A Public-Private-Partnership Model for National Cyber Situational Awareness

Timea Pahi and Florian Skopik

Digital Safety and Security Department
AIT Austrian Institute of Technology, Austria

ABSTRACT

The information age has led to the merger of various infrastructures, from both business and governmental sectors and their functions, such as information technology, communication and transport systems, banking and finance, energy supply and process control systems. The protection of these systems is essential to resilience and reliability of critical infrastructures and their key resources, consequently to the national security and economic prosperity. The presented public-private-partnership cyber situational awareness (P3CSA) framework provides the mean for swift information flows among the national and private stakeholders working in a strong cooperation. The P3CSA framework 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 cyber situational awareness through customizable big data visualization for superior decision making at both strategic and tactical levels. The gained situational awareness 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.

Keyword: cyber situation awareness, national level, critical infrastructure

1 INTRODUCTION

Our society lives in a world dominated by information and communication technology. The protection of the cyberspace has become increasingly important for the nationwide security, economic well-being and public safety.

Nowadays private operators provide critical services, such as energy supply, transportation or banking services. Those services are essential to maintain public order and safety and thus, it is in the interest and responsibility of a state to guarantee the security of these infrastructures (NIST, 2014). Since the state cannot interfere with private operators, they need to set up a formal partnership. One of the visions is that the state directly supports infrastructure providers to secure their service operations by distributing important security information to target users, while they provide security-relevant information, such as their services' status, or spotted indicators of compromise in their networks, to the state. This data from every single organizations is essential to create a clear picture and cyber situational awareness of the operational environment, thus to create the basis for justified and effective decision making by complement authorities at national level. In the recent years, solutions for the technical data gathering and processing within organizations have been developed (Leopold, Bleier & Skopik, 2015), as well as strategies have been already researched based on cyber situational awareness in the national scope (ENISA, 2012). The objective of this paper is to fill the gap in between and create a link from the technical data to the strategic decisions regarding the tackling of cyber threats. Cyber situational awareness (CSA) is a required capability of national stakeholders and governments to effectively perform their operations relying on the contemporary knowledge about the technical status of critical infrastructures. This situational awareness requires a holistic methodology to synthesize perception, identify and visually represent the current trends, and construct future projections.

In this paper, we suggest the P3CSA framework that supports strategic and tactical decision making through processing and visualization of aggregated and interpreted security information obtained from private stakeholders. Developing a detailed picture of the nationwide security situation is a complex challenge. Similar to some conventional national cyber security strategies (Luiijf, Besseling & De Graaf 2013), our approach of the P3CSA model relies on strong collaboration between the state and private actors. Furthermore, it is noteworthy that a fundamental part of the P3CSA model is the human factor.

This paper consists of the following contributions:

- We motivate the need for a public-private partnership model, with humans-in-the-loop and shared responsibilities among the state and the private sectors.
- We propose a framework, which links the operational and the strategic level, and uses a common language and system to address and manage

cyber security threats in a cost-effective way based on national and business needs and in line with the European NIS directive (EC, 2013).
- We show an illustrative instantiation of the framework and demonstrate its application to gain and visualize cyber situational awareness to support tactical and strategic decisions making.

The remainder of the paper is organized as follows: Section 2 describes the background of situational awareness and the related work, Section 3 deals with the presentation of the cross-organizational collaboration, followed by the P3CSA framework and its abstraction levels in Section 4. After defining the stakeholders and responsibilities, the data reporting processes and visualization are described in detail in Section 5 and 6. Finally, the last section concludes the paper with the discussion of challenges and chances of the framework, including the future work.

2 BACKGROUND AND RELATED WORK

There are several definitions of situation awareness. The first definition was recorded in the mid-1980s, but the use of the term 'situational awareness' can be traced back to World War I (Onwubiko and Owens, 2012). Until 1995 nearly all of the existing situation awareness (SA) definitions had military application, motivated by the growing interest in understanding the pilots' mental model, processes of perception and decision making during the operations and air battles. A widely applicable general definition for situation awareness is proposed by Mica R. Endsley. His definition states that SA is "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the future" (Endsley, 1995). Most of the early definitions focus on the human aspect in distinct crisis situations. They describe SA as a cognitive knowledge, which can be enriched by experience. Regarding these former definitions SA is a based on knowledge about, and understanding of the environment. In 1997 a new approach is introduced, that technical sensors and their data could complement the human perception. This approach defines SA in human-machine systems as conscious awareness of actions within two mutually embedded four-dimensional envelopes (Beringer & Hancock, 1989). Endsley distinguishes between situation awareness, "state of knowledge", and situation assessment, "process of achieving, acquiring, or maintaining situation awareness". This distinction becomes important for the application of situation awareness in the cyber environment.

Cyber situational awareness (CSA) concerns awareness regarding cyber issues. The issues need to be fused with physical information to obtain full

understanding regarding the situation. Hence, cyber events offer additional insight about the overall situation (Franke & Brynielsson, 2014). Furthermore, CSA is a kind of asset that is inquired by governments and enterprises related to their information and control systems. From a technical view, CSA is compiling, processing and fusing data. Such data processing includes the need to be able to assess data fragments as well as fused information and provides a rational estimation of its information quality (Arnborg, Brynielsson, Artman & Walleniu, 2000). Based on the definition of situation awareness provided by Endsley, SA contains three steps or levels. The constructs of perception, comprehension and projection can be taken to denote increasing awareness levels from basic interception of important data, interpretation and combination of data into knowledge, and ability to predict future events and their applications (Endsley, 2000). McGuinnes and Foy extended the model by adding a fourth step, which is called resolution. This step tries to identify the best path to follow to achieve the desired state change to the current situation. Resolution results from a course of action from a subset of available actions (Tadda & Salerno, 2010).

CSA refers to the ability to create cyber consciousness during normal operation and crisis situation. It gives the ability that a human decision maker can appropriately respond to cyber attacks regarding the information collected in the cyberspace nationwide. In this sense, CSA is an adaptive and outward-focused consciousness that provides decision makers vital information on the operation of complex and dynamic systems. It involves both technical and cognitive aspects. The combination of information from cyber sensors (e.g. such as intrusion detection systems) and ordinary methods (e.g. human intelligence reports) is required to provide appropriate overall situational awareness.

3 THE NEED FOR CROSS-ORGANIZATIONAL COLLABORATION

The interconnected national infrastructure is as secure as the weakest component in the system. These dependencies create growing attack surfaces and additional vulnerabilities for cyber domains and even for the whole state. The tackling of borderless cyber threats requires extensive collaboration, such as cross-organizational or cross-domain information exchange, in order to mitigate devastating and potentially cascading effects of cyber attacks.

3.1 DEALING WITH A CHANGING THREAT LANDSCAPE

The information age changed the dynamics of conflict around the world. The grinding attrition of industrial-age of the past century, whereby interaction occurred face-to-face, is currently giving way to information-age conflicts (Moffat, 2006). According to a NATO communiqué, cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as conventional attacks. In addition, a cyber attack on one of the member states could lead to the invocation of Article 5 (NATO, 2014).

Classic military doctrines, in which the defender has numerous advantages, are completely up-ended in the cyber domain where the attacker is advantaged. The advantages to the cyber attacker are numerous and include: *anonymity:* the ability to hide in a global network across national sovereignty an jurisdiction boundaries complicates attack attribution; *targeted attacks*: adversaries can pick the time, place, and tools; *exploitation:* global reach to probe weaknesses of the cyber defense; *human weakness*: trust relationships are susceptible as evidenced in social engineering attack; and *forensics*: volatile and transient nature of evidence complicates attack analysis, which can be quite cumbersome. Although there are differences between kinetic and cyber domains, it is likely that many of these challenges to cyber operations can be addressed by applying lessons learned from the successful management of kinetic operations (Jain, 2005). The national and economic security depends on the reliable functioning of critical infrastructures. Our dependency upon networked organizations has the consequence that warfare is no longer limited to the physics of the conventional battlefield (Kott, 2014). Cyber attacks are borderless and can be launched from virtually everywhere. As the expansion of ICT systems increases, so does the vulnerability to attacks on national critical infrastructures through the cyberspace. Therefore, the focus is now on the potential vulnerabilities of the national infrastructure associated with the sustainability of the states.

3.2 COLLABORATION AS A GENERAL MITIGATION STRATEGY

As mentioned before, cyber challenges transcend national borders and different domains. In the past years, network attacks and service disruptions have become increasingly common and caused extensive problems because of the lack of effective risk management and collective or collaborative information-sharing framework at national level. Examples from the last five years are e.g. the worldwide cyber attack campaigns called “Red October”, Infection of South Korean financial institutions, major cyber attack against the Canadian government or the well-known Stuxnet computer-worm designed to infect the ICS of the centrifuges in the Natanz nuclear

facility in 2010 (NATO, 2013). All these attacks had the common objective of collecting information from government embassies, research firms, military installation, energy providers, nuclear and other critical infrastructures. Therefore, the P3CSA approach supports extensive collaboration, including different scopes. Since governments should exercise greater responsibilities in protecting the nation's critical infrastructure from physical and cyber attacks, this task includes building cyber capabilities as a part of conventional warfare. Information sharing is a key part of the government's mission to create cyber situational awareness of malicious cyber activity nationwide and international. The governments and security experts are faced with the challenging task to develop cooperative strategies and frameworks at the international level and implement these primarily with the relevant national public and private stakeholders in the countries.

4 THE P3CSA FRAMEWORK

Modern cybersecurity threats take advantage of the larger attack surface of critical infrastructures, caused by their inherent interconnectedness (Lewis & G., 2014) and often insufficient security design considerations, for instance in ICT networks and the industrial control systems such as SCADA systems (ENISA,2011), placing the state's public safety and economy at risk. To better address these risks, we propose a public-private partnership which has the capabilities to enhance security and maintain a safe cyber space.

4.1 DESIGN PRINCIPLES OF THE P3CSA MODEL

The designed "public private partnership cyber situational awareness" (P3CSA) framework follows the following design principles:

- P3CSA includes private as well as governmental organizations and covers all management and decision levels from the organizational scope to the European scope in order to provide a holistic picture of the cyber threats in the state. Our model is inspired by the Pan-European Public Private Cooperation of ENISA in the telecom sector (ENISA, 2014).

- The P3CSA model adapts organizational structures and predefined information channels to create a dynamic reporting mechanism. One of the most important objectives of the model is the multi-level early warning process that helps to avoid most attacks, or help to quickly detect and stop attacks to minimize their impact.

- Our model provides rapid insights into cyber situational awareness while actively countering information overabundance by flexible selec-

tion and interpretation of significant incidents and risks with highest probability or impact in the continuously changing threat landscape.

- The P3CSA processes are based on the human-in-the-loop model (HITL). It attempted to find the appropriate balance between human experts, such as incident classification or software development, and automatic processes, such as intrusion detection, data analysis etc. HITL allows the participants in the P3CSA model to interact or to change the outcome of different processes and incident.

- The cooperation structures are designed to respond to cyber incidents with cross-border and cross-domain dimension, and to improve preparedness and engagement of the public-private partnership, according to the future implementation of the EU NIS directive (EU, 2013).

4.2 THE P3CSA ABSTRACTION LEVELS

Both private and public stakeholders and partner organization form the basis of the P3CSA model at different levels, see in Figure 1. The concrete role-matching participants and actors for each level could be different depending on the context of implementation-specific factors. A possible example is shown in Table 1, where the data processing and information flows are pictured with the white arrows. The possible scopes in our model include European, national and organizational scopes. The often non-effective international cooperation between industries, law enforcement, regulatory bodies and international organizations pose a global challenge. Given the global nature of cyber threats, states must collaborate to identify and mitigate extended attacks. Therefore the widest scope is the international scope, which includes the grand strategic level. This level is responsible for the information collection by using international information sources. Furthermore, European-wide (or even global) early warnings are created by sharing and exchanging information to reduce the impact of wide-ranging cyber attacks and to improve prevention and resilience. Diverse legal spaces justify the need for a national scope which is divided in two levels; strategic and tactical level. This scope is a national nexus of cyber and communication integration for the governmental and private organizations, the intelligence community and for law enforcement. At the national scope, the National Security Council provides a strategic platform for cooperation between the members of the relevant state actors, such as representatives of Ministry of the Interior, Ministry of Defense, industry leaders, academia and law enforcement agencies.

Their missions are the following:

- Distribution of national cyber security policies and guidelines

- Sharing and exchange of information in international and national cooperation in order to expand national expertise
- Capacity building to ensure sustainability of essential services
- Establishing an efficient legal framework for tracing criminals and enabling prosecutions

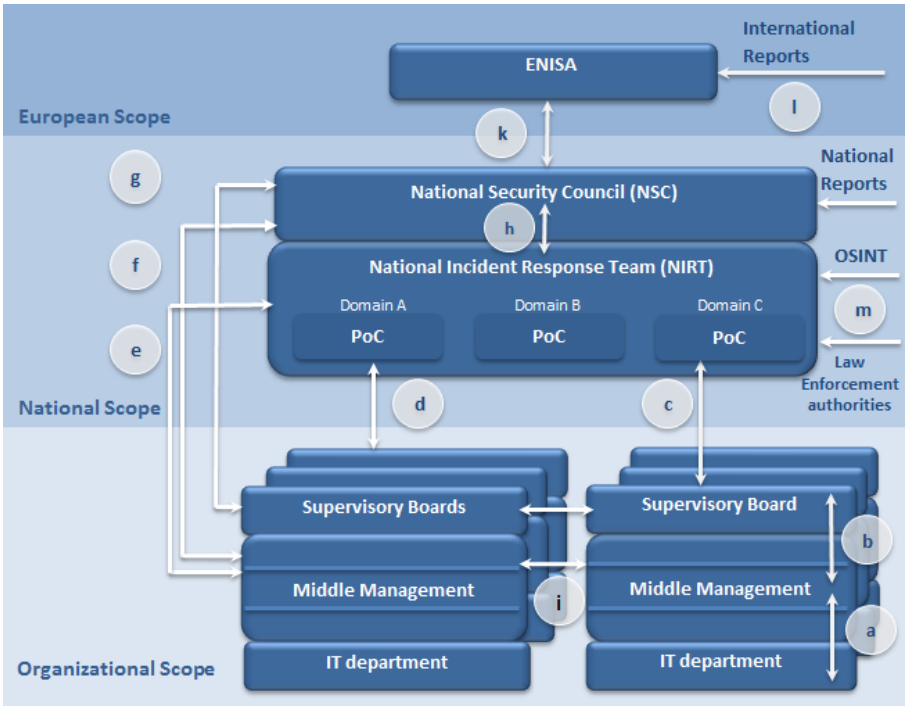

Figure 1 - Different CSA information flow levels

In contrast to long-term strategic decisions, tactical decisions usually help to implement the strategy developed at the higher levels. The tactical level, with the guiding role of the National Incident Response Team (NIRT), provides a collaborative platform for authorized cyber experts to collaborate with each other in a secure and trusted environment. NIRT is a high level expert group that assesses cyber threats and risks, responds to a cyber incident so that the network could recover as fast as possible and avoids potential future incidents. The members of the NIRT include threat analysts and Point of Contacts (PoC) from every CI domain, service providers, academics, or first responders such as regulatory bodies, law enforcement and emergency management. They provide federal guidance in each domain and across all domains. Threat analysts of the NIRT, they can include the PoCs, are trained to identify anomalous activities and focus on detecting extensive

attacks and advanced persistent threats crossing several organizations or domains. At the tactical level, the NIRT is responsible for internal and external data collection, incident classification, early warning and for rapid cyber incident response nationwide.

Scope	Level	Stakeholder/ Actor	Task
European	Grand strategic	ENISA	▪ Create international guidelines and global strategies
National	Strategic	National Security Council	▪ Presentation cyber security policies, guidelines and strategic proposals in the national scope ▪ Strategic and investment decision making
	Tactical	National Incident Response Team	▪ Threat and risk analysis ▪ Predict future events, trends and their impact nationwide ▪ Help the decision making by visualizing key facts ▪ Making concrete recommendations and countermeasures (e.g. antivirus configuration, software inventory etc.) ▪ Early warning at national level
Organizational	Executive	Supervisory Board	▪ Submission of information security policy in the organization ▪ Strategic and investment decision making
	Business	Middle Management	▪ Threat analysis and event classification ▪ Decisions on concrete countermeasures in line with security policies ▪ Incident reporting
	Operational	IT department	▪ Technical data collecting ▪ Asset management ▪ Enterprise-wide cyber threat analysis ▪ Real-time infrastructure monitoring ▪ Anomaly detection

Table 1 - Overview of CSA levels

The lack of wide adoption of a comprehensive system, that monitors the organizations' services' stability across the critical infrastructure domains, places the essential critical infrastructures at risk (EC, 2013). In the present cyber environment, incident detection and response is a permanent challenge for many organizations. Therefore, the narrowest scope is the organizational scope. It is divided in three different stages: executive level, busi-

ness and operational level. Actors of the *executive level*, such as the supervisory board or the top level management, are able to understand the effects of the vulnerable elements in their infrastructure. They are in charge of strategic and investment decision and about future implementations, and of enhance defense capacity in the company. The *business level* plays the bridge role between the executive and the operational level. There are different numbers of business layers in each organization, depending on size and maturity. Their tasks cover threat analysis, event classifications and report generation about cyber incidents.

The lowest layer is the *operational level* in the organizational scope. The cybersecurity issues cannot be solely solved at a technical level, but this is the significant level to curb threats, combat cybercrime and promote cyber security. At this level the IT department, including security engineers, security architects and system administrators, is accountable for the uninterrupted operation of the system and for its security. The main goals are the technical data colleting, asset management, infrastructure monitoring, statistical cyber threat analysis and rule-based anomaly detection. The technical team is responsible for an uninterrupted operation of the key services and resources. Decisions at this level relate to the day-to-day operation of business infrastructures. Private and public sectors should develop at operational level their own cyber resilience capabilities.

4.3 PROCESS MODELS FOR DATA COLLECTION, PROCESSING AND REPORTING

Traditionally, competing organizations are reluctant to share information especially when it comes to potentially sensitive security information (Barett & Konsynski, 1982). The organizations are attempting to preserve their anonymity. There is some information sharing platform used by the organization voluntarily. Malware Information Sharing Platform (MISP) is one of these initiatives for sharing, storing and correlating Indicators of Compromises of targeted attacks. In relation to this essential aspect, P3CSA provides the means to facilitate anonymous information sharing by explicitly stored and monitored rules by a third party. The P3CSA framework allows sharing information in a wide range to provide greater understanding of cyber situational awareness of incidents, vulnerabilities, intrusions, mitigation and recovery activities. The creation and maintenance of the incident reporting processes raise legal as well as technical issues. P3CSA provides an efficient and cost-effective way to comply the protection of national CI via information sharing, early warning and support of decision making with both adequate cyber situational awareness and legal requirements. The framework proposes a structure that allows sharing data and reports in in-

cremental steps. Internal and external data is collected, processed and reported to the levels above. The data collection, such as technical data from the operational level, helps companies to identify network traffic patterns, configuration gaps, malignant backdoors and routing anomalies. By processing technical data and detecting anomalies, the probability to detect the latest exploits and attacks against network infrastructures will be greatly increased. Proper data handling is a key-enabler to enhance the private and governmental organizations to react rapidly in a crisis situation to protect the indispensable services and systems.

In the proposed model, the operational level reports all relevant cyber incidents within an organization. The business management is responsible for the decisions whether the executive level should be notified about a current incident (see arrow-b). Stakeholders of the business level, for example the middle management, receive notifications about critical incidents, which could not be solved immediately by the technical team at the lowest level (arrow-a). However, even if an incident is solved at the lowest level; these are documented and reported monthly. The middle management notifies the Point of Contact in the national scope just about incidents that meet the reporting requirements. The tactical level, e.g. threat analysts of the NIRT, will analyze the received data from the organizations. One significant process is the analysis comparing the conclusion of the internal investigation with diverse external sources, such as OSINT data. From the hundreds of references to cyber vulnerabilities every day, the National Incident Response Team isolates potential vulnerabilities being exploited and warns potentially affected organizations. Threat analysts detect and identify anomalous activities at national level. PoCs receive weekly reports from the organizations in their domain in order to identify common failures within the sector and trends and notify the possibly affected organizations within the domain and even other domains. In this case arrow-i refers to the communication channels between PoC and all organizations in the related domain; arrow-c refers to one of the organizations within the domain. Identifying distinct sorts of attacks and incident patterns is only possible with a sufficient archive. It means that the databases need to be fed with information, i.e. the National Incident Response Team should receive incident reports periodically from the organizations. The comprehensive and growing database managed by the tactical partners is a key resource in both national and international cybersecurity. On one hand, the business level will be directly in contact with the strategic level (illustrated with arrow-f) regarding strategic intelligence and its activities, such as strategy implementation at the lower levels. On the other hand, they can be directly connected (in compliance with organization-internal policies) to the tactical level in the national

scope (illustrated with arrow-e) for example, if the organization needs prompt help or assistance in its current operating environment, related to the tactical intelligence. In the same manner, the executive level can communicate directly with the strategic level without the tactical level and the companies' levels among each other (arrow-g). A possible simplified information flow in the P3CSA framework is shown in Figure 1. The P3CSA framework is, due to its modularity, flexibly applicable regardless of the size of the organizations and state.

In case the PoCs find suspicious anomalies, they will collaborate with the affected partner organizations to examine the network activity associated directly with the potential cyber attack in more detail. After gaining additional information using internal and external information sources about the cyber incident (shown as arrow-m), the NIRT issues early warnings to the potential victims, provides information about the anomalies and offers counsel on the effects' mitigation or security measures in order to protect critical services (arrow-c and arrow-d). The National Incident Response Team summarizes the number of references to particular vulnerabilities being exploited weekly, such as a top ten incidents list and the possible technical solutions. The organizationally and personally identifiable information must be handled in a privacy-aware way by the NIRT. The report generated by the NIRT at tactical level could be shared with the strategic level (arrow-h) and with the relevant organization (see arrow-m), e.g. ENISA, at international level (arrow-k). The organizations at the European scope use the international information sources, such as national CERT reports and international reports (including from Europol, Interpol and ICSPA illustrated with arrow-l).

Contrary to national CERTs, the National Incident Response Team shares actively information obtained using the communication channels provided by the P3CSA framework with the partner organization according to the early warning and cyber situational awareness raising function of the P3CSA approach. The reports of the NIRT are sent using secure protocols. The access to the data collected by the National Incident Response Team is strictly limited. The gained cyber situation awareness allows the NIRT to generate a cross-domain trend analysis at national level. This data analysis provides for governmental and private organizations an accurate cyber situational picture in near real-time for making the right strategic decision.

5 FROM TECHNICAL DATA TO LIVE-DASHBOARD

The actors at tactical and strategic level in national scope have to take situation-dependent security-relevant decisions in order to deal with threats and

mitigate impacts of cyber attacks. Therefore, the P3CSA framework requires different approaches at each level of the cyber situation awareness gaining process. The different approaches include inter alia different data correlation processes and visualization methodology. One of the crucial differences is the timescale. Strategies require long-term planning and decision making with respect to the following objectives: reduce national vulnerability to cyber attacks, prevent attacks against critical infrastructures, have a current and accurate picture about the cyber situation nationwide, build strategic relationships among public and private participants, preserve economic prosperity and forecast future threats. By using behavioral models and predictive analysis (Yan & Zhang, 2013), the experts try to identify connections between advanced campaigns, attacker groups and their motivation. In contrast to the strategic scope, the tactical scope handles (near) real-time risks and challenges.

	Information Attributes	Processed Data (Input & Output)	Decisions & Activities
Strategic Scope	▪ Refers to the what and why ▪ Information for long-term planning and direction ▪ Processing time: months ▪ Internal and external data ▪ Information about the impact, opportunities ▪ Recognize emerging trends and patterns nationwide and international ▪ Response time: Future- oriented ▪ Context is the threat environment ▪ Strengthen digital intelligence ▪ Focus on planning and enhancing security level	▪ Threat Impact ▪ Cyber threat actors ▪ Attacker motivations & desired effects ▪ Discovered campaigns ▪ Monetary loss ▪ Espionage ▪ Guidelines ▪ Behavioral models ▪ Predictive analysis ▪ Reports about advanced & state-sponsored attacks ▪ Statistics about victims demographics	▪ Share & exchange information in international and national cooperation ▪ Cyber security awareness raising campaigns ▪ Adapt legal framework ▪ Practice for recruitment of cyber defense experts ▪ Researches on techniques and tactics ▪ Establish cooperation culture (private-public) ▪ Education initiatives ▪ Pooling & sharing defense capabilities ▪ Start investigations ▪ Strengthen offensive and defensive cyber security capabilities ▪ Prepare emergency plans

Table 2 – Strategic intelligence

They are using the companies' data to identify the techniques, tactics and procedures of incidents, and analyze the current situation of the essential infrastructures domain-wide. Table 2 and 3 show the main differences between the two levels. The challenging part after data processing and information extraction is how to provide proper assistance for the decision makers. In many fields, analysis of complex systems and activities benefit from visualization of data and analytical products (Healey, Hao & Hutchinson, 2014). As mentioned above, cyber situation awareness is gained at various levels. The collected technical data and reports represent a vast volume of information that need to be processed daily by cyber experts. The situation awareness based solely on low level technical data is clearly insufficient. Therefore, it needs to be completed with various data sources.

	Information Attributes	Processed Data (Input & Output)	Decisions & Activities
Tactical Scope	▪ Refers to the how ▪ Information for short-term goals ▪ Processing time: days ▪ Mainly internal data ▪ Information about the current condition, attack techniques, tools and practices ▪ Recognize emerging trends and patterns within the domains ▪ Response time: near real-time ▪ Context is the operating environment ▪ Strengthen digital resilience ▪ Focus on handling risks and counter attacks	▪ Overall risks in sectors ▪ Affected domains ▪ Reports about incidents, tactics ▪ Course of actions ▪ Vulnerabilities ▪ Indicators ▪ Target & victims ▪ Attack techniques ▪ Malwares & tools ▪ Vulnerability database	▪ Enrich threat intelligence ▪ Early warning of affected domains ▪ Develop and share good practices ▪ Create coherent reports for strategic decisions ▪ Implement top-level strategies ▪ Minimize damage and recover time ▪ Assist in patching vulnerabilities ▪ Technical discussion forum for organizations ▪ Improve offensive and defensive cyber security assets, tools, techniques and in-depth knowledge

Table 3 – Tactical intelligence

The use of big data analysis techniques is great help to governments (Kim, Trimi & Chung, 2014). This upcoming technology has the potential to improve threat detection, but harnessing the information and connect the relevant data in short-time is challenging. "The problem was not a lack of in-

formation, but, in fact, an overabundance of it (Barack Obama, 2010)"said Obama after an attempted terror attack. It demonstrates also that large corporations and government agencies are overwhelmed with information in general. Modern technology provides the opportunity to produce visualization of data and make it feasible to detect patterns and deviations that would not be discovered through pure manual observation. Visualization significantly simplifies and makes the information selection process in security intelligence more efficient. Big data visualization techniques present one option to deal with the continually changing threat landscape.

At the tactical level, live dashboards and detailed reports provide up-to-date information about the targeted organizations and domains or graphs sorted on the type of the attack in each domain provided by the National Incident Response Team, especially by the Point of Contacts. In the same manner, the visualization could focus on the top exploits, vulnerabilities, new techniques, attack methods or types etc. This makes the isolation of different attack vectors possible. The threat analysts at the tactical level identify attack methods being reported as part of incidents. The forecasting of trends is enabled by looking for increased reporting activity in different intervals, e.g. using count-based or time-based sliding windows (Golab & Ozsu, 2013). The time interval could be hours to days at tactical level and months at the strategic level. The analysis provides also strategically useful information for the National Security Council on cyber attack sources and vectors depending on the focus of the data processing. Threat analysts at the strategic level are looking for threat actors, their motivation and connections among the incidents. Their focus is on the threat impact regarding the national security. Live dashboards at strategic level visualize statistics about statewide cyber threats and potential future attack surfaces. The graphical representation of previous attacks on a timeline could help to discover periodic behavior at national level. The most challenging task of threat analysts is to find connections among the peaks of malicious activity crossing the domains and predict likely future attacks. The P3CSA framework can be also used to monitor new attack trends or campaigns at strategic level.

The possible outcomes after threat analysis and visualization processes are national vulnerability database, attack trends, statistics, summaries and screens with interactive dashboards. They can be treated by the National Incident Response Team (or optional by the CERT). Regarding one of the tactical objectives of cyber situational awareness, to sharing and exchange information in public-private cooperation, the reports and documents, such as vulnerability database, should be freely available to all partners, however within special trust circles depending on the sensitivity of information. The

P3CSA framework is structured to increase the speed and the quality of information flows and reporting about cyber incidents in national critical infrastructures. By producing the appropriate visualization of the reported technical data and information, the security analysts in the National Incident Response Team can detect patterns and identify attacks in order to mitigate those and present information to the National Security Council about the threat environment.

6 ILLUSTRATIVE APPLICATION CASE

The following scenario presents how P3CSA helps to deal with a wide-range botnet infection in the ICT domain. In the last years, botnets have evolved to sophisticated distributed systems compromising millions of computers with decentralized control. There is much interest to localize command and control (C&C) communication traffic by exploiting its special behavior. In recent years, a number of new techniques have been proposed to mine complex traffic data in organizations in order to support C&C detection (Kaspersky, 2015). This use case describes how the P3CSA framework could enhance CSA and cyber security nationwide.

The *IT department's* monitoring tools of the A-net Company, a large Internet service provider; identify anomalies in the company's traffic in the last days. They suspect to detect a botnet-infected host through command and control server communication at *the operational level*. After analyzing the packet content, the IT department detects a botnet malware which matches current signature databases. As local incident response in the organization scope, they trace back and analyze the infected hosts, which are found in the financial department. According to the incident guideline at the operational level, the IT department notifies *the middle management* about the incident, because the event covers several criteria of reporting obligation, such as presence of a malicious application and misuse of organizational resources. This accounting process is shown above in Figure 1 with arrow-a. The report includes a description of incident-related events; including the dates and times of the traffic anomalies in the organization's network traffic, lists of systems, accounts and components affected by the cyber attack. Furthermore, the report could include discretionary suspected actors and indicators, a list of the persons working on the mitigation of the incident, the amount of the time spent working on the incident recovery and the type and version of software running on the compromised components. After reporting the incident, the IT department is looking for further infected components in the organizational scope by analyzing current traffic for periodic behavior and by identifying connections between suspicious system behavior and potential attack vectors. A botnet relies on C&C communications channels traffic

between its members for the attack execution. C&C traffic occurs prior to any attack; hence, the detection of botnet's C&C traffic by the IT department enables the detection of members of the botnet before substantial harm happens.

After having discussions among the department heads about the bot-infection *at the business level*, they decide to inform the executive level according to the incident management guidelines. The incident covers several criteria of reporting obligation, such as misuse of organizational services causing possible immaterial damage, such as loss of reputation and reliability that can lead to loss of customers, or presence of spyware in the company. The botnet-malware could be programmed to download spyware which mines online browsing habits and exploits sensitive data including passwords, e-mail addresses and financial information of the A-net Company. In this case, the risk and the negative business impact of an incident increase enormously. At this time of the incident handling, the IT department does not know whether the current incident endangers key resources or services in the company and they are not sure about the number of the infected components. T*he Supervisory Board* and *top level management* realize the situation and qualify the middle management to solve the problem in strong cooperation with the *National Incident Response Team.*

Figure 3- Interactive tactical dashboard sample

This step is pictured with arrow-e in Figure 1. The information security officer informs the *Point of Contact* (PoC) of the ICT domain. The PoC uses the information channels to the relevant persons at tactical level, such as first responders or members of information security organizations, and OSINT information sources to gain more information about the recently reported botnet attacks. *At tactical level*, the threat analysts process the technical data and reports received from all organization focusing on attack techniques, tactics and exploited vulnerabilities. After data analysis they have a current cyber situational awareness about the conditions in the different organizations, emerging trends and patterns within the domains and about the used techniques and tools. This type of tactical intelligence could be provided via live dashboards, such as shown in Figure 3. Because the NIRT deals with near real-time challenges, the live dashboard in this case visualizes the current threat level of the ICT domain and the present incident reporting activity. Because of the dependencies among the domains, it shows the possibility that the incident will have a cascading effect in connected domains. To monitor the effectiveness of the mitigation measures, the number of reported incidents and detected effects are shown periodically. They realize that the number of the DDoS attacks using botnets is growing against ISPs lately nationwide. Furthermore, a C&C server was discovered, analyzed and put offline by a special police unit. The responsible law enforcement authority sends the list of IP addresses of the backtracked bot-members to the NIRTs in all national scopes. In the presented P3CSA model, every PoC receives periodically a list of IP address ranges currently used by each company in his domain.

Hence, they have the accurate cyber situational awareness at the tactical level, in order to easily identify the affected companies in their domains, even the compromised computers in the company. After the NIRT collected all relevant information about the specific incident in the A-net Company, it notifies all organizations employing the same or similar components which were compromised by the botnet-infection about identified IoCs and possible proactive measures. This early warning and mitigation process is posed by arrow-d the communication channel to the whole domain, and arrow-c is the channel to the affected organization.

Contrary to tactical intelligence, the intelligence of the National Incident Response Team prepares different type of data to support future-oriented decision making regarding the threat environment nationwide *at the strategic level*. The *National Security Council*, including state actors and major market stakeholders, deals with the impact and the reason of the cyber incidents. Based on the different objectives at this level, decision maker require

other type of data interpretation, like summaries about the most significant risks and challenges, reports about cross-border botnet campaigns, attacker groups and their motivations. This information intelligence is required to make complex decisions in accordance with the strategic mission and vision.

7 CONCLUSION AND OUTLOOK

The protection of the national critical infrastructures is essential to reliability and resilience of key resources, national security and economic prosperity. The aim of the P3CSA framework is to provide prompt information flows among the national stakeholders working in a wide-range cooperation, to provide an early warning system and enhanced cyber situational awareness for superior decision making at strategic and tactical level. Part of the challenge is the identification of suitable roles, information sharing processes, and proper handling and interpretation of vast volumes of information public and private organizations deal with on a daily basis. Sorting the security relevant information is a complex task for preparing both tactical and strategic intelligence. The P3CSA framework provides guidance for public and private organizations at both levels on incident identification, assessment and reporting. Moreover, it enables (near) real-time situational awareness of emerging information security events and incidents to support critical decisions. This is done by continuously analyzing numerous internal and external sources related to the topic. Threat intelligence analysts are working at tactical level to identify utilizable information with support from national cyber security experts. They reveal vulnerabilities that are present in national and international scope in order to find highly sensitive components and systems in the national CI based on known exploits and incident reports. The Point of Contact in each domain notifies the organizations about the potential threats on a regular basis. The multifaceted information sources allow analysts to isolate the specific target elements, for example by domains, and through the attributes of those targets, to better understand malware and attacker behavior.

Finally, the P3CSA framework is prepared to implement smooth information sharing processes based on reporting responsibilities in responding to advanced cyber threats. The framework covers the following functions: compile and analyze information security incident information, visualize the processed data, detect potential attack surface, early warning for private and public organizations about the current threats and vulnerabilities and consult national security agencies, such as NSC and NIRT, to develop and share

best practices and national preparedness. The effective implementation of the P3CSA structure requires powerful incident identification capabilities and reporting across all domains and organizations in order to protect national critical infrastructure used to deliver national security and essential services to the citizens. The P3CSA framework is designed for cooperation and efficient collaboration between all relevant public and private stakeholders, and building on existing initiatives to avoid duplicating efforts and promote cybersecurity. This presented concept reconsiders cyber security around five focal points; *contemporary multi-level data processing, proper communication channels, with visualization enhanced decision making, early warning and cross-border mitigation measures*. In this paper we presented a comprehensive model for cyber situational awareness which makes the mitigation of large-scale cyber attacks and the stopping of escalation into a national crisis for governments possible. Eventually, we illustrated a realistic use case for our approach.

Future work deals with the development and implementation of the framework and its legal requirements. Next, a P3CSA pilot will be deployed in Austria at the national level, demonstrating how the system facilitates the processes of cyber incident detection, analysis and mitigation nationwide within the interconnected critical infrastructures.

8 ACKNOWLEDGEMENTS

This work was partly funded by the Austrian security-research programme KIRAS (operated by the FFG) and by the Austrian Ministry for Transport, Innovation and Technology (BMVIT) in course of the projects “Cyber Incident Information Sharing” and “Cyber Incident Situational Awareness”.

9 REFERENCES

Arnborg, S., Brynielsson, J., Artman, H., & Walleniu, K. (2000, July). Information awareness in command and control: Precision, quality, utility. In Information Fusion, 2000. FUSION 2000. Proceedings of the Third International Conference on (Vol. 2, pp. THB1-25). IEEE.

Barack Obama, following an attempted terror attack on 25 December 2009

Barrett, S., & Konsynski, B. (1982). Inter-organization information sharing systems. MIS Quarterly, 93-105.

Beringer, D. B. & Hancock, P. A. (1989). Exploring situational awareness: A review and the effects of stress on rectilinear normalisation. In Proceed-

ings of the Fifth International Symposium on Aviation Psychology. Columbus: Ohio State University, Volume 2, 646-651.

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.

Endsley, M. R. (2000). Theoretical underpinnings of situation awareness: A critical review. Situation awareness analysis and measurement, 3-32.

ENISA, National cyber Security Strategies, Practical Guide on Development and Execution, December 2012

ENISA, Corporative models for effective Public Private Partnership: Good Practice Guide, 2011

ENISA, Four Years of Pan-European Public Private Cooperation, November 2014

ENISA, Protecting Industrial Control Systems. Recommendations for Europe and Member States, 2011

European Commission (2013), Proposal for a directive of the european parliament and of the council concerning measures to ensure a high common level of network and information security across the Union, EUR-Lex, Document 52013PC0048.

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

Golab, L., & Ozsu, M. T. (2003). Issues in Data Stream Management. SIGMOD Record, 32(2), 5.

Healey C. H., Hao L. & Hutchinson S. E.(2014) Visualizations and Analysts, In: Cyber Defense and Situational Awareness, New York: Springer, 145-150.

Jain, A. (2005). Cyber Crime: Cyber crime: issues and threats (Vol. 2). Gyan Publishing House.

Kaspersky, Statistics on Botnet-Assisted DDoS Attacks In Q1 2015, Retrieved August 15, 2015, from

https://securelist.com/blog/research/70071/statistics-on-botnet-assisted-ddos-attacks-in-q1-2015/

KIM, G. H., TRIMI, S., & CHUNG, J. H. (2014). Big-Data Applications in the Government Sector. Communications of the ACM, 57(3), 78-85.

Kott A., Buchler N., Schaefer K.E (2014) Kinetic and Cyber, In: Cyber Defense and Situational Awareness. C. Wang, & R. F. Erbacher (Eds.). Kott, A. (2014). New York: Springer.

Leopold, H., Bleier, T., & Skopik, F.(2015) Cyber Attack Information System. Springer-Verlag Berlin Heidelberg.

Lewis, T. G. (2014). Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. International Journal of Critical Infrastructures 6, 9(1-2), 3-31.

Malware Information Sharing Platform, http://www.misp-project.org/, Last accessed: 11.01.02016

Moffat, J. (2006). Mathematical modelling of information age conflict. Advances in Decision Sciences, 2006.

National Institute of Standards and Technology (NIST), & United States of America. (2014). Framework for Improving Critical Infrastructure Cybersecurity.

North Atlantic Treaty Organization (2013), The history of cyber attacks – a timeline, Retrieved August 12, 2015, from http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

North Atlantic Treaty Organization (2014), Wales Summit Declaration, 73.

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

Skopik, F., Ma, Z., Smith, P., & Bleier, T. (2012). Designing a cyber attack information system for national situational awareness. In: Future Security Springer Berlin Heidelberg. Volume 2, 646-651.

Tadda, G. P., & Salerno, J. S. (2010). Overview of Cyber Situation Awareness. Cyber situational awareness, 46(1), 15-35.

Yan, X., & Zhang, J. Early Detection of Cyber Security Threats using Structured Behavior Modeling. ACM Transactions on Information and System Security, 5.

BIOGRAPHICAL NOTES

Timea is an engineer student in IT Security, holding a Bachelor Degree in Security and Defense Studies. Her current research field includes national cyber security and cyber situational awareness at the Austrian Institute of Technology.

Florian is Senior Scientist and Senior Project Manager in the ICT Security Research Team at the Austrian Institute of Technology, where he coordinates numerous research national projects on national cyber security.

Reference to this paper should be made as follows: Pahi, T. & Skopik, F. (2016). A Public-Private-Partnership Model for National Cyber Situational Awareness. *International Journal on Cyber Situational Awareness*, Vol. 1, No. 1, pp31-53.