PRELIMINARY COMMUNICATION

Annals of Disaster Risk Sciences

Vol 3, No 1 (2020): Special issue on cyber-security of critical infrastructure

Cyber Situational Awareness in Critical Infrastructure Protection

Jouni Pöyhönen, University of Jyväskylä
Jyri Rajamäki, Laurea University of Applied Sciences
Harri Ruoslahti, Laurea University of Applied Sciences
Martti Lehto, University of Jyväskylä

Address for correspondence: Harri Ruoslahti, Laurea University of Applied Sciences, Finland, harri.ruoslahti@laurea.fi

Abstract

The European Union promotes collaboration between authorities and the private sector, and the providers of the most critical services to society face security related obligations. In this paper, critical infrastructure is seen as a system of systems that can be subject to cyber-attacks and other disturbances. Situational awareness (SA) enhances preparations for and decision-making during assessed and unforeseen disruptive incidents, and promoting Cyber effective situational awareness (CSA) requires information sharing between the different interest groups. This research is constructive in nature, where innovative constructions developed as solutions for domain-specific real world problems, while the research question is: "How can cyber situational awareness protect critical infrastructures?" The Observe – Orient – Decide – Act (OODA) loop is examined as a way to promote collaboration towards a shared situational picture, awareness and understanding to meet challenges of forming CSA in relation to risk assessment (RA) and improving resilience. Three levels of organizational decision-making are examined in relation a five-layer cyber structure of an organization to provide a more comprehensive systems view of organizational cyber security. Successful, crisis-management efforts enable organizations to sustain and resume operations, minimize losses, and adapt to manage future incidents, as many critical infrastructures typically lack resilience and may easily lose essential functionality when hit by an adverse event. Situation awareness is the main prerequisite towards cyber security. Without situation awareness, it is impossible to systematically prevent, identify, and protect the system from cyber incidents.

Keywords

Critical infrastructure, Cyber situational awareness, Five-layer cyber structure, OODA Loop, Risk assessment

1. Introduction

One strategic area in Finland´s Cyber Security Strategy 2019 is promoting collaboration between authorities and companies to support the continuity of infrastructure and services that are critical to society (Tke Security Committee, 2019).

The European Union (EU) Network and Information Security (NIS) Directive (European Commission, 2016) increases the demand for collaboration between authorities and the private sector (Public Private Partnership, PPP) in the important field of cyber security. 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 are put under security related obligations, and the application of the directive imposes security and information requirements on the aforementioned operators of critical infrastructure. The goal is to improve situational awareness and information sharing. Critical infrastructure consists especially of crucial service providers defined in the NIS Directive.

The supply chains of critical infrastructure organizations are complex systems of systems characterized by a conglomeration of interconnected networks and interdependencies. The general networks and work processes involved in the operation of an organization can be illustrated as a logistical framework comprising of interconnected parts: a supplier

network, production process, client network, and information and material flows. According to the European Commission (EC) the Information and communication technology (ICT) sector is vital to all segments of society. ICT systems are part of the infrastructure of critical organizations and thus constitute a significant part of the operations that support the core processes of the organization. Corporate-level ICT systems are related to the administration and management of information and the material flows in the network, and on the production level are industrial automation systems (industrial control systems, ICS) (Edwards, et al., 2016) (EU Commission, 2009).

Weed (2019) applies a systems view to describe the structure of critical infrastructure as a complex whole comprised of several separate organizations (or systems). Critical infrastructure can thus, be seen as a system of systems, and such structures are subject to disturbances, e.g. cyber-attacks. Reacting to cyber disruptions is ultimately based on how society and its organizations can adapt to complexity and to the insecurity that it brings; Weed (2019) stresses the importance of understanding the technologies, risks and actors, and the growing cyber security needs of the complex environment of critical infrastructure.

Developing better situational awareness (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 cyber networks. The target state can be achieved with an efficient process that includes a three-level—strategic, operational and technical/tactical—operating model to support decision-making and utilizing national and international strengths. Strategic agility and speed are needed to prepare for incidents in dynamic cyber environments (Pöyhönen, et al., 2019).

The research question of this study is: “How can cyber situational awareness protect critical infrastructures?”

2. Methods and Structure of the Paper

This is a constructive research. When using the constructive research approach, innovative constructions or artefacts (e.g. processes, practices or tools) are created as solutions for domain-specific real world problems (Crnkovic, 2010). In constructive research, both theoretical and practical components should be considered and the problem as well as the solution should be tied with the theoretical comprehension. Four elements: practical relevance, practical functioning, theory connection and theoretical contribution should be included in problem solving constructs of constructive research (Lehtiranta, et al., 2015).

The following sections look at the cyber structures and decision-making levels of critical infrastructure organizations, and a systems approach is applied to organizational cyber security. The Observe – Orient – Decide – Act (OODA) loop is examined as a possible tool to promote shared situational picture and awareness. Challenges of forming cyber situational awareness are also examined in relation to risk assessment and improving resilience. The final section are discussion and conclusions.

3. The Cyber Structure of Organizations

Libicki (2007) structures the cyber world based on the idea of the Open Systems Interconnection Reference Model (OSI). The OSI model groups communication protocols into four layers. Each layer serves the layer above it and is served by the layer below it. The Libicki cyber world model has the following four layers: physical, syntactic, semantic and pragmatic.

Cyber security professor from the University of Jyväskylä, Martti Lehto (Lehto & Neittaanmäki, 2018) has updated the Libicki four layers cyber world model by adding a fifth layer in order to consider the networking needs of an organization. The five-layer cyber structure of an organization is described in figure 1.

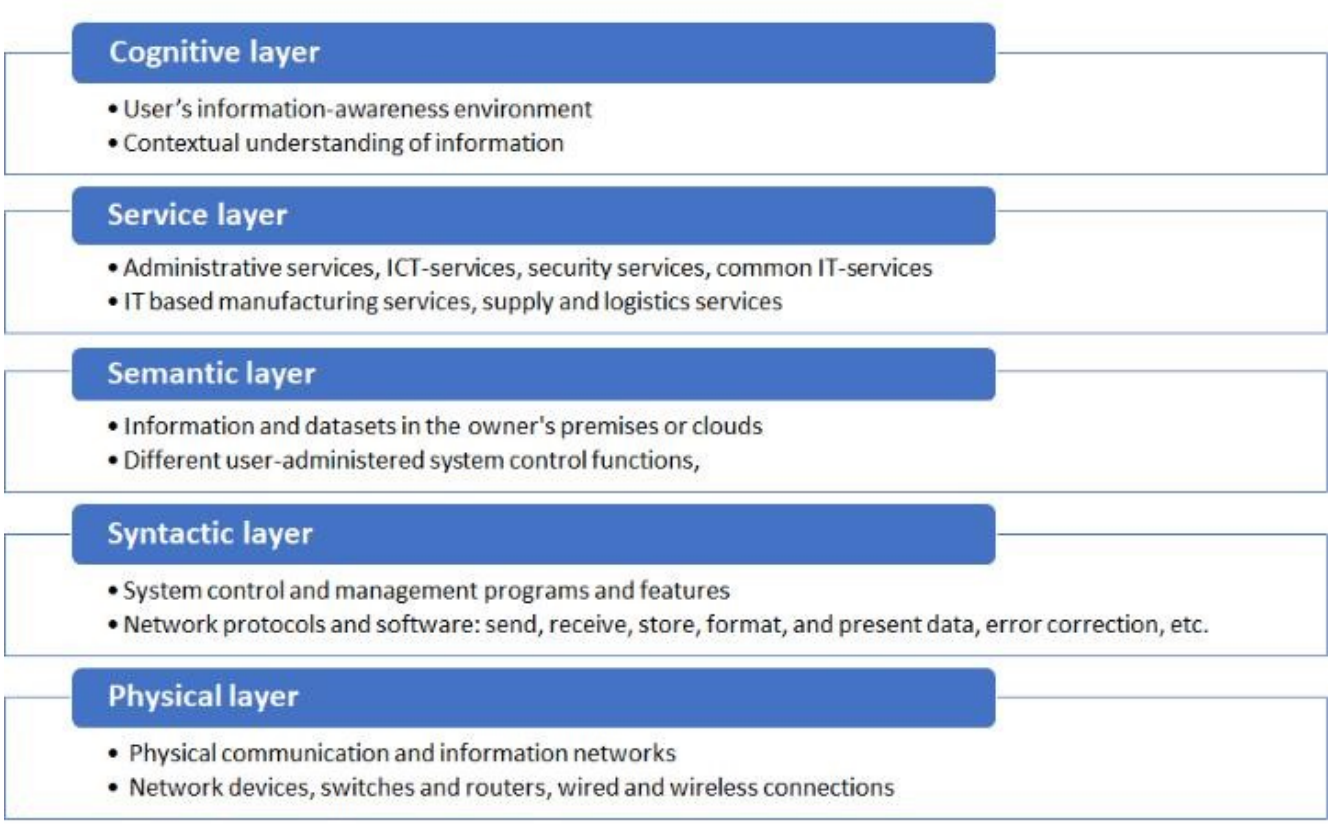

Figure 1. The five-layer cyber structure of an organization (modified from Lehto & Neittaanmäki, 2018)

As seen in figure 1, in the case of the five-layer model structure, the physical layer contains the physical elements of the communications network, such as network devices, switches and routers as well as wired and wireless connections. The syntactic layer is formed of various system control and management programs and features, which facilitate interaction between the devices connected to the network, such as network protocols, error correction, handshaking, etc. The semantic layer contains the information and datasets in the user's computer terminals as well as different user-administered functions, such as printer control. The service layer is the heart of the entire network. It contains such as administrative services, ICT-services, security services, IT based manufacturing services, supply and logistics services. The cognitive layer portrays the user's information-awareness environment: a world in which information is being interpreted and where one's contextual understanding of information is created.

Protecting the ICT-systems against threats implies measures taken based on risk assessment (RA), and they ensure the availability of primarily digital information in the operating processes being examined. The measures are highly significant for the overall availability of the systems that support the business processes of the organization. Availability plays a key role in achieving business results and promoting the reliability of activities. Further central goals include the reliability and content integrity of information within the processes and used by the processes. Overall trust should be built from these starting points, based on the target organization's realistic idea of its own capabilities to reliably manage the challenges involved in operations within the cyber world. The following section addresses the significance of trust in the cyber environment for the operations of an organization. Moreover, trust-enhancing measures applicable to an organization are mapped.

3.1 Decision-making Levels and System View

We have integrated the three decision-making levels of an organization to the five-layer cyber structure in order to have a more comprehensive system view of the cyber security environment of the organization. This applies a systems approach to organizational cyber security subsect and subject, the principle of which is described in figure 2.

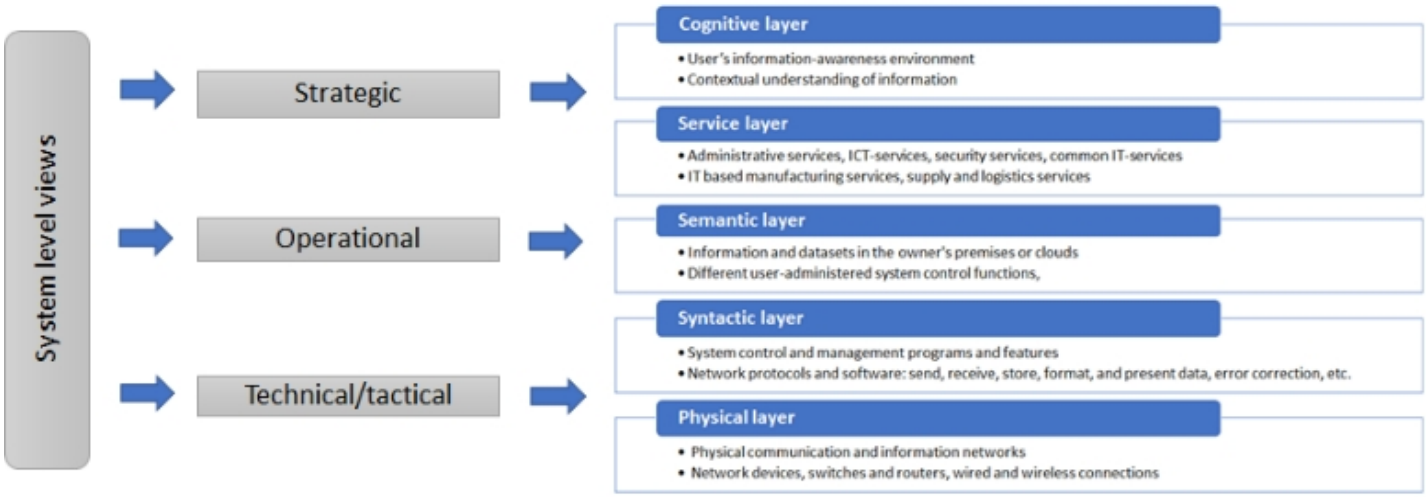

Figure 2. System level view to organizational cyber security (modified from Lehto & Neittaanmäki, 2018)

4. The OODA Loop for better Cyber Situational Awareness

Tikanmäki and Ruoslahti (2019) conclude that to build shared situational awareness organizations need information from the environment to notice the events surrounding them, and to understand their impact on their activities. The Observe – Orient – Decide – Act (OODA) loop, used e.g. in project ECHO (ECHO, 2019), is a framework that can provide structure to the collaboration aiming to better Cyber Situational Awareness (CSA).

The OODA loop assumes continuous improvement; repeating the process allows for learning from previous experiences. Lessons learned that are fed to the loop activate better performance, and ideally this occurs every time the four steps are completed. Zager and Zager (2017) find that the faster the completion of the cycle of the OODA loop enhances decision-making, which may suggest models for faster decision-making processes and improvements in the information syntheses quality.

According to Pahi, Leitner and Skopik (2017) the OODA loop focuses on the human aspects of crisis situations. The OODA loop model is often used for decision making and cyber defense actions. The basic form of the OODA loop stands for a cycle including four phases: observation, orientation, decision, and action. Originally, it has been implemented for decision making in air operations. The OODA-model in cyber defense works in phases: during the observation phase, sensor information concerning the infrastructure and assets are gathered; during the orientation phase, that information are analyzed to find out what is happening; during the decision phase, the countermeasures, incident response, mitigation and recovery activities are chosen; and during the action phase, these chosen activities are employed; and a new loop cycle begins with a new observation phase (Kokkonen, 2016).

As seen below in figure 3, the OODA loop decision cycle depends completely upon tactical, operational, and strategic agility. “Without OODA loops we can neither sense, hence observe, thereby collect a variety of information for the above processes nor decide as well as implement actions in accord with those processes. Without OODA loops embracing all the above and without the ability to get inside other OODA loops (or other environments), we will find it impossible to comprehend, shape, adapt to, and in turn be shaped by an unfolding, evolving reality that is uncertain, ever changing, unpredictable.” (Boyd, 1995)

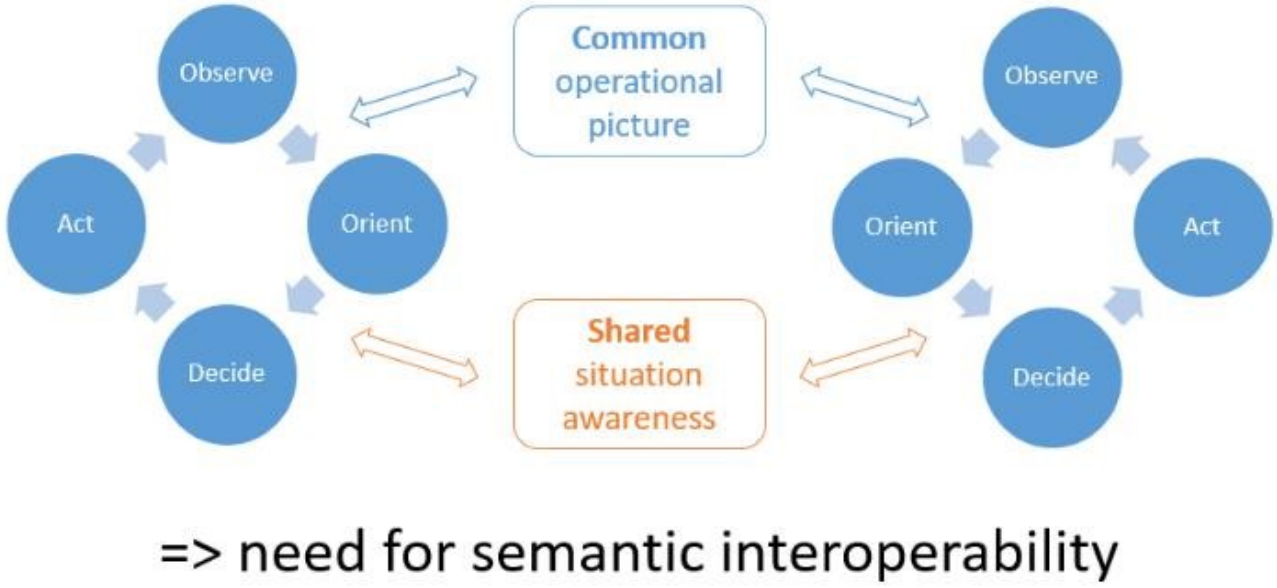

Figure 3: Decision making in complex environments (ECHO project, 2019)

According to Pahi, et al. (2017) one key success factor in establishing CSA is promoting cooperation between the public and private sector. The OODA loop, in figure 3 above, may be one way of creating structure to do this. SA for organizations is established on both a technical and organizational level, while on a national level information is collected and analyzed to support national decision-making note Pahi, et al. (2017). Exchanging and analyzing information between organizations may enable collecting information both on organizational and network levels to enhance continuity planning and resilience on both levels.

The State Security Networks Group Finland coordinates the KRIVAT service, an information-sharing and cooperation framework specifically designed for the management of disturbances. Resilience and preparedness is enhanced by supplementing existing preparedness and disturbance- management activities of critical infrastructure operators during major disturbances. KRIVAT responds to a recognized need for clearer communication structures and better situational awareness between critical infrastructure organizations (Ruoslahti, et al., 2018). Project ECHO – European network of Cybersecurity centres and competence Hub for innovation and Operations – aims to establish a coordinated network of cyber security specialists and service providers on a European level (ECHO project, 2019).

5. Challenges to have SA in the ICT Systems of an Organization

Successful, crisis-management efforts enable organizations to sustain and resume operations, minimize losses, and adapt to manage future incidents (Linkov, et al., 2013a). Effective response to disturbances and collaboration during those disturbances depend heavily on shared situational awareness. According to Linkov, et al. (2014) many critical infrastructures typically lack resilience and they may easily lose essential functionality when hit by adverse events. The city of Baltimore, for example, suffered a ransomware attack that disrupted its critical services for weeks. To handle critical functions city officials were forced to implement manual procedures, and Baltimore spent more than $18 million on recovery efforts (Fortinet, 2019).

Ruoslahti, et al. (2018) promote resilience event management cycles (plan or prepare, absorb, recover, adapt and learn, and self-modify) should be taken into account in relation to Cyber Physical Systems (CPS), which are composed of cyber, technical, social and ecological systems. Known best practices and earlier experiences of CPS and critical infrastructure sectors can be used to design and maintain resilience.

Industrial fields that critical to society are increasingly CPS in nature. Critical infrastructure use resilience and business continuity planning practices and standards to guide their planning and preparedness; risk assessment, business impact analysis, and business continuity planning are used commonly by critical infrastructure industries (Ruoslahti, et al., 2018).

Risks in collaboration in and among networks can only be reduced, not avoided. Organizational resilience provides tools and conditions to understand and reduce these risks and mitigate crises (Vos, 2017). To build resilience in networks, and also to guide connected stakeholder networks Gustafsson, et al. (2012) find that co-creation requires interaction among various actors and knowledge creation processes. According to Pirinen (2017) situational intelligence is needed to build

resilience, and that the key factors in network collaboration are the roles, engagement, responsibility, and the mutual interactions and impacts of the actors. Resilience requires cooperation by and between social networks and communication is co-constructed by the multiple stakeholders, even while they most likely have different interests and various interdependencies (Vos, 2017).

5.1 Cyber Risk Review

The definition of strategy derived from the organizations cyber security vision guides the actions taken in order to achieve the goals. In the first stage, it is most practical to facilitate the definition of strategy by performing risk analysis on cyber threats. If an organization is familiar with the factors affecting the operation of processes, their most vulnerable points in the cyber world and the cyber-attack methods that most probably threaten the processes, it possesses the most relevant information for creating protective plans for potential treats. Vulnerability analysis against attack methods is a systematic tool for identifying and assessing risks related to process operation as well as for choosing the most suitable measures to enhance cyber security. By adding three decision-making levels to the five-layer cyber structure, in order to have a comprehensive system view of organizational cyber security environments, the risk analysis can be practical. The NIST standards could be utilized to support the risk based cyber security assessment and comprehensive system view from organization cyber world. For example NIST 800-39 (2011) publication places information security into the broader organizational context of achieving mission/business success, and according to NIST 800-39 the aim is to:

- Ensure that senior leaders/executives recognize the importance of managing information security risk and establish appropriate governance structures for managing such risk;
- Ensure that the organization's risk management process is being effectively conducted across the three tiers of organization, mission/business processes, and information systems;
- Foster an organizational climate where information security risk is considered within the context of the design of mission/business processes, the definition of an overarching enterprise architecture, and system development life cycle processes; and
- Help individuals with responsibilities for information system implementation or operation better understand how information security risk associated with their systems translates into organization-wide risk that may ultimately affect the mission/business success.

Linkov et al. (2014) note that resilience can be enhanced by studying and improving the interconnectivity of the relevant critical infrastructure networks, and according to O'Rourke and Briggs (2007) also enhancing the surrounding social networks is an important component of societal resilience.

5.2 Cyber Resilience Review

Trust can be developed by utilizing preparedness planning. Linkov et al. (2013a) introduce a resilience matrix framework (later: "Linkov model") that can be used for this planning. It combines the four stages of a system 1) plan/prepare, 2) absorb, 3) recover and 4) adapt with the four domains of a system 1) physical, 2) information, 3) cognitive and 4) social. Later on Linkov et al. (2013b) apply their model further to cyber systems. Their purpose is to develop efficient metrics to measure the resilience of cyber systems.

In case of cyber systems, the cells of the resilience matrix can be interpreted as follows: How capable the system is to prepare/absorb/recover/adapt in case of a cyber disturbance executed within the physical/information/cognitive/social domain? Adding one metric to a certain domain often requires adding metrics to other domains too. Resilience metrics are used for recognizing and prioritizing the needs, for tracking progression and for sharing resources. Thus, they constitute an essential part of planning and decision-making (Linkov et al., 2013b).

The Linkov model and its different stages are especially suited for the operational and technical-tactical level preparedness planning, and that way for ensuring the continuity of operations. Considering the structure of the previously described system level view to organization cyber security, it is possible to find those targets from the operation of an organization that have a central position in preparedness planning. The company-specific content of operations has to be based on the present state analysis carried out before using the Linkov model, and on the situational awareness, in the form of target organization's strengths, weaknesses, possibilities, threats and their mutual relations. Based on the analysis, the related needs of each organization can be planted on the planning stages of Linkov's model. Table 1 describes an example of actions structured according to the Linkov model from a previous case study (Pöyhönen, et al., 2018).

Table 1: Research results (Pöyhönen, et al., 2018) structured to the Linkov model (Linkov et al., 2013a).

	Plan/Prepare	Absorb	Recover	Adapt
Physical	• Technical situational awareness • Segmentation • Alternative resources	• Recognition of disturbances, their scope and impacts • Protection of sensitive information • Deployment of alternative resources • Isolation of disturbance	• Maintenance of situational awareness • Ramp-up • Testing	• Updates
Information	• Classification and prioritization of critical systems • Business Impacts • Preparation of sensitive information protection • Communication plans	• Documentation • Informing of authorities and stakeholder	• Documentation • Informing of the press	• Aggregation of documents
Cognitive	• Perception of situational awareness • Scenarios and models • Situational management • Resourcing • Training and benchmarking • Feedback system	• Analysis of situational awareness • Additional resources • Prioritization • Censor information	• Allocation of expertise • Collection of data and log information	• Log analysis • Impact analysis • Situation analysis • Feedback analysis • System updates • Continuous improvement
Social	• Naming of stakeholders' contact persons • Training for exceptional situations	• Informing about operations	• Informing about operations	• Staff training • Informing about development operations • Update of stakeholder information

The contents of table three are based on a previous case study (Pöyhönen et al, 2018), where the findings indicate that:

- The following operations of the planning and absorb stages within the physical domain of Linkov's model were recognized: taking care of the functionality, supervision and control of the technology, planning of the system isolation and needed operational segments, and planning of the alternative networks and routes. In case of a disturbance situation, firstly, the situational awareness of the incidence, its nature, distribution and scope are clarified, as well as its impact. After that, the plans are put to use for their needed parts. In the recovery stage, the cleanliness and functionality of the systems is ensured for all of their parts. Then, the comprehensive ramp-up of the machines is guided through. The adaptation stage is determined by the experiences got from the incident, but at least the technical protection operations must be considered carefully.
- The documentation planning is emphasized in the operations of information domain, by paying attention to the situation-specific documentation itself, and the critical operations and related requirements has to be documented already in the planning stage. The aforementioned documentation both serves the operation in a disturbance situation and enables the information documentation during the disturbance situation and in a recovery stage, so that the utilization of situation-specific experiences and learning in the adaptation stage is made possible. The informing of essential stakeholders and different authorities must also be included in each stage.
- In our case study, the plan of cognitive domain grew the most of all domains. Thus, it can be seen very significant in both management, in building the situational awareness, in continuity management, in prioritizing the operations, and in managing and controlling different resources, including services. All these operations play a decisive role in a disturbance situation, in the recovery stage and in the adaptation stage when utilizing the knowledge gained from the previous stages.
- The planning stage of the social domain consists of more specific communication plans than in the information domain, including the named contact persons, and both internal and external interest groups. The wide scale situation-specific informing in the different stages results from the planning of the social domain. In addition, the planning of the social domain includes the whole staff training in managing all the different stages.

6. Conclusions

The overall target of cyber security is that all systems and infrastructures are resilient. Situation awareness is the one of the main prerequisites towards cyber security. Without situation awareness, it is impossible to systematically prevent, identify, and protect systems from cyber incidents and if, for example, a cyber-attack happens, to recover from the attack. Situation awareness involves being aware of what is happening around your system to understand how information, events, and how your own actions affect the goals and objectives, both now and in the near future. It also enables to select effective and efficient countermeasures, and thus, to protect the system from varying threats and attacks. Information exchange between organizations becomes essential in creating and up keeping CSA, while the protection of critical infrastructure calls for risk assessment, preparation and resilience on a single organization level.

Acknowledgement

This work was supported by project ECHO, which has received funding from Horizon 2020 research and innovation programme of the European Union under the grant agreement no. 830943. The European Commission funds cyber pilot projects like the European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO) to promote opportunities for researchers, solution providers and practitioners to study and co-create new knowledge for innovation from multiple perspectives.

References

Boyd, J. R. (1995). The Essence of Winning and Losing. s.l.:s.n.

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.

Crnkovic, G. D. (2010). Constructive research and info-computational knowledge generation. In: W. C. &. C. P. L. Magnani, ed. Model-Based Reasoning in Science and Technology: Abduction, Logic, and Computational Discovery.

Heidelberg: Springer Berlin, p. 359–380.

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

ECHO project (2019). s.l.: s.n.

Edwards, N. et al. (2016). Supply Chain Decision Analytics: Application and Case Study for Critical Infrastructure Security. Proceedings of The11th International Conference on Cyber Warfare and Security ICCWS 2016, pp. 99-106.

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

EU Commission (2009). Critical information infrastructure protection. COM (2009) 149 final, Brussels: Commission of the European Communities.

European Commission (2016). 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. [Online] Available at: https://eurlex.europa.eu/eli/dir/2016/1148/oj [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].

Fortinet (2019). Fortinet Q2 2019 Quarterly Threat Landscape Report, s.l.: Fortinet, Inc..

Gustafsson, A., Kristensson, P. & Witell, L. (2012). Customer co-creation in service innovation: a matter of communication?. Journal of Service Management, 23(3), pp. 311-327.

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.

Lehtiranta, L., Junnonen, J.-M., Kärnä, S. & Pekuri, L. (2015). The constructive research approach: Problem solving for complex projects. In: B. Pasian, ed. Designs, Methods and Practices for Research of Project Management. s.l.:Gower Publishing Limited..

Lehto, M. & Neittaanmäki, P. (2018). The modern strategies in the cyber warfare. Cyber Security: Cyber power and technology. Berlin: Springer.

Libicki, M. C. (2007). Conquest in Cyberspace – National Security and Information Warfare. New York: Cambridge University Press.

Linkov, I. et al. (2014). Changing the resilience paradigm. Nature Climate Change, Volume 4, pp. 407-409.

Linkov, I. et al. (2013a). Measurable Resilience for Actionable Policy. Environmental Science & Technology.

Linkov, I. et al. (2013b). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), pp. 471-476.

O'Rourke, T. D. & Briggs, T. R. (2007). Critical Infrastructure', Interdependencies, and Resilience. The Bridge, Volume 37.

Pahi, T., Leitner, M. & Skopik, F. (2017). Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers. ICISSP, pp. 334-345.

Pirinen, R. (2017). Towards Common Information Systems Maturity Validation - Resilience Readiness Levels (ResRL). Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, Volume 3, pp. 259-266.

Pöyhönen, J., Nuojua, V., Lehto, M. & Rajamäki, J. (2018). Application of Cyber Resilience Review to an Electricity Company. The proceedings of the 17th European Conference on Cyber Warfare and Security ECCWS2018, pp. 380-389.

Pöyhönen, J., Nuojua, V., Rajamäki, J. & Lehto, M. (2019). Cyber situational awareness and information sharing in critical infrastructure organizations. Information & Security: An International Journal, Volume 43, pp. 236-255.

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.

Tikanmäki, I. & Ruoslahti, H. (2019). How Are Situation Picture, Situation Awareness, and Situation Understanding Discussed in Recent Scholarly Literature?. In: A. S. a. J. F. Jorge Bernardino, ed. Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management. Portugal: SCITEPRESS – Science and Technology Publications, Lda., pp. 419-426.

Tke Security Committee (2019). Finland´s Cyber Security Strategy 2019. [Online] Available at: https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/ [Accessed 15 02 2019].

Weed, S. A. (2019). US Policy Response to Cyber Attack on SCADA Systems Supporting Critical National Infrastructure, s.l.: Air Force Research Institute.

Vos, M. (2017). Communication in Turbulent Times: Exploring Issue Arenas and Crisis Communication to Enhance Organisational Resilience, Jyväskylä: Jyväskylä University School of Business and Economics.

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

Zager, R. & Zager, J. (2017). OODA loops in cyberspace: A new cyber-defense model. Small Wars Journal, 20(11).