Cyber Situational Awareness in Critical Infrastructure Organizations

Jouni Pöyhönen[1], Jyri Rajamäki[2], Viivi Nuojua[1] and Martti Lehto[1]

[1]University of Jyväskylä

[2]Laurea University of Applied Sciences

Abstract The capability related to cybersecurity plays an ever-growing role on overall national security and securing the functions vital to society. The national cyber capability is mainly composed by resilience of companies running critical infrastructures and their cyber situational awareness (CSA). According to a common view, components of critical infrastructures become more complex and interdependent on each other, and that way, ramifications of incidents multiply. In practice, the actions relate to developing better CSA and understanding of a critical infrastructure organization. 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 target state is achieved with an efficient process that includes a three-leveled (strategic, operational and technical/tactical) operating model related to the organization's decision-making. Cyber environment is dynamic meaning that especially the strategic agility is required when preparing for incidents. The pervasive incidents targeting society are a challenging cyber environment when it comes to the critical reaction speed required by the situation management.

1 Introduction

The national cybersecurity capability is vital for overall security of society and securing its crucial functions. Mostly, the national cybersecurity capability consists of resilience of private critical infrastructure (CI) companies, and of the cyber situational awareness (CSA) they constantly maintain. CI can be described as a three-leveled 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 (Pöyhönen & Lehto, 2017). It is generally supposed that CI becomes more complex and its parts are increasingly dependent on each other, and

that way, the ramifications of the incidents can be multiple compared with the original impact. The operation of CI and the threats having an impact on it are not limited only on organizations or administrative borders (Virrantaus & Seppänen, 2013).

Fig. 1. Plain structure of critical infrastructure.

An efficient incident management requires tight collaboration between the management, situational awareness (CA) and communication. A good management requires: 1) unquestionable managerial responsibility, casting of different operators and decision-making ability of the ministerial authority, 2) building of situation awareness (situational understanding, evaluation of situational development), 3) crisis communication, 4) information sharing, and supporting technical solutions, 5) business continuity management, and 5) co-operation.

This study is a continuum of the research 'Cyber strategic management in Finland' (Lehto, et al., 2018), in which one task was to formulate management proposals for the management of nationally pervasive incidents concerning cyber environment. A good CSA has an essential impact on the incident management. The collection of research data was created on the basis of open theme interviews with a material-based content analysis, a document analysis and international comparison information. All three levels of the CI system of systems (see Fig. 1) were represented. There were altogether 40 interviewees from 25 private or public Finnish organizations, who were leaders or persons responsible for the information/cyber security of their organizations. The observations, presentations and models presented in this article, are based on qualitative analysis of this data.

The research questions of this study are:

1. How the cyber situational awareness of a CI organization can be developed?
2. What kind of cyber situational awareness challenges exist in CI?

In Finland, the significance of the private businesses is emphasized in the operation of critical infrastructure, since approximately 80% of the operations can be estimated to belong to their responsibility. During the research, six private businesses were interviewed, as well as public authorities, such as the National Cyber Security Centre Finland (NCSC-FI) and the National Emergency Supply Agency (NESA). Section 2 deals with the need for SA, related decision-making levels, and the SA models applied in this study. In Section 3, the formation of situational awareness in Finnish critical infrastructure organizations are explored. Section 4 discusses the challenges of SA in critical infrastructure. Section 5 concludes this study.

2 Fundamentals of situational awareness

In order to function, every organization needs information about its environment and events, and also about their impact on its own operation. An appropriate and fast SA is based on correct information and evaluations, and it is emphasized in case of incidents when very pervasive decisions must be made quickly. In order 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 SA and understanding on all the operational levels, which enables a timely decision-making and operation. SA 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. (Ministry of Defence, 2010)

The organizations' and decision-makers' formation of SA is supported by the situation awareness arrangements. In general, SA 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 SA. 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 analyzed information with those in need. The surrounding data space is organized such that the information is understood correctly, and that the operators have a chance to get the information important to their operation. (Ministry of Defence, 2010)

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 are unfamiliar attacks to the traditional protection ways and can proceed quickly, when a fast information sharing and good SA play an important role in the 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. (National Audit Office of Finland, 2017)

2.1 Decision-making levels

Organizations operate in very complex, interrelated cyber environments, in which the new and long used information technical system entities (e.g. system of systems)

are utilized. Organizations are depended on these systems and their apparatus in order to accomplish their missions. The management must recognize that clear, rational and risk-based decisions are necessary from the point of view of business continuity. The risk management at best combines the best collective risk assessments of the organization's individuals and different groups related to the 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 own operation but also at individuals, other organizations and the whole society. (Joint Task Force Transformation Initiative, 2011)

Joint Task Force Transformation Initiative (2011) 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. That way, the 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 emphasized 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 in order 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. (Joint Task Force Transformation Initiative, 2011)

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

2.2 Situational awareness models

Endsley (1995) has developed a SA model when working on several different research assignments in the service of United States Air Force. Fig. 2 describes the general structure of the model. The core of SA consists of the three basic elements: detection (Level 1), situational understanding (Level 2) and its impact assessment towards the future (Level 3). This SA 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 experiences and evaluation ability bring their own impacts on the table. Decision-making, in turn, guides the operation that reflects back to the observed operational environment.

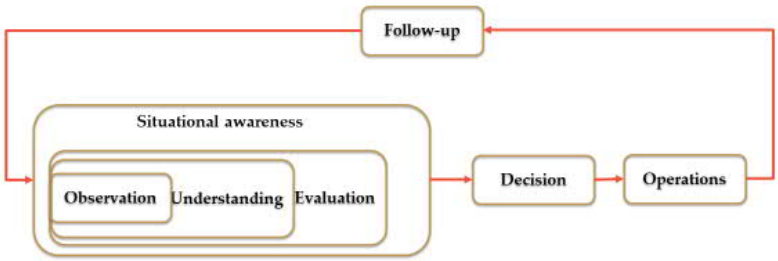

Fig. 2. Situational awareness and dynamic decision-making [adapted from Endsley (1995)].

Faber (2015) regards the SA development operations, concerning both public and private businesses, as one of the most significant near future goals aiming to improve cyber security. He recommends applying Endsley's model to the follow-up needs of a cyber operational environment.

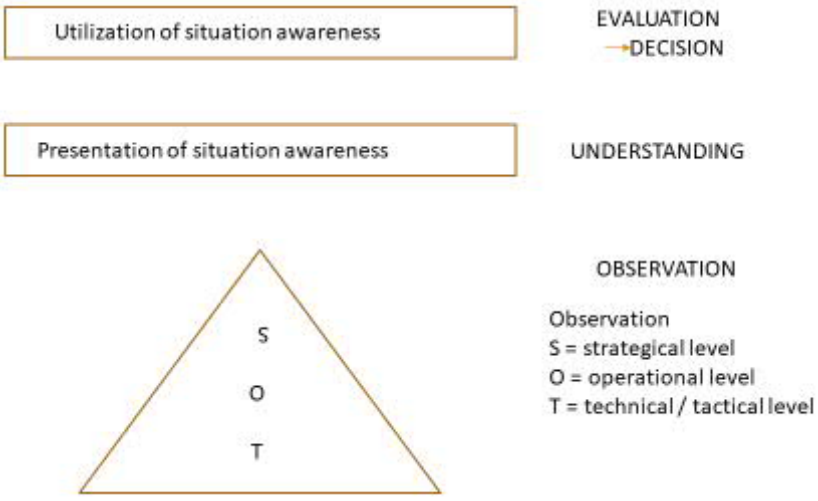

Fig. 3. Framework for forming situational awareness.

The general structure of Endsley's SA model is applied when solving this study's research questions. The framework for forming of critical infrastructure SA is introduced in Fig. 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 perception that serves each decision-making level. The SA that is formed of observations is a prerequisite for understanding the observations (Level 2). After that, the impact analy-

sis and assessment of the observations is made possible by utilizing the understanding about situation awareness (Level 3). There, the 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.

3 Formation of SA in a critical infrastructure organization

This section explores the formation of SA in Finnish critical infrastructure organizations. Examinations are made at the technical/tactical, operational and strategic decision-making levels.

3.1 Situational awareness on a tactical level

Both technical, networked and management situation awareness are emphasized when building SA. 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 cyber security. (Lehto, et al., 2017)

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

In addition, the critical companies for security of supply have the Finnish cyber threat prevention mechanisms *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 so called advance warning that can be received from the organization's international or national operation networks. In a center 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 and at the hands of their own or carried out by the service provider. Securing of organizations' business process operations requires more and more ability of analyzing. The intensification of protection operations or for example the introduction of alternative operational models are the most important goals of the operation. The analyzing capability determines the choice of needed operations and, that way, plays an important role in the organization's decision-making process. The analyzing ability must enable a severity classification and a cyber-physical view.

The analyzing is based on SA and usually happens in SOCs, where the information coming from different censors 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 the international or national operational networks relate to the analyzing ability. Personnel's capability to interpret available observations correctly has a significant meaning in composing situation-specific analyses.

A typical reaction to an incident or anomalous operation comes from an incident response manager based on SA and its analyzing. 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 organization's whole management all the way 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 case of a nationally extensive incident, the CI organization in question keeps in touch to the NCSC-FI, and utilizes not only the authority network but also the industry's own network and its business networks. In this communication, the organization's SA and its situation-specific analyzing are combined.

The companies that are critical for emergency supply have a requirement to inform authorities, such as NCSC-FI, in case of an incident. Based on the Directive on security of network and information systems (NIS Directive), an authority can expand this demand to the critical infrastructure organizations whom the duty to notify does not yet apply.

3.2 Situational awareness on an operational level

The operational level operations are used to advance the strategic goals. The comprehensive security- and trust-adding operations require a comprehensive cyber security management. Its starting point must 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 must be continuous monitoring of the operational processes' usability, and the decision-making support in case of incidents that require analyzing and decisions.

NCSC-FI and NESA has been identified Finland's administrative point of contacts on the business level. NESA with different pools, especially the digital pool of Finland, support companies in developing and maintaining CSA. Because of the operation goals, NESA brings together authorities and IT businesses. The private sector should recognize its own tasks to advance national cyber security. Finnish collaboration models between authorities and private businesses have been created, and they are internationally comparable.

The KRIVAT—information sharing network between critical infrastructure companies—service of the State Security Networks Group Finland is an example of an information sharing and cooperation framework, which is specifically designed for the management of disturbances and continuity of CI operations. It, thus, exists to specifically enhance the preparedness of CI. KRIVAT is a framework for action, and its main purpose is to supplement the existing preparedness and disturbance-management activities of critical infrastructure operators during major disturbances. It responds to a recognized need for clearer communications structures and better situation awareness between organizations for disturbance management. Finland is one of a few countries where CI companies are, in case of disruptions, required to cooperate with one another, and facilitating open information sharing is key to the KRIVAT community. (Ruoslahti, et al., 2018).

The technical protection ability of most significant CI organizations and the observation ability based on that are on a good level in Finland. Different collaboration networks are widely used, and organizations keep in touch with NCSC-FI regularly. The analyzing ability of anomalous operation and the incident management ability are base on capable personnel in CI companies and functional collaboration networks.

3.3 Situational awareness on an uppermost management level

CI organizations' uppermost management should continuous develop and maintain the reliability of their piece of the national CI. The strategic choices relate to the reputation of an organization. The management must make concrete strategic choices and 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. By the model, other organizations may evaluate the company's cybersecurity level, and management can become aware of the company's weaknesses and possible insufficiencies in contingency planning, and take care at least of the basics. The operations require strategic level decisions from the organization's uppermost management.

Finland's national cyber security execution program 2017–2020 aggregates the pervasive and significant information and cyber security 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 the national cyber SA. (The Security Committee, 2017) (Lehto, et al., 2018)

The implementation programme for Finland's cybersecurity strategy for 2017-2020 expresses the need for a light cybersecurity evaluation tool by which organizations are able to take care of reaching the minimum level of security. The National Cyber Security Index (NCSI) was developed for the follow-up of the national cyber security related capability. It is based on twelve sectors that are sorted into four groups as follows: 1) General Cybersecurity indicators, 2) Cybersecurity basic indicators, 3) Event and crisis management indicators, and 4) International event indicators (e-Governance Academy, 2017). The NCSI index has four cybersecurity viewpoints per each twelve sections: 1) effective legislation, 2) functioning individuals, 3) collaboration arrangements, and 4) the results from different processes. Table 1 introduces the measure tool that is based on the NCSI index. It measures the organization's cybersecurity capability. The tool is developed for the use of businesses and other organizations. The evaluation is based on the requirements, business, interest group collaboration and results.

Table 1. Structure of an organization-specific measure tool.

	Requirements	Business	Interest group collaboration	Results
GENERAL INDICATORS				
Ability to develop the organization's cyber security culture				
Ability to analyze its cyber environment				
Magnitude of cyber security 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

The widespread commissioning of the measure tool in CI organizations would make it possible to follow the cyber security development of the whole area in the same way as it serves the strategic level needs of a single organization.

4 Situational awareness challenges

The most significant challenges of an organization's CSA deal with to the observation of the vulnerabilities and operational deviation of the complex technical system wholeness (Kokkonen, 2016). Main challenges at the technical level consist of two aspects: CSA of enterprise ICT assets and CSA of industrial automation.

4.1 Enterprise ICT systems

The vulnerabilities of the ICT assets of the organization have to be identified continuously against the emerging threats. The organization considers real-time forming of the CSA of ICT systems and assets which is in accordance with the Information Technology Infrastructure Library (ITIL) service model. Fig. 4 represents an organization's framework for forming the CSA of its own ICT systems. ICT assets and the ticketing system as well as CERT messages and SOC log analysis that arrive via Security Information and Even Management (SIEM) (see Fig. 4) represent Level 1 elements of Endslay's model (see Fig. 2). The objective is to achieve from them a real-time expression which describes information security. The CSA which is formed of the observations is a precondition for the understanding of observations (Level 2). After this the preconditions to estimate effects which are in accordance with the observations form good using the CSA and utilizing the

knowledge of the structure of the ICT system of the interpreter of the CSA and technical know-how (Level 3). The final objective is naturally the making of the situation-specific right decisions and the control of the measures which maintain the capacity of the ICT systems and information reserves which are in accordance with the decisions.

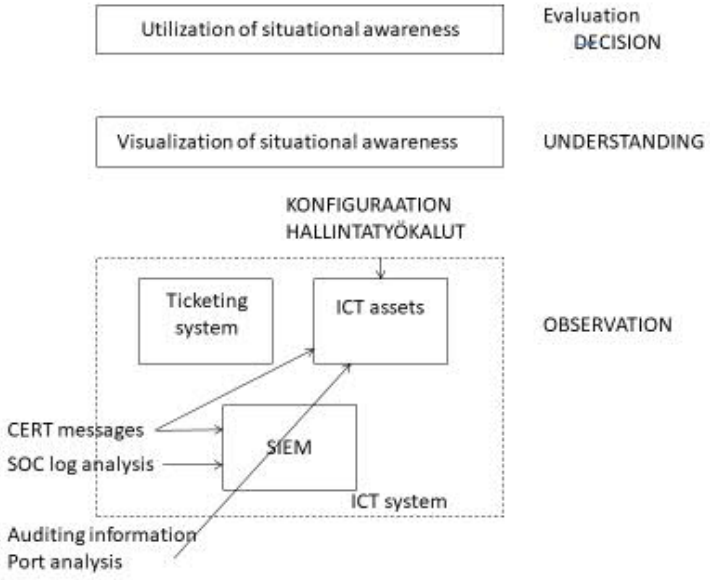

Fig. 4. Forming of the CSA of enterprise ICT systems.

ICT systems and assets can be controlled with the tools of the control of the configuration (Discovery tools). These tools help to analyze the properties of the firewalls and to clarify the services which function in the ICT systems. The real-time situation information of the user experience of information processing systems and of information reserves which is in accordance with the ITIL service model consists of the support requests of the service which are directed to them (Ticketing system). On the other hand, the SIEM system helps to form the situation consciousness of known threatening factors (CERT messages) and of logs of ICT systems (SOC log analysis) as a subject of the examination. So every one of the above mentioned arrangements produces the CSA for its part. The final objective is to accomplish the automatic connecting of this information which is directed to the structure of the ICT system which is in accordance with the ITIL services of the target organization.

4.2 Industrial automation

The Controller Area Network (CAN) is an automation bus that was originally designed for real-time data transfer of distributed control systems to cars. Later, the CAN bus was developed as a universal automation system for many automation solutions. CAN bus is widely used also in critical infrastructure and is used in this section as an example.

One of the characteristics of the CAN bus is that its traffic is not supervised in any way due to the lack of timing of control. In other words there are no authentication mechanism. The Cybersecurity and Infrastructure Security Agency (Cybersecurity and Infrastructure Security Agency, 2017) warned the users of the bus of the vulnerability, which enables a physical entrance to the automation system, and makes the DoS attack possible. The seriousness of the attack depends on how the CAN bus has been carried out in a destination system and how easily the potential attacker can use the input port (typically OBD-II). This differs from the earlier frame based attacks that were usually perceived by IDS or IPS. The utilizing of the vulnerability concentrates on the message bits which govern the bus and causes functional disorders in the CAN nodes in the sending of the right message frames (Cybersecurity and Infrastructure Security Agency, 2017).

The CAN communications protocol, ISO-11898:2003, describes how information is passed between devices on a network and conforms to the Open Systems Interconnection (OSI) model, which is defined in terms of layers. Actual communication between devices connected by the physical medium is defined by the physical layer of the model. The ISO 11898 architecture defines the lowest two layers of the seven-layer OSI/ISO model as the data-link layer and the physical layer, shown in Fig. 5.

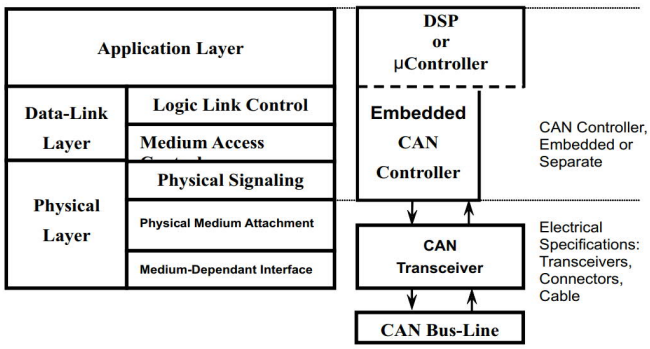

Fig. 5 CAN bus in the OSI/ISO model [adapted from Corrigan (2016)]

The application layer establishes the communication link to an upper-level application specific protocol such as the vendor-independent CANopen™ protocol. This protocol is supported by CAN in Automation (CiA), the international users and

manufacturers group. Many protocols are dedicated to particular applications, such as industrial automation, diesel engines, or aviation (Corrigan, 2016).

CAN message and frames

The four different message types, or frames (see Fig. 6), that can be transmitted on a CAN bus are the data frame, the remote frame, the error frame, and the overload frame.

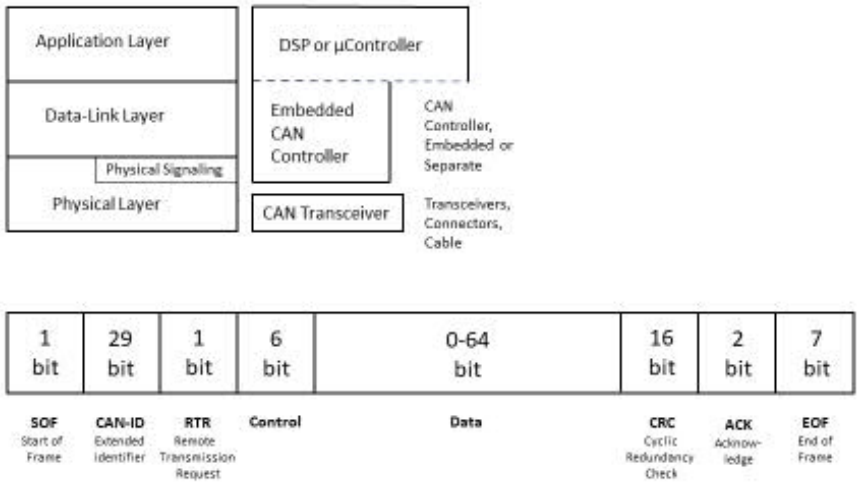

Fig. 6. CAN bus message

The data frame is the most common message type, and comprises the arbitration field, the data field, the CRC field, and the acknowledgment field. In Fig. 6 the arbitration field contains a 29-bit identifier and the RTR bit, which is dominant for data frames. Next is the data field, which contains zero to eight bytes of data, and the CRC field, which contains the 16-bit checksum used for error detection. The acknowledgment field is last.

The intended purpose of *the remote frame* is to solicit the transmission of data from another node. The remote frame is similar to the data frame, with two important differences. First, this type of message is explicitly marked as a remote frame by a RTR bit in the arbitration field, and second, there is no data.

The error frame is a special message that violates the formatting rules of a CAN message. It is transmitted when a node detects an error in a message and causes all other nodes in the network to send an error frame as well. The original transmitter then automatically retransmits the message. An error mechanism in the CAN controller ensures that a node cannot tie up a bus by repeatedly transmitting error frames.

The overload frame is mentioned for completeness. It is similar to the error frame with regard to the format, and it is transmitted by a node that becomes too busy. It is primarily used to provide for an extra delay between messages.

Arbitration is a mechanism for conflict resolution between network nodes. When the network path is free, any of the nodes in the network can start the message send process. If another node also wishes to send at the same time, the order of the transmissions is decided using a bitwise arbitration mechanism. During arbitration, both nodes start their transmission. The transmission starts with a start bit, followed by an id field (identifier, CAN-ID). The sending order decision is made based on the value of the id field and the other node or nodes discontinue their transmissions. The messages are sent ordered by priority, where the zero value is dominant. In practice this means that if a node currently sending a bit with a value of one sees that another node is sending a zero bit, it backs off. In other words, it discontinues its own transmission, forfeiting its turn to the node sending the dominating bit. In practice the message with the smallest decimal id value has the highest priority (Johansson, et al., 2005).

CAN bus pros and cons

According to Voss and Comprehensible (2005), CAN bus was designed for maximal speed and reliability. At the technical level this mean, among other aspects, that the network communication uses a provider–consumer model instead of the common sender–receiver model. The second feature aiming for performance gains was the lossless bus arbitration described above. Improving the reliability of the data transmitted between the nodes was achieved with a mechanism that insures the integrity and timeliness of the messages. These mechanisms are based on bus arbitration, using checksums checking the payload and resending failed messages. (Voss & Comprehensible, 2005)

Based on these design decisions, CAN bus is effectively a broadcast network, where any node can send a message and all nodes are listening to the network and reacting to the messages they are interested in. The only thing the recipients check is the protocol correctness of the received message. (Voss & Comprehensible, 2005)

CAN bus speed is 1 Mbit/sec, which these days does not seem fast. Yet for transmitting short messages and having an effective collision avoidance mechanism, CAN bus is more suitable to be used in real-time applications than connected protocols such as TCP/IP, even if those would be using greater transmission speeds. (Voss & Comprehensible, 2005)

With further development the CAN bus has became a dominant technology for the data transmission of vehicle basic functions. During the last two decades the number of electronic systems in vehicles has increased and at the same time they have become more complex. CAN bus vulnerabilities can be traced back to design decisions described above, the most significant of these being the lack of authentication mechanism. The receiving entity does not have any mechanism to verify the

origins of the received message or the validity of the data received. In other words, the control unit does not have a mechanism to detect message forgery. This characteristic makes vehicle CAN busses vulnerable to attacks, such as message forgery, unauthorized data use and denial of service. The DoS vulnerability can be exploited by sending a large number of high priority messages. These attacks can affect the vehicles systems in such a way as to cause loss of control, incorrect functionality, premature wear or rendering the vehicle unable to function at all. (Carsten, et al., 2015)

Attack surfaces

The taxonomy of CAN bus attack surfaces is usually divided into two parts: remote exploits and exploits requiring physical access to the CAN bus. In addition to this, some researchers have expanded the use of physical connections by constructing experiments that enable man-in-the-middle type of attacks on the CAN bus (Lebrun & Demay, 2016).

Physical connection to a CAN bus is not technically complex to achieve. The simplest physical connection can be implemented through the vehicle's diagnostics port. This approach does not require any alterations to the vehicle in question. The limitation of this approach is the amount of network data observable at this point of entry, depending heavily on the make and model of the vehicle. CAN bus traffic seen through the diagnostic port is restricted by segmenting the network. These limitations can be avoided by choosing another point of entry from the desired segment. In most cases this approach requires alterations to the vehicle's wiring harnesses, because segment-specific connectors are rarely implemented in production vehicles.

Remotely exploitable attack surfaces that would have a direct effect on the vehicle's physical functionalities are usually more challenging to exploit. In practice, this normally means a multistage attack where the attacker first has to find a vulnerable and remotely accessible service to gain a foothold. As an example, this kind of service can be found from the vehicle telemetry or infotainment systems. After gaining a foothold on one of the connected systems, the attacker needs to find a way to gain access to another system that has connectivity to the more critical segments of the vehicle's CAN bus. This type of attack has been successfully conducted by some vehicle security researchers.

Cyber security of CAN bus (vehicle) study has been conducted at the University of Jyväskylä (AaTi study).The focus of the AaTi study was to survey anomaly detection methods applicable to CAN-networks. This research complements previous research and patents by understanding network-traffic characteristics using recordings obtained from a test vehicle. The study shows that attacks against vehicle networks can be categorized into three groups. The network can be injected (a) with special messages such as diagnostics messages; (b) with normal messages that disturb vehicle functionality or (c) by sending normal messages after the real sender

has been rendered unfunctional. The most common situation is probably when the real sender is still functional, and the attacker sends normal CAN messages. These kinds of attacks can be detected by observing message send intervals, since in a normal situation the intervals should remain regular.

In the first phase of research a neural network implementation was tested for its ability to detect abnormalities in message data payloads. The aim of this implementation was to provide technical means to learn different payload possibilities and predict the data incoming in the following messages. This would have created the possibility to detect abnormal data payloads. The problem with using neural networks arose from its resource intensiveness and lack of prediction accuracy. The next experiments focused on anomality detection methods based on message timing.

The first time-based method we tested was One-Class Support Vector Machine (OCSVM), which is a variation of the popular machine learning method. This method defines boundaries around normal behavior and classifies all other traffic as abnormal. In the implementation, a moving window with a set number of messages was used as a data-entity. The characteristics of the messages are then calculated using OCSVM and, based on the results, the whole window is declared normal or abnormal. The characteristics used in this implementation were average interval and standard deviation.

After this fist experiment, other methods based on message interval were surveyed. Kernel density estimation models interval deviation for each message identifier. This value can then be compared to incoming messages in order to detect abnormalities. Modeled deviation provides a density function for the interval that can be used for likelihood value calculation for incoming messages. A drop in the calculated likelihood that exceeds a predetermined threshold can be detected as an anomaly and an alarm can be triggered. Because kernel density estimation is also a resource-intensive method and the observed test data did not show multipeak properties, a simplified version using the same principles of this method was implemented. This method aims to model message identifier deviation using key values. This implementation of absolute deviation achieves substantial gains in resource efficiency and without decline in the performance of the detection properties. The modeling was done using standard deviation in order to use the two key values: average and standard deviation. In the practical implementation training phase average, lower and upper bound values were calculated for each message identifier for classification purposes. A moving window was used as a data entity. If the values within the window went below the lower bound or exceed the upper bound, the whole window is declared an anomaly in the network traffic.

All of the above mentioned methods have their own challenges in either resource intensiveness, accompanied in some cases with inaccuracy of predictions. Based on the experience described in the method comparison chapter, a novel method for detecting CAN bus anomalies based on message arrival intervals was developed and a patent application for this method has been filed.

As different digital platforms become ever more common in automated processes, the protection of different processes and the cyber security of the infrastructure is going to play a significant role in the overall safety of these platforms. For future researchers in this field, the group would like to recommend the usage of outcomes found in the AaTi study as well as the utilization of the patented method as a part of future CAN bus implementations in order to improve cyber security and situation awareness of automation networks.

5 Conclusions

For the first research question (how the cyber situational awareness of a CI organization can be developed) it is stated that as the target state of the organization's cyber SA 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) Cyber security management in all circumstances; b) Strategic choices for operational continuity management
- Critical success factors: a) Good SA 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

In May 2017, the WannaCry ransomware campaign was affecting various organizations with reports of tens of thousands of infections in over 150 countries. On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. These examples show necessity of the technical/tactical level CSA. However, as this article expresses, there are significant challenges with regard to the technical/tactical level CSA. The WannaCry ransomware utilized a Windows vulnerability and because CSA was insufficient in many organizations, it prevented quick countermeasure. Also in the Ukreine case, the attack was not perceived from the technical system because of inadequate cyber situational awareness.

References

Carsten, P., Yampolskiy, M., Andel, T. & McDonald, J., 2015. In-Vehicle Networks: Attacks, Vulnerabilities, and Proposed Solutions. *CISR '15 Proceedings of the 10th Annual Cyber and Information Security Research Conference* , p. 477–482.

Corrigan, S., 2016. *Introduction to the Controller Area Network (CAN).* , s.l.: Texas Instruments.

Cybersecurity and Infrastructure Security Agency, 2017. *ICS Alert (ICS-ALERT-17-209-01), CAN Bus Standard Vulnerability,* s.l.: s.n.

EECSP Expert Group, 2017. *Cyber Security in the Energy Sector,* Europe: Energy Expert Cyber Security Platform (EECSP).

e-Governance Academy, 2017. *National Cyber Security Index (NCSI).* [Online] Available at: https://ncsi.ega.ee/
[Accessed 8 6 2019].

Endsley, M. R., 1995. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors and Ergonomics Society,* 37(1), pp. 32-64.

European Commission, 2016. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016.* [Online]
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
[Accessed 8 6 2019].

Faber, S., 2015. *Flow Analysis for Cyber Situational Awareness.* [Online]
Available at: https://insights.sei.cmu.edu/sei_blog/2015/12/flow-analytics-for-cyber-situational-awareness.html
[Accessed 8 6 2019].

Horsmanheimo, S. et al., 2017. *Kriittisen infrastruktuurin tilannetietoisuus (Situational awareness of critical infrastructure),* Helsinki: Prime Minister's Office.

Janhunen, K., 2015. *Valtionhallinnon häiriötilanteiden hallinta - miten VIRT-toimintaa kehitetään?.* Finland: The Ministry of Finance.

Johansson, K. H., Törngren, M. & Nielsen, L., 2005.), Vehicle applications of controller area network. In: D. H. B. William S. Levine, ed. *Handbook of Networked and Embedded Control Systems.* s.l.:s.n.

Joint Task Force Transformation Initiative, 2011. *NIST Special Publication 800-39: Managing Information Security Risk - Organization, Mission, and Information System View,* Gaithersburg: National Institute of Standards and Technology.

Kokkonen, T., 2016. *Anomaly-Based Online Intrusion Detection System as a Senor for Cyber Security Situational Awareness System.,* s.l.: Jyväskylä studies in computing 251. University of Jyväskylä.

Lebrun, A. & Demay, J. C., 2016. *Canspy: a platform for auditing can,* s.l.: s.n.

Lehto, M. et al., 2017. *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.

Lehto, M. et al., 2018. *Kyberturvallisuuden strateginen johtaminen Suomessa (Strategic management of cyber security in Finland),* Helsinki: Prime Minister's Office.

Ministry of Defence, 2010. *Yhteiskunnan turvallisuusstrategia (The Security Strategy for Society).* Helsinki: Ministry of Defence.

National Audit Office of Finland, 2017. *Kybersuojauksen järjestäminen,* Helsinki: National Audit Office of Finland.

National Emergency Supply Agency, 2019. *Organisation.* [Online]
Available at: https://www.nesa.fi/organisation/
[Accessed 8 6 2019].

Pöyhönen, J. & Lehto, M., 2017. *Cyber security creation as part of the management of an energy company.* Dublin, 16th European Conference on Cyber Warfare and Security, pp. 332-340.

Ruoslahti, H., Rajamäki, J. & Koski, E., 2018. Educational Competences with regard to Resilience of Critical Infrastructure. *Journal of Information Warfare,* 17(3), pp. 1-16.

The Security Committee, 2017. *Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020 (Implementation Programme for Finland's Cyber Security Strategy for 2017-2020).* Helsinki: The Security Committee.

The Security Committee, 2017. *Yhteiskunnan turvallisuusstrategia (The Security Strategy for Society).* Helsinki: The Security Committee.

Traficom, 2019. *About us.* [Online]
Available at: https://www.traficom.fi/en/traficom/about-us
[Accessed 8 6 2019].

Virrantaus, K. & Seppänen, H., 2013. *YHTEISKUNNAN KRIITTISEN INFRAN DYNAAMINEN HAAVOITTUVUUSMALLI,* Helsinki: MATINE.

Voss, W. & Comprehensible, A., 2005. *Guide to Controller Area Network. Massachusetts.* Massachusetts: Copperhill Media Corporation.