The final version was published in: Pahi T., Leitner M. and Skopik F. (2017). Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers.In Proceedings of the 3rd International Conference on Information Systems Security and Privacy - Volume 1: ICISSP, ISBN 978-989-758-209-7, pages 334-345. DOI: 10.5220/0006149703340345

Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers

Timea Pahi, Maria Leitner, Florian Skopik
AIT Austrian Institute of Technology, Vienna, Austria
firstname.lastname@ait.ac.at

Keywords: situational awareness, national cyber security center, information sharing, survey, cyber security.

Abstract: National cyber security centers (NCSCs) are gaining more and more importance to ensure the security and proper operations of critical infrastructures (CIs). As a prerequisite, NCSCs need to collect, analyze, process, assess and share security-relevant information from infrastructure operators. A vital capability of mentioned NCSCs is to establish Cyber Situational Awareness (CSA) as a precondition for understanding the security situation of critical infrastructures. This is important for proper risk assessment and subsequent reduction of potential attack surfaces at national level. In this paper, we therefore survey theoretical models relevant for Situational Awareness (SA) and present a collaborative CSA model for NCSCs in order to enhance the protection of CIs at national level. Additionally, we provide an application scenario to illustrate a hands-on case of utilizing a CSA model in a NCSC, especially focusing on information sharing. We foresee this illustrative scenario to aid decision makers and practitioners who are involved in establishing NCSCs and cyber security processes on national level to better understand the specific implications regarding the application of the CSA model for NCSCs.

1 Introduction

More and more private organizations own critical infrastructures and run essential services in our modern states, such as electricity and water supply, transportation, banking and health care – just to name a few. However it's in the responsibility of the national governments to maintain public order and safety of citizens and therefore, to guarantee the security of these infrastructures.

Thus, a formal arrangement to foster the collaboration of the public and private sector has to be established. The vision is that national cyber security centers (NCSCs) collect and assess cyber security-relevant information from single organizations (i.e., critical infrastructure operators). Due to the expected large amount of information available, they must be able to derive important knowledge about emerging threats, ongoing incidents and their potential impact on national security earlier than any single organization could ever do. At national level, the isolated views of single organizations can be merged and the dots connected. Only this way, large-scale attacks, long-running campaigns, and especially threats against vertical markets and distributed supply chains can be identified and eventually mitigated.

Recently, this vision has made a huge leap forward. With the political agreement on the European directive on security of network and information systems (NIS Directive) (European Parliament, 2015) in July 2016, the European Union has put legal and regulatory frameworks in place that require operators of essential services and digital service providers to report high-impact cyber security incidents to authorities, e.g., to a NCSC. It is further foreseen that mentioned authorities take and process information about security incidents to increase the network security level of all organizations by issuing early warnings, assisting with mitigation actions, or distributing recommendations and best practices.

However, while most of the essential technical building blocks already exist today, there is a major lack of understanding on how to eventually adopt and present collected information to strategic levels in order to create situational awareness (SA) – and provide a sound basis for justified and effective decision making by competent authorities.

Thus, the contributions of this paper are as follows:

- **Survey of Models for SA:** We collect and analyze the applicability of data processing models required to create a complete process for gaining

and apply the gained cyber situation awareness (CSA).

- **Definition of CSA model for NCSCs:** We define an own CSA model and suggest extensions of surveyed models to make them fit for CSA, which requires extended capabilities compared to classic SA.
- **Information Sharing Scenario:** We demonstrate an application scenario of our CSA model focusing on information sharing in NCSCs.

The remainder of this paper is organized as follows. Sect. 2 outlines the methodology of the survey. Sect. 3 presents the results of the survey describing the applicability of the most prominent models for CSA. Sect. 4 elaborates on the implementation of CSA in NCSCs. An application scenario for CSA and its implications is summarized in Sect. 4.2. Finally Sect. 5 concludes the paper.

2 Methodology

In this paper, we use two methods to investigate the current state of the art in SA: (1) literature review and (2) classification. Based on these two steps, we identified shortcomings and propose a CSA model for NCSCs and validate it with a hands-on application scenario.

In the *Literature Review*, we used *Snowball sampling* in order to identify relevant and contemporary literature and find a golden standard within the topic of SA. Snowball sampling is focusing on sampling techniques that are based on the judgment of the researcher (Biernacki and Waldorf, 1981). The technique is used to define feasible issues in complex research areas, where subjects are hard to identify. This non-probability approach enables researchers to locate most of the relevant literature through checking references in the bibliography as a primary source for further research. After identifying relevant sources and focal points, the next phase contains further iteration of the literature research in order to gain a holistic picture about the particular research area.

Furthermore, a *Classification* was used to analyze and assess the definitions and models for SA. The widely-known and applicable general definition and theoretical model for SA by Endsley (see Sect. 3.1) was used as a basis for the collection and analysis of the applicability of the selected models. The cognitive SA model of Endsley can be divided in six components or levels, in *Perception, Comprehension, Projection, Decision, Performance of Actions and Feedback*. These levels are required for SA gaining and application in the national cyber security centers. These levels give the framework and serve as a basis for the analysis of the different models in Section 3.7. The model of Endsley demonstrates how SA provides a primary basis for decision making in dynamic systems. Although alone this model can not guarantee the success of the decision making (Artman, 2000), the created CSA model needs to integrate other existing models for providing the suitable input processes upon which decision are based in the NCSCs.

The selected models, based on their high citation rate, cover at least partially one or more components needed for gaining or applying SA. Most of the models use different names for the same levels instead of the original model. The contextually appropriate theoretical models are the following: Situation Awareness Model by Endsley (Endsley, 1995), the OODA Loop (Boyd, 1996), the JDL Data Fusion Model (White, 1987), the Cyber Situational Awareness Model (Okolica et al., 2009), the Situation Awareness Reference Model (Tadda and Salerno, 2010) and the Effective Cyber Situational Awareness Model (Evancich et al., 2014).

3 Survey of SA Models

Cyber security has become one of the important issues for our highly networked society. Within the field of cyber defense, situational awareness is particularly prominent. It is related to science, technology and practice to understand events and entities in the cyber space. There are several definitions for situation awareness. The first definition was in the mid-1980s recorded, but the use of the term situational awareness can be traced back to World War I. (Onwubiko, 2012) Until 1995 nearly all the existing SA definition have military approach, because of the growing interest in understanding how pilots maintain awareness during the flight. The widely applicable general definition for SA is proposed by Endsley (Endsley, 1995). Table 1 outlines the selected models for the survey. In the following, we will briefly describe each model.

3.1 Situation Awareness Model by Endsley (1995)

SA is specified in (Endsley, 1988) as: *"Situation awareness is the perception of the element in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future"*. SA presents a level of focus that goes beyond traditional information-processing approaches in attempting to explain hu-

Table 1: Overview of SA models

Abbrv.	Model	Focus	References
SAM	Situation Awareness Model	Cognitive decision making	(Endsley, 1995)
OODA	OODA Loop	Cognitive decision making	(Boyd, 1996)
JDL DFM	JDL Data Fusion Model	Processing and fusion of data and SA	(Steinberg et al., 1998)
CSAM	Cyber Situational Awareness Model	Business continuity planning and CSA	(Okolica et al., 2009)
SARM	Situation Awareness Reference Model	Situational awareness	(Tadda and Salerno, 2010)
ECSA	Effective Cyber Situational Awareness	CSA in computer networks	(Evancich et al., 2014)

man behavior in operating complex systems, e.g. pilots. Based on the definition of SA provided by Endsley, the SA forming consists of three levels (see (Endsley, 1995)):

- *Level 1 - Perception of the Elements in the Environment* is the first step in achieving SA. This level covers the perception of status, attributes, and dynamics of relevant elements in the environment.
- *Level 2 - Comprehension of the Current Situation* is based on outputs of the Level 1. Level 2 includes the understanding of the significance of the relevant elements.
- *Level 3 - Projection of Future Status* covers the ability to predict the future actions of the elements in the environment. This is achieved through knowledge of the status and dynamics of the elements and comprehension of the situation.

Endsley's model of SA (SAM) illustrates also the component Decision, Performance of Action, Feedback and the variables that can influence the development and maintenance, such as environmental and individual factors.

- *Decisions* are strongly influenced by SA, because it forms the major input to decision making. The decision can be affected by various factors, such as individual factors (e.g. goals, experience or abilities) or by task and environmental factors (e.g. workload, stressors or complexity).
- The relationship between the SA and *Performance of Actions* can also be predicted (Endsley, 1995). Appropriate SA increases the the probability of good performance and course of actions, but cannot guarantee it. The actions are also influenced by the same factors as the decisions.
- *Feedback* covers state of the environment or the system affected by the decision and by the performance of the selected actions.

In the SA model play time an important role. As SA is a dynamic construct affected by the surrounding environment and various factors, therefore it serves also as input in the model. These factors and aspects need to be considered also in the CSA model for NCSCs in order to timely react to the detected threats in the dynamically changing cyber space.

3.2 OODA Loop (1976)

The OODA loop was originally developed in an attempt to explain why American fighter pilots were more successful than their adversaries in the Korean War (Boyd, 1996). Compared to the SAM, the OODA Loop is made originally for supporting decision making processes. Many decisions are required in dynamic environments, especially in the ever-changing cyberspace. Therefore one of the main requirements is the obtaining and maintaining of an accurate SA. Kaempf et al (Kaempf et al., 1993) confirm also the relevance of the SA in the decision making processes. They claim that the recognition of the situation is a challenge for the decision makers. The following four major stages belong to the OODA Loop (see (Brehmer, 2005)):

- *Observe* involves the perception of some features of the environment.
- *Orient* refers to orienting within a specific environment.
- *Decide* involves deciding what are the next steps.
- *Act* involves implementing what has been decided.

The SAM and the OODA Loop describe the cognitive processes of decision making in complex environments. These models can serve as a solid base for SA gaining and decision making in NCSCs facing the evolving threat environment.

3.3 JDL Data Fusion Model (1980)

Contrary to the focus on the cognitive processes in the SAM and the OODA Loop, the next model describes the technical information processes of the SA gaining. The Joint Director's of Laboratories (JDL) Subgroup developed the Data Fusion Model (JDL DFM) (White, 1987) as an approach to refine data collected from various systems. The JDL DFM was designed to take data from any aspect of the world, e.g., flight

information or network traffic, and process it in a way that the output is more useful. The output is supposed to better estimate, predict, or assess the environment under observation (Raulerson, 2013). The JDL model has five different levels of data processing, from level 0 to 4. The levels of the JDL DFM are described as follows in (Steinberg et al., 1998):

- *Level 0* - The *Sub-Object Data Assignment* is responsible for the sensor-based data collection.
- *Level 1* - The *Object Refinement* level combines the data from Level 0 with sensors data to detect security events. The main objective of the level is to identify, detect and characterize entities, such as computers, adversaries, data flows or network connections. The output of Level 1 is a list of entities and their properties.
- *Level 2* - The *Situation Refinement* level combines various entities to provide an overview of the current state of the system or environment.
- *Level 3* - The *Threat Refinement* level predicts future states of the system or possible attacks against the system.
- *Level 4* - The *Process Refinement* level manages the system's capability for sensors and their health.
- *Level 5* - The *Cognitive Refinement* represents the link between the security analysts and the JDL DFM. In this process the analyst (performing the human cognitive processes) receives the technological support from the JDL system.

The result of these data processing levels serve as basis for the gaining accurate and present SA such as in NCSCs. Inaccurately designed data processing steps could lead to incorrect situational awareness and possibly to wrong decisions.

3.4 Cyber Situational Awareness Model (2009)

The Cyber Situational Awareness Model (CSAM) (Okolica et al., 2009) proposes a methodology for building an automated discovery engine for CSA. They further argue that any SA system must perform the three functions (perception, comprehension and projection) as described in (Endsley, 1988). These three functions match to the levels *Sense, Evaluate and Assess* in the CSAM. The system senses its environment, it takes its raw sense data and assemble it into a meaningful understanding of its environment, and uses its current understanding to predict future developments.

- *Sense* - The function includes data gathering through sensors.
- *Evaluate* - The system complies these information into a concept which matches to already existing threat concepts.
- *Assess* - The system predicts possible future activities and attacks.

All these functions are essential in NCSCs to foreseen emerging threats and to be able to prevent future attacks.

3.5 Situation Awareness Reference Model (2010)

The SA Reference Model (SARM) in (Tadda and Salerno, 2010) is a combination of the JDL DFM and the SAM. The SARM provides a set of definitions of the necessary elements of the model, such as entity, group and events.

- *Level 0* is the data and sensor management.
- *Level 1* is about *Object Recognition & Tracking* covers the perception level from SAM.
- *Level 2* (Comprehension) and *Level 3* (Projection) cover the *Situation Assessment*. According to the authors, Level 3 in the JDL Data Fusion as well as Level 2 on Endsleys model address the current situation, while the Level 3 in the JDL Data Fusion Model is associated with the future
- *Level 4* covers the feedback feature in the system. This process includes refinement for internal and external processes.

This model enables flexible reactions to the changing threat landscape.

3.6 Effective Cyber Situational Awareness (2014)

The Effective Cyber Situational Awareness model (ECSA) by (Evancich et al., 2014) focuses on a particular type of CSA: a holistic view of SA within a computer network applying network monitoring. The ECSA model includes three main phases:

- *Network Awareness* includes the analysis and enumeration of assets and of defense capabilities.
- *Threat or Attack Awareness* establishes a current situation picture of possible attacks and vectors against the network in question.
- *Operational or Mission Awareness* establishes SA of the operation e.g., how decreased or degraded network operations will affect the mission of the network.

ECSA aims at providing better intelligence about the status of the network than regular CSA. The ECSA is CSA that improves decision making, collaboration, and resource management (Evancich et al., 2014). Moving from CSA to ECSA requires that the CSA created by the system provides the analysts to have a better intelligence about the status of the network. Therefore ECSA tries to provide actionable intelligence about the network.

3.7 Survey Summary

The interpretation of the SA changes according to the application area. SA gaining processes need different information depending on the scope, ECSA requires for instance particularly network information, while SA in the NCSCs use a wide range of information type. Despite the broad application range most of the models for SA gaining share one similarity: they are based on the general definition and most cited model of SA by Endsley (Endsley, 1988) (for more details see Section 3.1). Therefore the described components by Endsley serve as a basis for creating a novel process for SA gaining and applying by combining already existing, suitable models.

Figure 1 summarizes the analysis of the presented models.

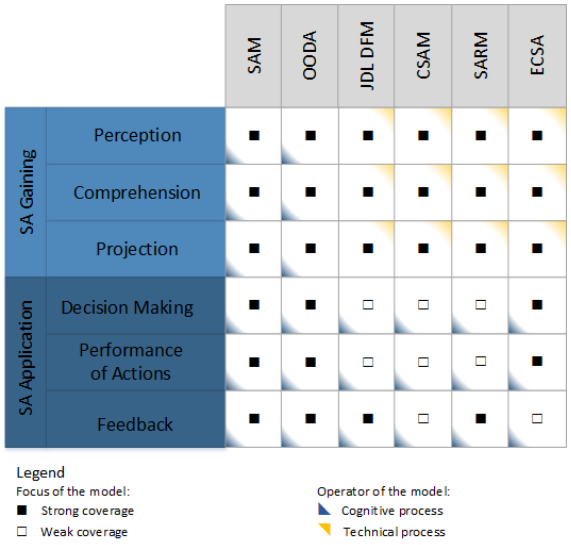

Figure 1: Applicability of Different Models for SA

Based on the six components of the SAM (see Section 3.1) are the models analyzed and assessed regarding their applicability in NCSCs. The processes of the models are divided into two main categories, in SA Gaining (with Perception, Comprehension and Projection) and in SA Application Processes (with Decision, Performance of Action and Feedback). The significant processes within the models are represented by filled black squares, while the processes with weak coverage by blank squares. The analysis of the models is based on two main aspects: on the *focus* of the models and on the *operator* (i.e. a person or a machine/program that establishes SA). Both aspects are displayed in Figure 1.The processes performed by machines are marked with the blue edge below, while processes using cognitive skills of human operators are marked with the yellow edge above.

3.7.1 Focus of the Models for SA

To define the focus and the scope of each relevant model for gaining and applying SA, the models are compared to the components of the SAM (see Section 3.1). Establishing SA is a major and complex task. Therefore, two main processes, *SA Gaining* and *SA Application*, are required. Figure 1 illustrates the phases of SA gaining (Perception, Comprehension and Projection) and SA application (Decision, Performance of Actions and Feedback).

The **SA Gaining** phase contains the three levels based on SAM (Endsley, 1995): *Perception, Comprehension and Projection* (see Figure 1). Based on the SAM *SA is a useful present knowledge about, and understanding of the environment*. This process is covered in all models (see e.g., the Perception and Comprehension Level in the SAM or the Observe and Orient Stage in the OODA loop). In the remaining models are sensors and algorithms responsible for the perception and comprehension of the environment. The component Projection is essential in models, because SA is typically forward looking, projecting what is likely to happen in order to inform effective decision processes (Kaber and Endsley, 2004).

SA Application contains the Decision, Performance of Actions and Feedback phase. SA is essential in dynamic environments where the information flow is high and wrong decisions can lead to serious consequences, such as in the defense of the critical infrastructures. Figure 1 shows the models that describe the decision making more comprehensive, such as the SAM, OODA and ECSA, and the models that improve the decision making by providing better intelligence, such as JDL DFM, CSAM and SARM. The OODA Loop describes for instance the steps for decision making in detail, while the ECSA provides technical features for decision making by predicting possible scenarios. The models provide an assistance by creating SA or additionally by providing options for actions for the decision makers. Ideally, the SA gaining process contains a feedback cycle between the environment and the decision maker.The Feedback component by the SAM is complemented with a

process refinement functions. The operator can have for instance the possibility to verify or modify the SA gaining processes or even their results. The feedback loops could vary enormously depending on the application area. Therefore this component is not a focus in most of the models.

3.7.2 Operators in SA Models

With the *operator* aspect, the analysis aims to assess how SA is established by humans or machines (e.g., programs) in the SA models. Figure 1 marks the technical processes with blue edges and the cognitive processes with yellow edges.

The first models, such as the SAM and the OODA Loop, focus on the human aspect in a crisis situation. They describe SA as a cognitive knowledge, what can be enriched by experience. In these model, the operator is a human, e.g. a pilot or a soldier. As of the 1980s technical sensors and their data complement the human perception, see for instance the JDL DFM. This approach defines the need for human and machine information processes in SA gaining and application. Each presented CSA model, such as CSAM, SARM and ECSA, tries to reproduce and improve the cognitive SA gaining processes with the integration of technical solutions. The CSAM proposed to be an automated data processing system sense the environment. The other models, such as the SARM and ECSA, have a different approach. They integrate the human operator in the SA creating processes with a verifier and improver role, while the SA gaining processes are totally automated. All approaches need to be integrated in the CSA model to combine the advantages of the different models in order to enhance the cyber defense capability at the national level.

In summary, based on this understanding, the modern CSA models combine the technical processes with the required human aspect. The automatized processes are usually the SA gaining processes, while the human capabilities play a significant role in the application of the gained SA. Nowadays only the SA gaining processes could be reproduced by technical processes, perhaps fully automated systems will response to the changing threat landscape in the future.

4 Situational Awareness in National Cyber Security Centers

In the previous section, the analysis shown that the presented models focus on certain phases of the SA gaining and application processes. The combination of the models can provide more comprehensive support for creating CSA in the NCSCs. The proposed CSA model presents the requirements and the necessary SA gaining and application components in the NCSCs. Finally an illustrative application scenario demonstrates the validity of the CSA model.

4.1 CSA Model for NCSCs

Governments worldwide are adopting their security strategies and capabilities (Franke and Brynielsson, 2014) or national incident response plans in order to protect the critical information infrastructures (CII) within the new threat landscape in the cyber age. Most of the initiatives are based on the National Cyber Security Strategies (NCSS). Relating to the NCSS (Luiijf et al., 2013), the governments identify essential national cyber capabilities, and clearly assign ownership of these capabilities and responsibility to a centralized NCSC. These approaches to the national cyber security are reactive and focus on the recovery processes and not necessarily on prevention. The model illustrated in Figure 2 proposes a preventive CSA model for NCSCs that addresses several requirements:

- CSA for NCSCs is a versatile, dynamic and complex process that should consider different stakeholders (national and international). The CSA model should have a collaborative approach based on data correlation and information sharing by providing suitable interfaces, i.e. Reporting Interface.
- The complete CSA model should focus on prevention, i.e. implementing an early-warning system that can prevent and detect national incidents.
- The CSA model should be flexible and open to future threats and threat actors.
- The CSA model should provide capabilities for cognitive and technical SA Gaining and Application.

Figure 2 shows the necessary SA gaining and application processes general for decision-makers in the NCSCs. The model contains CSA in three different levels with different information sources:*Organizations, National Cyber Security Center* and the level of the *Decision Makers*. The gained CSA oat the Organization level serve as a basis for creating an accurate and holistic picture about the status of critical infrastructures in the national scope (see the *SA Gaining Information Flow* in Figure 2). The participating organizations and their reporting activity through the *Reporting Interface* are primary information sources for the SA gaining processes, such

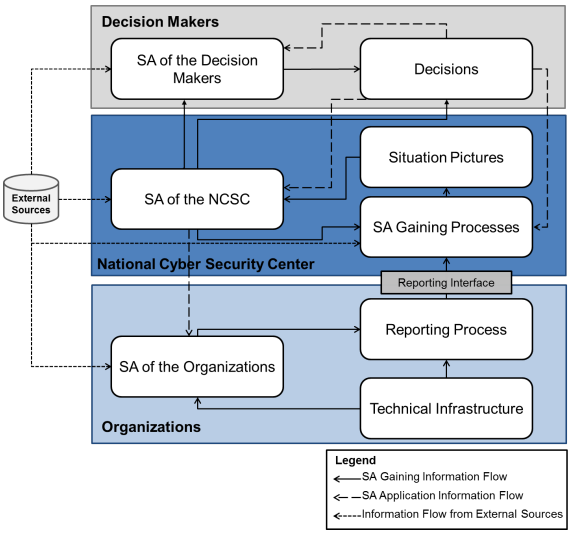

Figure 2: CSA model for NCSCs

as Perception, Comprehension and Projection, in the NCSC. Application of the CSA is present in every level, it is presented in the Figure only on the Decision Makers level because of the high relevance for the national cyber security level. The organizations and the NCSC take also decisions and perform actions on a daily basis, for the national security relevant actions are for instance the reporting of the noticed cyber incident and the undertaken measures to protect their own system. The information flow downwards, the decisions and the actions of the political decision maker have an influence on the underlying levels (see *SA Application Information Flow*). One decision from the political level could have serious consequences in case of the large-scale espionage campaign, such as releasing documents containing sensitive information (for instance the analysis of the espionage at RUAG (GovCERT.ch, 2016)). One legislative could entirely shape the cyber capability of the state, such as introducing mandatory reporting of cyber incidents, for instance in the USA or in Estonia.

Figure 2 shows also the stakeholders and entities that are involved in the SA gaining and application processes in the NSCS. As the government and their NCSS play an essential role in establishing and maintaining cyber security at national level, the model must also include the private sector, especially the providers of the critical infrastructures (CI). The governments and the private sectors need to establish formal partnerships, because the technical information from the CI domains serve as primary information source for the NCSCs. These centers are often formed as Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs). The stakeholders are the following in our simplified model: high-level decision makers, the NCSC and participating public and private organizations. The **Decision Makers** include the government and other relevant private or public stakeholders. The **NCSC** is focusing on collecting, interpreting and evaluating cyber security relevant information at national level. This is required for translating the cyber incidents within the CI domains into strategic and tactical actions at national level. The NCSC can consist of National Incident Response Teams (NIRTs); i.e. the expert team of the NCSC. The NCSC supports the decision making by creating various situation pictures and gaining SA at their level. SA is current and predictive knowledge of the environment, as well as all factors, activities and events (Conti et al., 2013). Therefore, CSA includes the holistic and current knowledge about the CI at national level. The situational pictures, also known as Common Operating Pictures (COPs), support the stakeholders and decision makers to have an appropriate CSA about the current situation. The main tasks of these centers are the information gathering from the CI domains, and from external sources (see *External Sources* in Figure 2), such as national CERTs and open source information, information processing and sharing among the participating organizations about cyber incidents. The experts of the NCSCs generate situation pictures with various focal point. These situation pictures establish the decision maker's CSA about the status of the national CI.

The **Organizations** include all participating public or private CI (or CII) service providers. The key approach to CI protection is the identification and modeling of the relevant activities, resources and services in each organization. These activities form the basis for the analysis and assessment to determine current impacts of assets and missions and to derive plausible future trends and their future impacts or effects on assets and missions (Tadda and Salerno, 2010). The organizations are usually divided into CI domains. We use the following categorizations with following domains: Electric Power, Oil and Gas Distribution, Transportation Systems, Information Technology and Communication, Banking and Finance, Public Health and Healthcare, Emergency Services, Water, Agriculture and Food, Government Facilities and Military Installations.

The presented CSA model for NCSCs includes proactive cyber capabilities in order to prevent cyber attacks through information sharing and multi-level monitoring related to cyber attacks. This modern CSA model helps to close the gap between the capabilities of the public and private sector related to cyber security. The following fictional scenario de-

tails further the application of the presented theoretical CSA model for NCSCs.

4.2 Illustrative Application Scenario

4.2.1 Scenaio Design and Background

The following application scenario focusing on information sharing takes different attacker models and motivations into account, in order to present the benefits and possible challenges of cyber attacks against critical infrastructures from various perspectives. It can be presumed, that the attackers in the following scenarios have a strong background and technical know-how, including in-depth expert knowledge regarding electrical engineering, electronics, cryptography, network security, embedded security, hardware security, and reverse engineering. Further, the attackers have solid knowledge of all latest attack vectors in those areas and have the power to put those attacks into practice. The attackers can be e.g. criminal organizations focusing on monetary return, e.g. groups of political activists, or also the cyber-divisions of adversarial governments. The scenario is designed basically with two objectives in mind. First, it must be complex enough to provide a basis for the complete functionality of the public-private-partnership in a modern CSA framework. Second, they must be realistic in the sense that the described scenario is possible within the next years. Even if the scenario is fictional, it indicates realistic future threats to the national CIs and provides a characteristic framework for the theoretical CSA model.

The following scenario is concerned with a part of a large-scale cyber espionage and how to identify and connect relevant information where big data volumes need to be handled. This is based on the Ukrainian cyber incident in December 2015. The cyber attacks in Ukraine are the first publicly acknowledged incidents to result in power outages (SANS-ICS, 3 18). Power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. In addition, there have also been reports of malware found in Ukrainian companies in a variety of critical infrastructure sectors (ICS-CERT, 2 25). Based on the DHS report, three Ukrainian oblenergos experienced coordinated cyber attacks that were executed within 30 minutes of each other. The attack impacted 225,000 customers and required the electric distribution companies to move to manual operations in response to the attack (SANS-ICS, 3 18). The threat actors are professionals with in-depth knowledge and actually sponsored by nation states. The Advanced Persistent Threats (APTs) are a cyber crime category directed at business or political targets. These attacks require complex resources and a high degree of stealthiness over a prolonged duration of operation in order to be successful. The drivers may cover additionally political and ideological motivations for the threat actors of a long-term cyber campaign. The following illustrative scenario covers a cyber attack on a power grid system and provides recommended actions for the relevant stakeholders in the modern CSA model.

The presented CSA model (see Section 4.1) offers concepts and methodologies for a multi-level data collection, swift cross-organizational information sharing processes, proper cross-domain incident communication, an early warning system and enhanced CSA through customizable big data visualization for superior decision making in both strategic and organizational scopes. The gained SA facilitates identifying and responding to cyber threats, enhances the security of essential infrastructures, increases the resistance of critical services for the society and supports decision makers to deal with cyber crises. The illustrative scenario has the following characteristics:

- Scope of the cyber incident: National scope (large-scale)
- Possible threat actors: Foreign intelligences, Hackers, Insiders, Phishers
- Quality of the threat actors: Professionals
- Attack complexity: High
- Level of authentication needed to exploit: Multiple instances
- Impact on Confidentiality/Integrity/Availability: Medium / Medium / High
- Motivation: Political, Ideological, National security
- Likelihood: Medium
- Target domains: Electric Power

With this use illustrative application scenario (see Figure 3), we aim to demonstrate the following for the CSA model:

- describe the incident detection at CI providers (see Section 4.2.2)
- demonstrate information sharing capabilities between the NCSC and the CI (see Section 4.2.3)
- describe how SA is provided at the level of the organizations (see Section 4.2.4), NCSC (see Section 4.2.5) and decision makers (see Section 4.2.6).

4.2.2 Incident detection in the energy domain

In the fictional European country, Norland, three main energy suppliers are responsible for the electricity generation, distribution and transmission and for serving customers within the country. In Norland are two

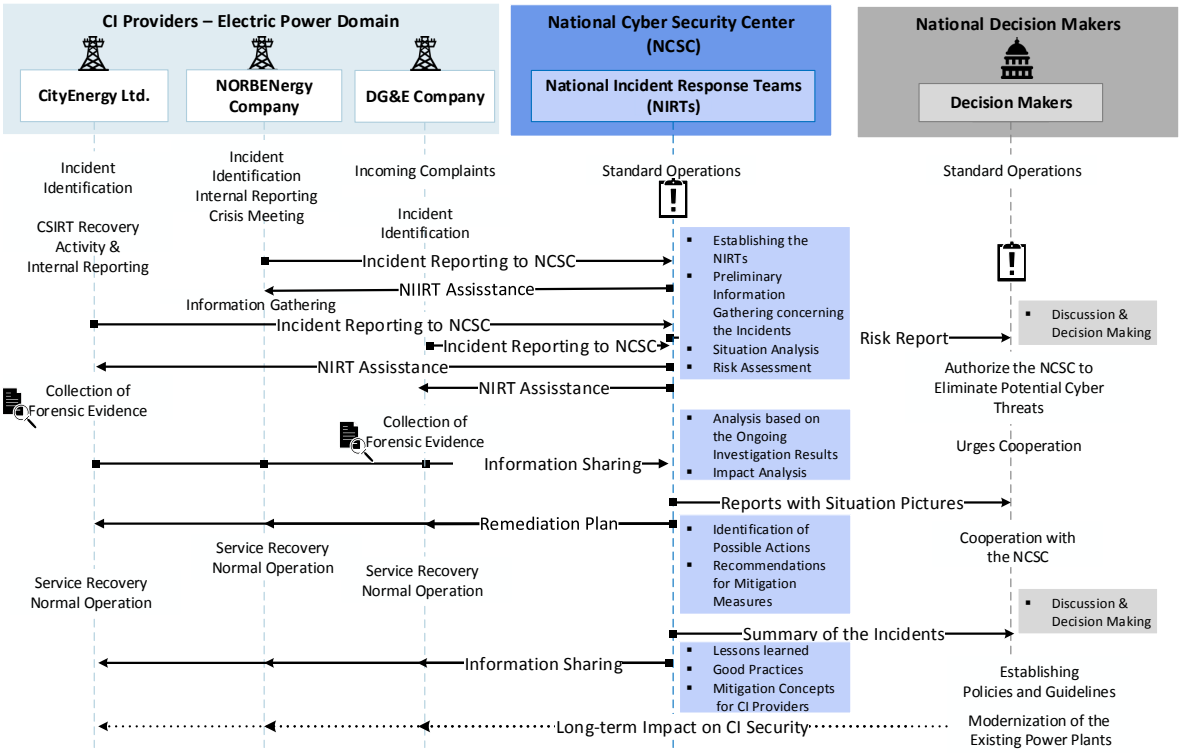

Figure 3: Information Sharing Scenario

thermal power plants (DG&E Company) and three hydro power plants on the Norben River (CityEnergy Ltd and NORBENergy Company. 80% the electricity is produced by the three hydro power stations, and the remaining 20% is generated by dilapidated infrastructure of the thermal power plants. The demand of electricity is increasingly higher than the domestic generation. Therefore Norland needs to import energy from the neighbor states.

One of the three main energy service provider,the NORBENergy Company, realizes at 10 a.m. that two of their substations are not in service. The responsible technicians check the substations and make necessary temporary solutions in order to supply energy to several important facilities from the remaining substations. In the meantime, the company's IT team reports the incident to the CISO and tries to recover the system according to the incident response plan. Two hours after the service outage, the organization summons an adhoc meeting and more IT employees because of the crisis situation. Before the emergency meeting with the management, the IT team assess the situation of the services and technical infrastructure, conducts an analysis related to the possible energy supply level. Based on the impact analysis, the members of the meeting decide to report the incident to the NCSC at 1 p.m. in order to quickly fix the supply problem. In the meantime, the IT team tries to find a solution and solve the problem and the call center deals with the incoming complaints from the customer-side.

The largest energy service provider, the CityEnergy Ltd, notice also major failures and substation outages in their systems at the same time. The company observes the service outage due to the 7/24 service monitoring system of the company, namely that four of their substations were disconnected from the power supply system. The CSIRT of CityEnergy starts immediately the necessary actions with respect to the disaster recovery plan. The company activates their own incident response team and begins with the data gathering about the incident, business impact and risk analysis. Parallel the initial actions of the CSIRT, they report the incident internally to the executive level. 2 hours after the incident detection, the CSIRT attempts to recover the missing services without any success. Furthermore, the call center appears to be paralyzed but the actual causes are still unknown. Therefore, the company alerts the NCSC at 2 p.m.

The owner of the thermo power plant, DG&E Company, receives numerous complaints, that customers noticed problems concerning the energy supply. The employee of the call center alerts internally

the technicians. Based on the system analysis, the technician realizes that both of their substations are disconnected and not working. The DG&E Company has an obsolete and technically outmoded infrastructure and no disaster recovery plan, business continuity plan or incident response team. The IT team covers only 2 employees, who try to identify the cause of the failure unsuccessfully. After one hour, the first internal report is provided to the management. The executive director of the company realizes that they have not the necessary expertise to solve the service outage. But the company is a participating organization of the NCSC, therefore the DG&E Company reports the NCSC about the service outage at 2 p.m.

4.2.3 Information Sharing and Reporting

The NCSC receives an incident report from the NORBENergy Company through the NCSC Reporting Interface. The company has a small customer base with 50,000 customers, but belongs to the important CI providers in the country. Shortly after the incident report, the NCSC composes a group of experts, called NIRT, concerning the energy domain in order to collect open source information about the possible causes and to clarify important details about the service outage. The NCSC contacts NORBENergy and sends the NIRT in order to assist at the service recovery. One hour after the first report comes another report from the energy domain. The largest energy distribution company, CityEnergy Ltd, notifies that their substations are not under their control and disconnected from the system. As is in the first case establishes the NCSC a new NIRT in order to offer assistance to the energy provider (depicted with NIRT Assistance in the Figure 3).

Based on the preliminary information gathering of the NCSC, there have been reports of malware found in the neighbor countries compromising systems in the energy domain. These findings presents a potential risk at the national level, that the systems (actually ICS or SCADA systems) are infected and/or compromised in the energy sector. The NCSC informs the competent national authorities about the potential cyber attacks against the energy service providers. The reporting activity is presented as Risk Report in the Figure 3. The detailed impact analysis and recommendations could be delivered only after further investigations in the victim organizations. The decision makers authorize the NCSC to use all available means to eliminate the potential cyber threats endangering the national energy infrastructure and urges unconditional cooperation from the victim organizations with the incident response teams of the NCSC. The Reporting Interface receives a new notification, but this time from the thermal power plant company, the DG&E Company. The NCSC sends immediately a response team to the energy provider in order to collect forensic evidence on the incident.

4.2.4 SA for Organizations

The primary aim of the NIRT assistance in crisis situations is to support the company to recover the essential services and business processes of the victim organizations. The first phase of the assistance process is carried out in progressive stages and covers usually the SA Gaining Processes of the modern CSA models, mainly the Perception and the Comprehension. The Projection belongs partly to the second phase of the assistance process. The first levels of the modern CSA models, namely the perception of status, attributes of the relevant services within the victim companies. The next stage is the understanding of the current situation in the compromised system. The NIRTs are gathering and sharing more and more information. In that way they could reconstruct the attack tactics, techniques and procedures at the end of the assistance. After the incident reports, the NIRTs are collecting evidence locally in the compromised systems, seeking for vulnerabilities, patching insecure systems, investigate concerning potential attack vectors and point of failures.

4.2.5 SA for NCSCs

In the second phase of the assistance includes the Projection. This sub-process is running partly parallel to first phase using existing knowledge concerning the national energy domain and external information sources, and partly after the completion of the first phase using their findings as a basis. In our scenario, the experts in the NCSC headquarter are assessing the current situation within the energy domains and the potential effects and future impact of the cyber attack at various levels. The analysis is based on the ongoing investigation results (see Information Sharing in Figure 3 to the NCSC)and on various external information sources. These reports will serve as a basis for the decision makers in order to gain an adequate CSA.

On the one hand the NIRTs are building remediation plans for the victim organizations and optionally provide assistance in the full recovery processes. This activity (depicted as Remediation Plan in Figure 3) complies with the Resolution sub-process in the modern CSA models for the participating organizations. On the other hand, the NCSC is summarizing the findings out of the Projection and Resolution

sub-processes. These reports contains situation pictures about the current and the possible cyber situation in the energy domain, demonstrates fundamental dependencies among the essential services and offers demonstrations of potential cascading effects. All of these situation pictures could be sum up as the SA of the NCSC. The NCSC sends and presents the required sections to the national decision makers. The CSA gained by the NCSC serve as a basis for the high-level decision makers to gain their own SA concerning the cyber attack against the national CI.

One of the essential tasks of the NCSC is to identify possible actions and make recommendation for mitigation measures at the organizational level in order to prevent conflicts or for avoiding escalation at the national level. The recommendations of the NCSC covers the resolution in the modern CSA models and serve as a basis for the decision making. According to the recommendations of the NCSC, the victim organizations are able to recover the essential service within 4 hours with the help of the NIRTs.

4.2.6 SA for Decision Makers

The report about the cyber incident and the situation assessment of the NCSC enhance the CSA of the decision makers in the relevant (special political) institutions. The summary of the incidents reconstructs the history and the attacker‘s tactics, techniques and procedures (TTPs). According to the report, the service outage in the three electricity distribution companies were caused by remote cyber intrusion arriving presumably from the neighboring state. The cyber attack compromised company internal computers and SCADA systems at 10 in the morning. The cyber attack was coordinated and synchronized beginning with an extensive reconnaissance of the victim networks. The advanced campaign covered the following techniques: long-term reconnaissance with malware infection via spear phishing, weaponization by embedding BlackEnergy malware within Microsoft Office documents, using stolen credentials to the business networks, use authorized VPN connections to enter ICS network, SCADA hijack with malicious operation, DDoS attack against the companies‘ call center. Each company had been infected with BlackEnergy malware delivered with spear phishing mails and selected files were deleted by executing KillDisk malware at the end of an advanced campaign.

According to the fact that there may also be political motivation behind the cyber attack, the decision makers need to reconsider the country’s energy policy concerning the energy dependency, and the national energy supply infrastructure. Due to the excellent potential and feasibility of hydro resources in Norland, the government plans the increase the generation capacity in the existing power plants and to construct new electricity generating capabilities. The defined strategic goals cover the reduction the dependence on energy import (including natural gas imports and other fossil energy sources) thorough the capacity increase of the domestic power plants. The modernization and construction covers the enhancing of the security capabilities of the power plants, including cyber security aspects. Consequently, the long-term strategy of the national decision makers has a major impact on the cyber security of the national CI providers and their security architecture (see Long-term Impact in CI Security in Figure 3). Furthermore, the relevant governments institutions establish policies and set down guidelines. These documents provide specific mitigation concepts, best practices and checklists for ICS and Supervisory Control and Data Acquisition defense in the energy domain. The secondary goal is to enhance the safety and security in the CI domains focusing on the Energy domain.

The last phase covers the Feedback phase (cmp. Figure 1). The NCSC provides summaries of the public information concerning the cyber attack and the technical analysis by the NIRTs. These documents are available for all participating company (see Information Sharing to companies in Figure 3) and they cover the identified lessons learned, good practices, and specific mitigation concepts for CI providers focusing on the defense of SCADA and ICS systems. These documents created by the NCSC‘s experts could be considered as guidelines or the political decision makers could raise the content of the document to directive or to national legislation concerning CI providers and raise the CSA on the organizational level.

5 Conclusion

Due to the increasing attack surfaces on ICT and CII systems and limited, national cyber capabilities, the number of service disruptions and cyber attacks against essential systems and networks is constantly rising. Hence, CSA is a required capability of national stakeholders in order to be able to ensure the safety and security of the national critical infrastructures. Despite the international guidelines and recommendations, there is still no holistic model for gaining and applying CSA of the national CI. Furthermore, our survey of the existing models for SA gaining and application argues on the strengths and limits of the models concerning new requirements (see Section 3), i.e. a holistic approach is missing.

A key success factor to establish CSA is the pro-

motion of cooperation between the public and private sector. Depending on the scope, CSA on national level can only be aggregated by information sharing and collection in cooperation with organizations. Organizations establish SA on a technical and organizational level. At national level, this information is processed and analyzed in order to support national decision makers. In this paper, we proposed a CSA model for NCSCs for SA gaining and decision making in the event of large-scale cyber incidents with various escalation levels. This modern CSA model can manage cyber security incidents with prevention: using a common information-sharing environment allows the early detection of sophisticated attacks, or even large-scale cyber campaigns against the national critical infrastructures. To demonstrate our approach, we illustrated an information sharing scenario based on a past nation-state attack against the CIs.

For future work, we aim to further develop and investigate the CSA model for NCSCs focusing on legal aspects and examining the impact of international cooperations.

Acknowledgements

This study was partly funded by the Austrian FFG research program KIRAS in course of the project CISA (850199).

REFERENCES

Artman, H. (2000). Team situation assessment and information distribution. *Ergonomics*, 43(8):1111–1128.

Biernacki, P. and Waldorf, D. (1981). Snowball sampling: Problems and techniques of chain referral sampling. *Sociological methods & research*, 10(2):141–163.

Boyd, J. R. (1996). The essence of winning and losing. *Unpublished lecture notes*.

Brehmer, B. (2005). The dynamic ooda loop: Amalgamating boyds ooda loop and the cybernetic approach to command and control. In *International command and control research technology symposium*, pages 365–368.

Conti, G., Nelson, J., and Raymond, D. (2013). Towards a cyber common operating picture. In *Cyber Conflict (CyCon), 2013 5th International Conference on*, pages 1–17. IEEE.

Endsley, M. R. (1988). Situation awareness global assessment technique (sagat). In *Aerospace and Electronics Conference*, pages 789–795. IEEE.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37(1):32–64.

European Parliament (2015). The directive on security of network and information systems (nis directive).

Evancich, N., Lu, Z., Li, J., Cheng, Y., Tuttle, J., and Xie, P. (2014). Network-wide awareness. In *Cyber Defense and Situational Awareness*, pages 63–91. Springer.

Franke, U. and Brynielsson, J. (2014). Cyber situational awareness A systematic review of the literature. *Computers & Security*, 46:18–31.

GovCERT.ch (2016). APT Case RUAG. `https://www.melani.admin.ch/dam/melani/en/dokumente/2016/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf`. [Online; accessed 16-July-2016].

ICS-CERT (2016-02-25). Cyber-attack against ukrainian critical infrastructure (dhs). `https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01`. Accessed: 2016-04-25.

Kaber, D. B. and Endsley, M. R. (2004). The effects of level of automation and adaptive automation on human performance, situation awareness and workload in a dynamic control task. *Theoretical Issues in Ergonomics Science*, 5(2):113–153.

Kaempf, G. L., Wolf, S., and Miller, T. E. (1993). Decision making in the aegis combat information center. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 37, pages 1107–1111. SAGE Publications.

Luiijf, E., Besseling, K., and De Graaf, P. (2013). Nineteen national cyber security strategies. *Int'l Journal of Critical Infrastructures 6*, 9(1-2):3–31.

Okolica, J., McDonald, J. T., Peterson, G. L., Mills, R. F., and Haas, M. W. (2009). Developing systems for cyber situational awareness. In *2nd Cyberspace Research Workshop*, page 46.

Onwubiko, C. (2012). *Situational Awareness in Computer Network Defense: Principles, Methods and Applications: Principles, Methods and Applications*. IGI Global.

Raulerson, E. L. (2013). Modeling cyber situational awareness through data fusion. Technical report, DTIC Document.

SANS-ICS (2016-03-18). Analysis of the cyber attack on the ukrainian power grid. `https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf`. Accessed: 2016-04-25.

Steinberg, A., Bowman, C., and White, F. (1998). Revisions to the JDL Model. In *Joint NATO/IRIS Conference Proceedings, Quebec, October*.

Tadda, G. P. and Salerno, J. S. (2010). Overview of cyber situation awareness. In *Cyber Situational Awareness*, number 46 in Advances in Information Security, pages 15–35. Springer US.

White, A. (1987). Data fusion lexicon, joint directors of laboratories, technical panel for c3. *Naval Ocean Systems Center, San Diego, Tech. Rep*.