evaluations about how the changes in an area can affect the strategic and operational levels. The operational level's follow-up operations, in turn, may contain for example the analysis of the new or present technologies to recognize the risks to the business continuity. The follow-up operations of the strategic level can often concentrate on the organization's information system entities, the standardization of the operation and for example on the continuous monitoring of the security operation.[8]

From the necessity of the organization's risk, follow-up operations can be drawn the necessity of the whole organization's situational awareness. As mentioned, the formation of the organizations' and decision-makers' situational awareness is supported by the situation awareness arrangements. Thus, an appropriate situational awareness supports cyber risk management and more extensively the evaluation of the organization's whole cyber capability.

Theory of Situational Awareness

Mica Endsley has developed a situational awareness model when working on several different research assignments in the service of the United States Air Force.[3] Figure 2 describes the general structure of the model. The core of situational awareness consists of three basic elements: detection (Level 1), situational understanding (Level 2) and its impact assessment towards the future (Level 3). This situational awareness provides the foundation for conclusions and the following decision-making. Depending on the situation, the assignment- and system-specific features and the decision-maker's experience and evaluation ability bring their impacts on the table. Decision-making, in turn, guides the operation that reflects the observed operational environment.

Sid Faber regards the situational awareness development operations, concerning both public and private businesses, as one of the most significant near-future goals aiming to improve cybersecurity.[5] He recommends applying Endsley's model to the follow-up needs of a cyber-operational environment.

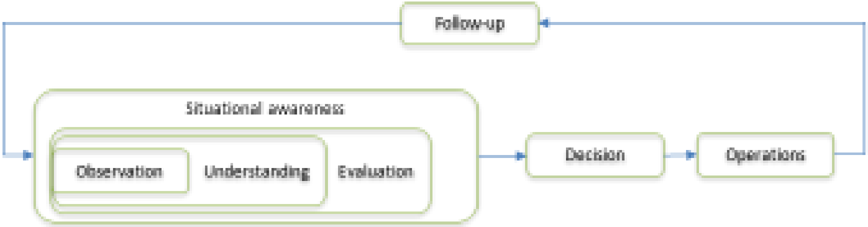

Figure 2: Situational awareness and dynamic decision-making (adapted from Endsley [3]).

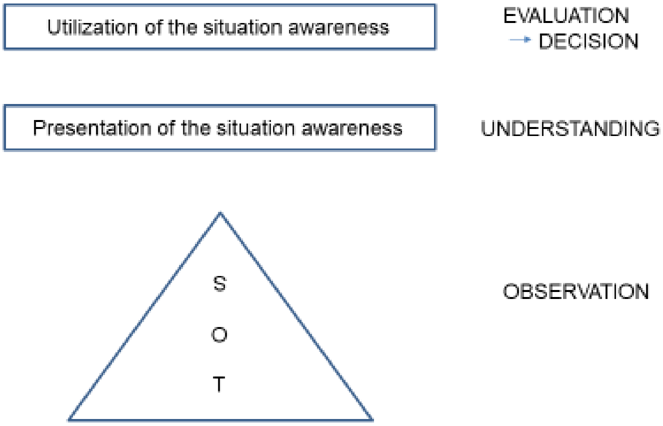
Utilization of the situation awareness
EVALUATION
→ DECISION
Presentation of the situation awareness
UNDERSTANDING
S
O
T
OBSERVATION

Figure 3: Framework for forming situational awareness.

The general structure of Endsley's situational awareness model is applied when solving our research questions.[3] The framework for forming the critical infrastructure situational awareness is introduced in Figure 3. The detection part (Level 1) of Endsley's structure is presented as the organization-specific detection needs of the strategic (S), operational (O) and technical/tactical (T) decision-making levels. The goal is to gain a perception that serves each decision-making level. The situation awareness that is formed of observations is a prerequisite for understanding the observations (Level 2). After that, the impact analysis and assessment of the observations are made possible by utilizing the understanding about situation awareness (Level 3). There, analysis capability plays an important role. The final goal is to make appropriate and situation-specific decisions on each decision-making level and conduct the operations followed by the decisions.

General Requirements for Situation Awareness

Horsmanheimo and co-workers set some requirements for the situation awareness in their research: [6]

- Situation awareness is a series of presentations whose shape does not matter. It is more essential than somebody manages it, makes analysis and decisions.
- Information is brought to the situation awareness system in collaboration. Every operator is independently responsible for the production and validity of the information related to their knowledge area.
- The information must be processed, analysed and understandable. It has to be meaningful for both oneself and other receivers.
- The information must be performed visually and clearly.
- The information must be performed without unnecessary technical details. The information must be understandable for people from other industries.
- Situation awareness system should be dynamic and tailored by users and industries. Information should be able to put on different views.
- Terminology and classifications should be uniform.
- Situation awareness system should be able to be included in the organization processes such that the maintenance of the situation awareness system would not become an extra task in grand incidents.
- Different operators should be able to define what kind of information they need and what kind of information they can input to the system.
- Situation awareness system should be able to be utilised for information exchange between different operators on different organization levels. Information should be able to be shared also with the supervisory organizations.
- The situational awareness system should be able to make predictions of what is happening by 3, 6 or 12 hours.
- The situational awareness system should be able to perform a temporal dimension to how the things have developed – whether the direction is worse or better.

Information Sharing Needs of an Organization

The EU Network and Information Security (NIS) Directive increases the collaboration between the member states in the important field of cybersecurity. It puts the most crucial service providers (critical industries such as energy, transport, health, and financing) and digital service providers (online marketplaces, search engines, and cloud computing) of society under the security-related obligations. The application of the Directive results in imposing the security and information requirements concerning the aforementioned operators. Also, the Directive supports in developing nationally better situational awareness.

The operations of the concerned Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 have been carried out nationally since 2018. The Directive states the subject matter and scopes the following: [4]

1. This Directive lays down measures to achieve a high common level of security of network and information systems within the Union to improve the functioning of the internal market.

2. To that end, this Directive: a) lays down obligations for all Member States to adopt a national strategy on the security of network and information systems; b) creates a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among the Member States and to develop trust and confidence amongst them; c) creates a computer security incident response teams network ('CSIRTs network') to contribute to the development of trust and confidence between the Member States and to promote swift and effective operational cooperation; d) establishes security and notification requirements for operators of essential services and digital service providers; e) lays down obligations for the Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

Principally, a functioning observation and analysing ability composed from different trust circles provides a good starting point for the development of Finland's national situational awareness.[9] By the most crucial service providers' and digital service providers' duty to notify, the national situational awareness can be developed. The duty to notify expands the previous procedure considerably and therefore covers a significant part of the critical infrastructure by private businesses. Also, the operation involves information sharing between the authorities, and more than before between the authorities and private business operators. In Finland, the operations required by the Directive relate to sector-specific laws and, consequently, their monitoring as well as the duty to notify happen sector-specific. The laws include the definitions of the crucial service providers' duty to notify. The situational awareness is built by the National Cyber Security Centre Finland.

The National Cyber Security Centre Finland

The National Cyber Security Centre Finland (NCSC-FI) is part of the Finnish Transport and Communication Agency, Traficom. Traficom is an authority in a permit, license, registration, and monitoring of transport and communication. It promotes traffic safety and the smooth functioning of the transport system and speeds up the development of digital society. Also, the agency supports sustainable development and ensures that everyone in Finland has access to high-quality and secure communications connections and services.[17]

Nationally, the NCSC-FI plays the most crucial part in forming and analysing the cyber situational awareness, and in incident management. It has three main tasks:

1. The NCSC-FI acts as a national communications security authority (NCSA) and is responsible for the security matters related to the electrical data transmission and processing of the safety-classified material. The NCSA operation is part of Finland's security authority organization.
2. The CERT (Computer Emergency Response Team) operation of the NCSC-FI takes care of the prevention, investigation and announcement tasks in case of information security breaches. The main purpose of the CERT operation is to produce and maintain the cyber situation awareness together with domestic and foreign cooperation partners and counterparts. As an essential part of

the CERT operation, the NCSC-FI acts as a national point of contact for information security breaches and threats. It also investigates these cases and helps the concerned parties.

3. The NCSC-FI manages the information security regulation tasks of Traficom. It acts as a national regulatory authority (NRA), i.e. as a guiding and monitoring authority.

The NCSC-FI is an authority that aggregates and builds national situational awareness. It collaborates closely with other authorities and private business operators.

HAVARO is a service that detects and warns about information security breaches, serves the critical companies for security of supply and the state administration. From the HAVARO system, the NCSC-FI has visibility to practically all the upcoming and outgoing traffic (metadata and content data). Many critical companies for security of supply and the state administration operators have put to use the HAVARO service, which indicates the trust in the NCSC-FI. That way, the information security breaches targeted at the organization can be reported automatically to the authority without a chance for censoring the incidents beforehand. The system has been implemented in collaboration with the National Emergency Supply Agency.

The companies and public administration operators participate in the HAVARO operation voluntarily. The operation of the system is based on the information security threat identifiers coming from different sources. With the help of the identifiers, harmful or anomalous traffic can be detected from the organization's network traffic. The NCSC-FI receives information about the anomalies and analyses them. In case of an information security threat, the organization is warned about it. Based on the information got from the HAVARO, also the other operators can be warned about the detected threat. That way, the system helps not only individual organizations but also in forming a general view about the information security threats against Finnish information networks.

The observation ability of information security threats is an important part of comprehensive risk management. For its part, HAVARO secures the organization's business continuity against the threats of the operational environment. However, HAVARO is not meant to be an organization's only information security solution, but it is designed to complete the other information security solutions of information security investing organization.

Also, Traficom provides the *GovHAVARO* service for the state administration operators. It completes the information and cybersecurity threat detection of the state administration's Internet traffic. The service providers are Traficom, Valtori – Government ICT Centre and Telia. The *GovCERT* services, in turn, support the state's round-the-clock information security operation by producing the support services for preventing, detecting and investigating information security breaches, as part of the GovSOC operation. They are provided by Traficom and Valtori.[7]

The incident management of the state administration and other public administration organizations, so-called VIRT operation, is a cross-administrative operational level collaboration, which prepares for severe and extensive information security incidents. It consists of operational planning and rehearsing for different information security incidents.[7]

The industry-specific cyber information-sharing groups (ISAC, Information Sharing and Analysis Centre) are established as collaboration organs between the organizations of different industries. Their operation enables:

1. Confidential handling of information security matters between the participants.
2. Augmentation of the organizations' information security know-how.
3. Development of the NCSC-FI's overall situational awareness.

The ISAC operation is based on regular meetings and specified operational models and participants. The ISAC information sharing groups have been established for the following industries: state administration (VIRT), Internet service providers, chemistry and lumber industry, banks, media, energy industry, food production and distribution, social and health care, and software manufacturers.

The National Emergency Supply Agency

The National Emergency Supply Agency (NESA) is an institution working under the Ministry of Economic Affairs and Employment of Finland. It is tasked with planning and operations related to maintaining and developing the country’s security of supply. As part of the security of supply organization, the NESA’s mission is to support the operation of the pools and sectors and to take care of the other legislative tasks given to it. Security of supply means the ability to maintain such economical basic operations of society that are necessary for securing the populations' living prospects, society's functioning and safety, and the material prerequisite for national defence in severe incidents and extraordinary circumstances.[13]

The national cybersecurity management requires a close-knit collaboration between the critical infrastructure operators (Public-Private Partnership, PPP). The NESA's information society pools take care of the collaboration.

Formation of Situational Awareness

The analysed collection of data was created based on interview material, document analysis, and international comparison information. The observations, presentations, and models presented in this article, are based on this data.

Situational Awareness on a Tactical Level

Both technical, networked and management situation awareness are emphasized when building the situational awareness. During the last years, Finland has formed its cyber situation awareness through the information-sharing mechanisms of different operators. It is about national and international collaboration. The improvement of information sharing and perception is still a matter of development when it comes to Finland's cybersecurity.[9]

The critical infrastructure operators use such protection techniques in their ICT systems that extend from the interface of the Internet and the organization's internal network right up to the protection of a single workstation or apparatus. These technical solutions make it possible to verify different harmful or anomalous observations. The typical technologies are related to security products such as network traffic analysis and log management (Security Information and Event Management, SIEM), firewall protection, intrusion prevention and detection systems (IPS and IDS) and antivirus. The situation awareness builds up to centralized monitoring rooms (Security Operations Centre, SOC). These technical solutions can be under the organization's control, or the service can be outsourced to the information security operator. A crucial goal is the situational awareness and protection of the business processes.

Also, especially the critical companies for security of supply have the HAVARO system in the external interface of their network. The system follows the network traffic and detects harmful and anomalous traffic. Then, the warnings come from the NCSC-FI.

The observation ability relates also to a so-called advance warning that can be received from the organization's international or national operation networks. In the centre of operation, there is always the organization's capability to pay attention to the abnormal operation that possibly occurs in the system. The overall observation ability is developed for example by benchmarking and practicing.

The organizations implement the analysis of incidents and anomalies from their own starting points, at the hands of their own or carried out by the service provider. The analysing ability requires more and more the securing of the organization's business process operation. The intensification of protection operations or for example the introduction of alternative operational models are the most important goals of the operation. The analysing capability determines the choice of needed operations and, that way plays an important role in the organization's decision-making process. The analysing ability must enable a severity classification and so-called cyber-physical view.

The analysing usually happens in centralized monitoring rooms (Security Operations Centre, SOC) based on situational awareness. In the monitoring rooms, the information coming from different sensors is aggregated and a situation-specific analysis is formed. Based on the analysis the needed operations are launched. The organization's possibilities to utilize the information gotten from international or national operational networks relate to the analysing ability. The personnel's capability to interpret the available observations correctly has a significant meaning in composing situation-specific analyses.

A typical reaction to an incident or anomalous operation comes at first from an incident response manager based on the situation awareness and its analysing. The magnitude and severity of an incident have an impact on the operations. Besides fast-reacting, the organization's management can be congregated to decide on the extension of the operations, and the allocation of the needed resources. Depending on the magnitude of an incident, the whole organization's management to the supervising board can be informed. Regarding the publicly traded companies, the organization's external informing is guided by the informing obligations based on the law.

In the case of a nationally extensive incident, the critical infrastructure organizations keep in touch with the NCSC-FI and utilize not only the authority network but also the industry's network and their business networks. In this communication, the organization's situation awareness and its situation-specific analysing are combined.

Part of the critical companies for security of supply have a communication demand for authorities, such as NCSC-FI, in case of an incident. Based on the NIS Directive, an authority can expand this demand to the critical infrastructure organizations whom the duty to notify does not yet apply.

Developing Competences for Situational Awareness of the Organization

The nationally significant critical infrastructure organizations have developed in forming the cyber situational awareness and observation ability concerning the technical and tactical preparedness. It is also improved by the industry-specific and even more large-scale networking of the organizations. Networking and information sharing are supported by a functional collaboration between the authorities and the private sector. The good situational awareness of different companies (situational awareness and its analysing) and the information sharing via their interest groups is, indeed, a crucial factor in the whole national cybersecurity. Figure 4 sums up the factors that have come up in this research and further the organization's tactical level cybersecurity. The starting point is always the capability of the organization's personnel in recognizing the possible anomalous activity in the used systems and in operating reliably and organized in different situations. In an ideal case, the operation is supported by the technical systems or the used services of the ICT or information security operators or by utilizing the operational network, participating in the authority collaboration, utilizing the consulting services or benchmarking or testing and exercising the operation.

Operational Level Situational Awareness

The operational level operations are used to advance strategic goals. Comprehensive security- and trust-adding operations require comprehensive cybersecurity management. Its starting point has to be the target's risk assessment, and the operation analyses carried out based on it. The operational level's concrete hands-on operations must be targeted at the confirmation of information security solutions and the composition of the organization's continuity and disaster recovery plans. The goal has to be the continuous monitoring of the operational processes' usability, and the decision-making support in case of incidents that require analysing and decisions.

The NCSC-FI and NESA are identified as state administrative point of contacts on the business level. The NESA and different pools, especially the digital pool, support companies in developing and maintaining the situation awareness of the cyber operational environment. Because of the operation goals, the NESA brings together a significant part of the authorities and IT businesses. The private sector

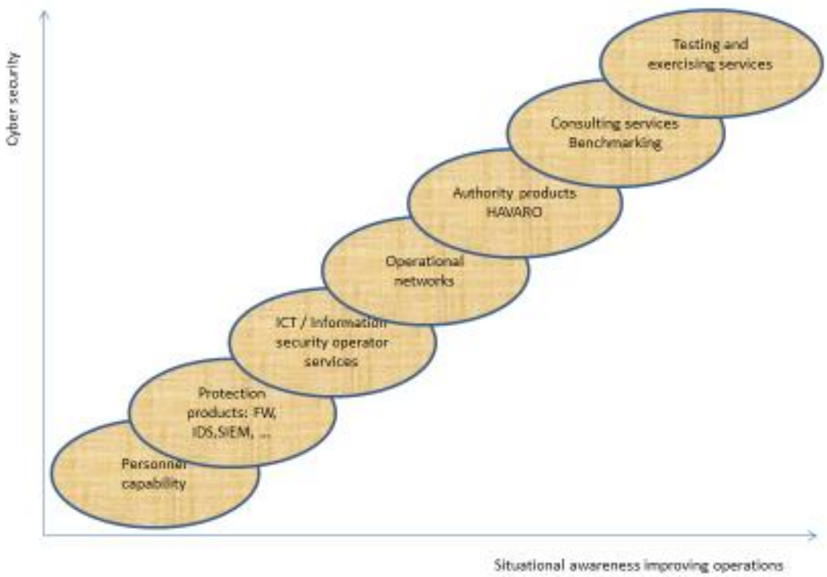
Cyber security
Testing and exercising services
Consulting services Benchmarking
Authority products HAVARO
Operational networks
ICT / Information security operator services
Protection products: FW, IDS,SIEM, ...
Personnel capability
Situational awareness improving operations

Figure 4: Development of an organization's cyber situational awareness as part of comprehensive cybersecurity.[10]

recognizes its tasks in advancing national cybersecurity. The collaboration models between the authorities and private businesses have been created, and they are internationally comparable.

With the support of the authorities, have been developed not only HAVARO for the security of supply critical operators but also KRIVAT service for critical infrastructure organizations such that the operators themselves form the network. The purpose is to strengthen the collaboration between organizations in grand incidents and speed up the recovery from them.

The technical protection ability of the most significant critical infrastructure organizations and the observation ability based on that are on a good level. Different collaboration networks are widely used. Organizations and the NCSC-FI keep in touch regularly. The analysing ability of anomalous operation and the incident management ability base on the capable personnel and functional collaboration networks.

Situational Awareness at Uppermost Management Level

One of the most fundamental cybersecurity tasks of the organization's uppermost management is the continuous development and maintaining of the trust in operation as part of the national critical infrastructure. The strategic choices relate to the reputation of an organization. The management is required to make concrete strategic choices and to support and guide the performance of the chosen operations through the whole organization. An important task of the management is to take care of the adequate resourcing of operations. About the chosen operations must be communicated extensively with the organization's personnel and other interest groups.

It is important to create a cybersecurity assessment model for the needs of the uppermost management. With the help of that model, for example, other organizations can evaluate their cybersecurity level, become aware of their weaknesses and insufficient contingency planning, and take care of at least of the basics. The operations require strategic level decisions from the organization's uppermost management.

Finland's national cybersecurity execution program 2017–2020 aggregates the pervasive and significant information and cybersecurity improving projects and operations of the state administration, business, and associations, and their responsibilities. The progress of the execution program can be followed by following the development of the different organization's capabilities during the concerned inspection period. The execution program includes extensively effective operations that are developed by other administrative-specific operations, and by the work related to the development of cyber and information security and business continuity management. At the same time, the follow-up results in the formation of national cyber situational awareness.[10, 15]

The National Cyber Security Index (NCSI) is developed for the follow-up of the national cybersecurity-related capability. It is based on twelve sectors that are sorted into four groups as follows: [2]

- General cybersecurity indicators
- Cybersecurity basic indicators
- Event and crisis management indicators
- International event indicators

The NCSI index has four cybersecurity viewpoints per every twelve sections. These are the effective legislation, functioning individuals, collaboration arrangements and the results from different processes. The operation of the index is based on the evaluations of the specialist group.

Table 1 introduces a measure that is based on the NCSI index. It measures the cybersecurity capability of an organization and is developed for the use of businesses and other organizations. The evaluation is based on the requirements, business, interest group collaboration and results. In this organization measure, the twelve sectors of cybersecurity are arranged into four groups as follows:

1. General indicators
2. Basic level indicators
3. Event and incident management indicators
4. National impact indicators.

The commissioning of the measure can be seen to be targeted at the national cybersecurity execution program's goal "A national light cybersecurity evaluation, by which the organizations can take care of reaching the minimum level of security, has been composed." By the organization-specific commissioning of the

Table 1. Structure of an organization-specific measure.

	Requirements	Business	Interest group collaboration	Results
GENERAL INDICATORS				
Ability to develop the organization's cybersecurity culture				
Ability to analyse its cyber environment				
Magnitude of cybersecurity training				
BASIC LEVEL INDICATORS				
Confirmation of operational resources				
Risk assessments				
Quality requirements of the information systems' operation				
Operation follow-up and measures				
EVENT AND INCIDENT MANAGEMENT INDICATORS				
Quality of contingency planning for incidents				
Situational awareness 24/7				
Ability to manage incidents				
Ability to recover from incidents				
NATIONAL IMPACT INDICATORS				
Operation in cyber operational networks				
POINTS				

measure, the aforementioned goal can be seen as achieved. The widespread commissioning of the measure in critical infrastructure organizations would make it possible to follow the cybersecurity development of the whole area in the same way as it serves the strategic level needs of a single organization.

Information Sharing on National Level

The NIS Directive requires explicit, identifiable and concrete operations to develop the national situational information sharing. The identification of collaboration partners and information producing operators generates prerequisites for society's encompassing information sharing and, that way, for the development of situational awareness. Figure 5 introduces a national information-sharing structure that enables the NIS Directive-based operation.

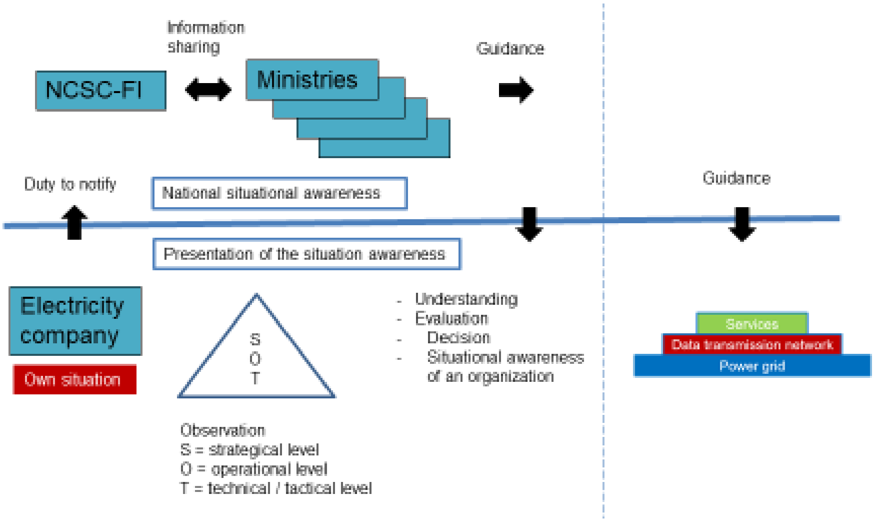

Figure 5: Information sharing on a national level.

The European EECSP report "Cyber Security in the Energy Sector" encourages to use the best practices of information sharing through some kind of analysing centre or analysing the process. Thus, the best practice sharing via interest groups and learning from that can be supported. The challenges related to the introduction of new technologies, the challenges caused by the mutual dependence of the market operators, or the challenges build-up by the links between the energy systems and networks are typical scenarios that can especially benefit from the sharing of best practices. Also, the procedure can be used for sharing delicate information that helps the operators in protecting their network proactively.[1]

In national information sharing, a critical infrastructure organization (electricity company in Figure 5) forms a cyber situation awareness from its starting points. In an ideal case, it bases on the observations from the different levels of the organization that is strategic, operational and technical/tactical level. Based on the information, the electricity company maintains its continuous situational awareness to support its decisions. In case of a cyber incident, the electricity company delivers information about its situation-specific analysis, based on the duty to notify, to the NCSC-FI and when need also to the responsible ministry. Based on their mutual information sharing, the NCSC-FI and responsible ministry form a national situational awareness about the matter. The responsible ministry takes care of the related and needed guidance operations to the other interest groups and the organizations of its area of responsibility. The NCSC-FI carries out continuous information sharing with the critical infrastructure organizations about the cybersecurity situation.

Finland's national strength in the organizations' possibilities in utilizing different networks when sharing the cybersecurity information has been emphasized in different researches.[9, 10] Here, three confidential information-sharing networks that are utilized actively are introduced. These have been formed in connection with business operation, or a separate trust circle has been established between some industry's companies that can reach also into an international collaboration. Also, nationally operates a trust circle between the authorities and private sector (Public-Private Partnership, PPP). Figure 6 illustrates the aforementioned trust circles in the company field.

The critical infrastructure organizations have functioning situation awareness arrangements and analysing capability, and they exchange information by utilizing their networks and are capable of incident management based on their starting points. The risk assessments and the procedure option analyses based on the evaluations are a significant part of the continuity management of the organization's business processes. The concrete hands-on operations of the operational level must be targeted at securing the information security solutions and composing the organization's operational continuity and disaster recovery plans. The goal must be in the continuous follow-up of the operational processes' usability, and the contingency planning for incidents.

The cyber operational environment is dynamic, which means that especially the strategic agility is required when preparing for incidents. On the other hand, the organization's strategic decision-making level must also have tools for evaluating the development of the whole organization's cybersecurity. In this paper, the commissioning of the measure that follows the organization-specific capability is recommended. There, the evaluation is carried out via the requirements set for the

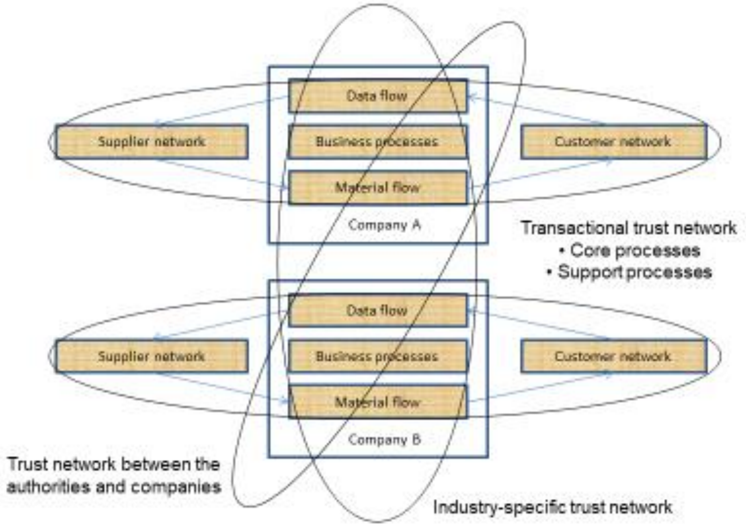

Figure 6: Trust networks related to an organization's cyber situational awareness development.

operation, business, interest group collaboration and results by utilizing four indicators. The four indicators have been derived from this cybersecurity measure from the international index, and they are the organization's general indicators, basic level indicators, event and incident management indicators, and national impact indicators.

Summary

The main novelty value of this study is the promotion of their practical measures which the NIS Directive required. In the big picture, the different parties related to the development of situational awareness must yet be able to improve their operation by even more efficient technical procedures, strengthen the network-like operation, and increase the utilization of public sector services. There will be good preconditions to the above-mentioned matter when cybersecurity capabilities of the organization are widely promoted as a part of the national critical infrastructure and the common objectives determined by the EU.

For the first research question, it is stated that as the target state of the organization’s cyber situational awareness and its interest groups' information sharing can be set the operation where the recognition of threatening incidents and reacting to them happens in an efficient process. It must include all the organization’s decision-making levels (strategic, operational and technical/ tactical) and utilize the national and international strengths of information sharing.

Based on the research the following basic requirements apply to the development of the organization’s incident management:

- Strategic goals: a) Cybersecurity management in all circumstances; b) Strategic choices for operational continuity management
- Critical success factors: a) Good situational awareness on all the organizational levels; b) Fast reaction ability and executive guidance; c) Clear operational models and their sufficient resourcing; d) Good information sharing between the different interest groups; e) Crisis communication
- Evaluation criteria and target levels: a) Effectivity of the operation; b) Optimal resourcing.

For the second research question, the techniques used by organizations, procedures developed for incident reacting and different trust circles form a nationally useful observation ability. This scattered organization-specific observation ability and the analysing information and data reserve it contains can be utilised nationally in the analysing phase for the management of wide-scale incidents. The arrangement requires the creation of mutual operational models for information sharing. Because it is very presumable that there are not enough centralized resources to be used for analysing a wide-scale and quickly evolving cybersecurity incident, as a solution should be outlined a network-like operation consisting of the experts from different organizations (virtual analysing). Then, the data reserve should be jointly used, and the experts would use their trust circles that reach to the international information sharing relations. The usability of data reserve forms the key for analysing. When building it must take into account not only confidentiality but also the data integrity and amount questions. In the referenced research, the evaluations of i.e. the formation of excessive data amount were presented, and then the analysing becomes more difficult too. Thus, the different technical solutions of data processing should be examined.

For the third research question, the main conclusion is that the organization-specific measures, which promote cybersecurity and situational awareness, make the filling of the obligations of the NIS directive (Part D) possible. Part D requires that the providers of central and/or digital service should take into use the security and notification requirements. In every member state, national and EU -level situational awareness is based on the ability to maintain situation consciousness. Thus, the measures presented in this study also will promote other objectives appointed by the NIS directive.

Acknowledgements

The part of the work performed by Laurea University of Applied Sciences was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943.

References

[1] EECSP Expert Group, "Cyber Security in the Energy Sector," Europe: Energy Expert Cyber Security Platform (EECSP), 2017.

[2] e-Governance Academy, "National Cyber Security Index (NCSI)," 2017, https://ncsi.ega.ee/, accessed August 6, 2019.

[3] Mica R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors and Ergonomics Society* 37, no. 1 (1995): 32-64.

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, *Official Journal* L 194, July 19, 2016, https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[5] Sid Faber, "Flow Analysis for Cyber Situational Awareness," Software Engineering Institute, Carnegie Mellon University, December 7, 2015, https://insights.sei.cmu.edu/sei_blog/2015/12/flow-analytics-for-cyber-situational-awareness.html, accessed August 6, 2019.

[6] Seppo Horsmanheimo, Heli Kokkoniemi-Tarkkanen, and Jouko Vankka, "Kriittisen infrastruktuurin tilannetietoisuus (Situational Awareness of Critical Infrastructure)" (Helsinki: Prime Minister's Office, 2017).

[7] Kirsi Janhunen, "Valtionhallinnon häiriötilanteiden hallinta - miten VIRT-toimintaa kehitetään?" (Helsinki: Ministry of Finance, 2015).

[8] Joint Task Force Transformation Initiative, “Managing Information Security Risk – Organization, Mission, and Information System View,” NIST Special Publication 800-39 (Gaithersburg, MD: National Institute of Standards and Technology, 2011).

[9] Martti Lehto and Jarno Limnéll, “Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi (Finland’s Cyber Security: The Present State, Vision and the Actions Needed to Achieve the Vision)” (Helsinki: Prime Minister's Office, 2017).

[10] Martti Lehto, et al., “Kyberturvallisuuden strateginen johtaminen Suomessa (Strategic Management of Cyber Security in Finland)” (Helsinki: Prime Minister's Office, 2018).

[11] Ministry of Defence of Finland, “Yhteiskunnan turvallisuusstrategia (The Security Strategy for Society)” (Helsinki, Ministry of Defence, 2010).

[12] National Audit Office of Finland, “Kybersuojauksen järjestäminen” (Helsinki, National Audit Office of Finland, 2017).

[13] National Emergency Supply Agency – Organisation, www.nesa.fi/organisation/, accessed August 6, 2019.

[14] Jouni Pöyhönen and Martti Lehto, “Cyber Security Creation as Part of the Management of an Energy Company,” *16th European Conference on Cyber Warfare and Security*, Dublin, 2017, pp. 332-340.

[15] The Security Committee, “Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020 (Implementation Programme for Finland’s Cyber Security Strategy for 2017-2020)” (Helsinki: The Security Committee, 2017).

[16] The Security Committee, “Yhteiskunnan turvallisuusstrategia (The Security Strategy for Society)” (Helsinki, The Security Committee, 2017).

[17] Traficom – About us, https://www.traficom.fi/en/traficom/about-us, accessed August 6, 2019.

[18] Kirsi Virrantaus and Hannes Seppänen, “Yhteiskunnan Kriittisen Infran Dynaaminen Haavoittuvuusmalli,” Helsinki, Matine, Apr 10, 2014.

About the Authors

Jouni **Pöyhönen** holds an MSc. Degree in Industrial Development and Management. Retired Colonel, he is currently PhD student in cybersecurity in the Faculty of Information Technology at the University of Jyväskylä. He has over 30 years' experience as developer and leader of C4ISR Systems in the Finnish Air Forces. He conducts project-based research in the cybersecurity programs, and has already published several related research reports and articles.

Viivi **Nuojua** holds an MSc degree in statistics and works as information security specialist in the Jyväskylä Energy Group. She works in the group's development function, in a close collaboration with the IT management. She is part of the information security steering group and technical information security group, involved in the group's comprehensive cyber security development. She is also PhD student in Cybersecurity in the Faculty of Information Technology at the University of Jyväskylä.

Martti **Lehto** is retired Colonel holding PhD in Military Sciences, with over 40 years' experience in C4ISR Systems in the Finnish Defence Forces. Currently he is Professor (cyber security and defence) in the University of Jyväskylä, conducting research, teaching and managing the M.Sc. Security and Strategic programme. He is also Adjunct professor in National Defence University in air and cyber warfare, with over 140 publications on the areas of C4ISR systems, cyber security and defence, information warfare, artificial intelligence, air power and defence policy.

Jyri **Rajamäki** is Principal Lecturer in Information Technology at Laurea University of Applied Sciences and Adjunct Professor of Critical Infrastructure Protection and Cyber Security at the University of Jyväskylä, Finland. He holds D.Sc. degrees in electrical and communications engineering from Helsinki University of Technology and a PhD in mathematical information technology from University of Jyväskylä.