Common Cyber Situational Awareness: An Important Part of Modern Public Protection and Disaster Relief

JUSSI SIMOLA AND JYRI RAJAMÄKI
Research, Design and Innovations
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 Espoo
FINLAND
http://www.laurea.fi

Abstract: - European Public Protection and Disaster Relief (PPDR) services such as law enforcement, firefighting, emergency medical and disaster recovery services have recognized that the lack of interoperability of technical systems limit the cooperation between authorities. Also Finnish PPDR authorities and politicians have recognized the importance of a common situational awareness in preparation for the future. When the purpose is to work effectively towards a common goal or solve various challenges, accurate and reliable information as a basis for situational awareness is needed. Cyber situational awareness is the part of situational awareness which concerns the "cyber" environment. Such situational awareness can be reached, e.g., by the use of data from IT sensors that can be fed to a data fusion process or be interpreted directly by the decision-maker. This study was conducted on the ground by visiting situation and command centers located in the Turku area in Southwestern Finland. The Southwestern Finland Police department, the Southwest Finland Emergency Services, the Hospital District of Southwest Finland and the Finnish Border Guard in Turku have their own situation/ command centers. The main purpose of the study was to find out local level factors which affect to utilization of situational awareness system. The aim was also to research the level of preparedness in regional administration including local PPDR departments. The main results can be summarized so that the operational field work of the PPDR authorities should be more standardized so that implementing new technology would be profitable. The lack of cooperation between situation centers prevent to create common situational awareness. In the future, cyber situational awareness can play an important role in emergency and crisis management because the scene of PPDR will increasingly often be a cyber-physical system.

Key-words: - Situational awareness, Public protection, Disaster relief, Preparedness, Cyber security

1 Introduction

European Public Protection and Disaster Relief (PPDR) services such as law enforcement, firefighting, emergency medical and disaster recovery services have recognized that the lack of interoperability of technical systems limit the cooperation between the PPDR authorities. This case study belongs to AIRBEAM FP7 project, whose major objective is to propose a situation awareness toolbox for the management of crisis over wide area taking benefit of an optimized set of aerial (unmanned) platforms, including satellites. The AIRBEAM project is a good example for creating a collective information sharing mechanism between PPDR authorities in national and cross-border operation´s.

In Finland, national projects such as ERICA, KEJO and TUVE are under development. The KEJO common field command ICT-system, ERICA Emergency Response Centre ICT-reform and TUVE information Security Network projects are all based on need to develop interoperability between the PPDR authorities. These projects indicate the importance of designing collective information sharing.

The main purpose of this case study is to find out local level factors which affect to utilization of situational awareness (SA) system. The aim is to research the level of preparedness in regional administration including local PPDR departments. A research topic is the level of preparedness to implement new technology in the local PPDR administrations. Another topic is to find out

ISBN: 978-1-61804-365-8

different agencies' level of preparedness of applying new technologies, especially in the cyber domain.

This paper has five sections. After this introduction, the second section briefly introduces the conceptual foundation of the case study. The third section describes research method and process. The fourth section presents the case study findings, and the last, fifth section includes discussion and conclusions.

2 Conceptual Framework

2.1 Situational Awareness

According to Endsley [1], a general definition of situational awareness 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 near future". From a technical viewpoint, situational awareness comes down to compiling, processing and fusing data, and such data processing includes the need to be able to assess data fragments as well as fused information and provide a rational estimate of its information quality [2]. The cognitive side of situational awareness concerns the human capacity of being able to comprehend the technical implications and draw conclusions in order to come up with informed decisions [2].

2.1.1 Cyber Situational Awareness

According to Franke and Brynielsson [2], cyber situational awareness is a subset of situational awareness, i.e., cyber situational awareness is the part of situational awareness which concerns the "cyber" environment. Such situational awareness can be reached, for example, by the use of data from IT sensors (intrusion detection systems, etc.) that can be fed to a data fusion process or be interpreted directly by the decision-maker [2].

2.2 Public Protection and Disaster Relief

The term public protection and disaster relief (PPDR) is used to describe critical public services that have been created to provide primary law enforcement, firefighting, emergency medical services and disaster recovery services for the citizens of the political sub-division of each country. These individuals help to ensure the protection and preservation of life and property. Public safety organizations are responsible for the prevention of and protection from events that could endanger the safety of the general public [3]. Such events could be natural or man-made. The main public safety functions include law enforcement, emergency medical services, border security, protection of the environment, firefighting, search and rescue (SAR) and crisis management [3].

2.2.1 Structural Changes in Finnish PPDR

The structural changes within public sector, such as the regional administration reform, the Emergency Response Centre (ERC) reform and so called social welfare and health care reform have influenced one way or another public sector employee´s work processes over the past ten years. In addition, technological development has occurred rapidly. ERC Centre) reform has affected to the entire working environment of Finnish PPDR authorities [4]. Changes in PPDR organization´s due to legislation have developed a need to create special operational working methods [5]. In addition, various information system projects such as KEJO and ERICA will change people's cooperation and working environments.

2.3 Situational Awareness at National Level

Government situation center ensure that the state leaders and central government authorities are kept informed continuously as illustrated in Figure 1. In Finland, the government situation center was set up in 2007, and it has the duty to alert the government, permanent secretaries and heads of preparedness and to call them to councils, meetings and negotiations at exceptional times required by a disruption or a crisis. The ministries have the duty to submit the situational picture for their entire administrative branch to the government situation center and notify the center of any security incidents in their field of activity. In urgent situations, the government situation center also receives incident reports of security incidents directly from the authorities. In addition, the government situation center follows public sources and receives situational awareness information in its role as the national focal point for certain institutions of the European Union and other international organizations.

ISBN: 978-1-61804-365-8

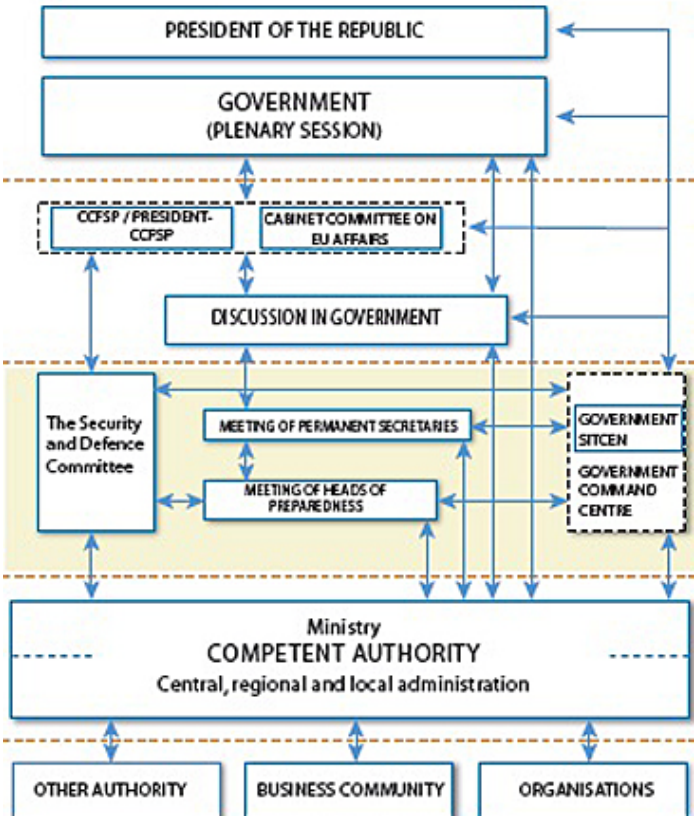

Fig.1 Management of disturbances in Finland

2.3.1 Cyber Situational Awareness at National Level

The National Cyber Security Centre Finland (NCSC-FI) operates within the Finnish Communications Regulatory Authority (FICORA) and offers an increasingly diverse array of information and cyber security services. In its role as a statutory supervisory and steering authority with a responsibility for information security tasks, NCSC-FI gathers information. FICORA's other operations yield more information governed by legislation on events relating to incidents, deviations and disturbance situations. The information gained from nationally or internationally detected information security incidents, deviations and threats (incident response function, CERT) is combined with the information gained from inspections of information systems and telecommunications arrangements (information assurance function, NCSA) and the information received in the role as a supervisory and steering authority. Combined, this information is used to produce NCSC-FI's combined cyber security situational picture, as illustrated in Figure 2 [6].

HAVARO is an alert and detection system FICORA has created in partnership with the National Emergency Supply Agency in 2012. For every Finnish organization, it is optional to join the HAVARO system, but joining brings many significant benefits. The information on situation awareness provided by the system increases understanding about the organization's own and general state of information security. The system produces information which makes it also possible

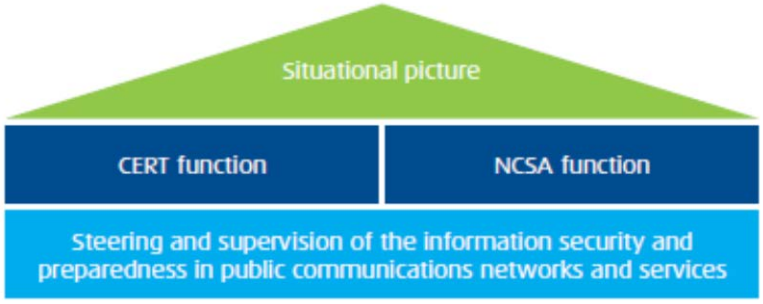

Fig. 2 Producing of Finnish National Cyber Security Situational Picture [6]

ISBN: 978-1-61804-365-8

to alert other players about a detected threat and develop better means of detection. Clients can determine what sort of data the system processes and the ownership of the data remains with the company itself, in its own devices. HAVARO does not compete with commercial players or replace any other information security solutions. The participating organization are responsible for the costs of equipment needed for their own network.

The system monitors information security incidents only, it is incapable of monitoring the communication of individual users. The handling of data in HAVARO is regulated by legislation and in agreements between users. Although the system has been released publicly, the list of players who have joined are kept secret.

The first experiences from the system have been positive and have proved that the traditional controls are not always sufficient in the prevention and detection of malware. Between January and August 2015, the HAVARO system made a total of 1,800 red observations. Red observations indicate that the system has observed harmful traffic, which points to a likely information security breach in the organization. Most observations concern utilization attempts made using mass distribution platforms, utilizing vulnerabilities in web browser add-ons (Adobe Flash in particular). A malware mass distribution platform is a program code which is run on a network server and utilized by criminals, the purpose of which is to install specific malware on the user's computer.

2.4 Cyber-Physical Systems

Modern infrastructures include not only physical components, but also hardware and software. These integrated systems are examples of cyber-physical systems (CPS) that integrate computing and communication capabilities with monitoring and control of entities in the physical world. Figure 3 presents a CPS that consists of two physical layers (platform layer and human layer) and a cyber layer between them. The current trend is that the cyber layer is expanding.

Many CPS applications are safety-critical which means that their failure can cause irreparable harm to the physical system under control and to the people who depend on it. In particular, the protection of our critical infrastructures that rely on CPS, such as the electric power transmission and distribution, industrial control systems, oil and natural gas systems, water and waste-water treatment plants, healthcare devices, and transportation networks play a fundamental and large-scale role in our society and their disruption can have a significant impact to individuals, and nations at large. Increasingly many CPS are operated under automated controls and a sophisticated cyber-attack can exploit weaknesses to its advantage.

3 Research Method and Process

PPDR services are tasked with the challenge of providing the first response in life critical circumstances. The ability to create right situation awareness and a reliable communication with each other are the most important things at the disposal of the PPDR services. This case study is carried out by the guidance of Yin [8]. Altogether four regional command/situation centers were selected to be researched in an empirical study: Southwestern Finland Police department, Southwest Finland Emergency Services, Hospital District of Southwest Finland and The Finnish Border Guards in Turku. The Finnish Border Guards have their own main situational/command center in Turku and it´s called for Maritime Rescue Coordination Centre. The situation center of the Southwestern Finland Police department and the command centre of the The

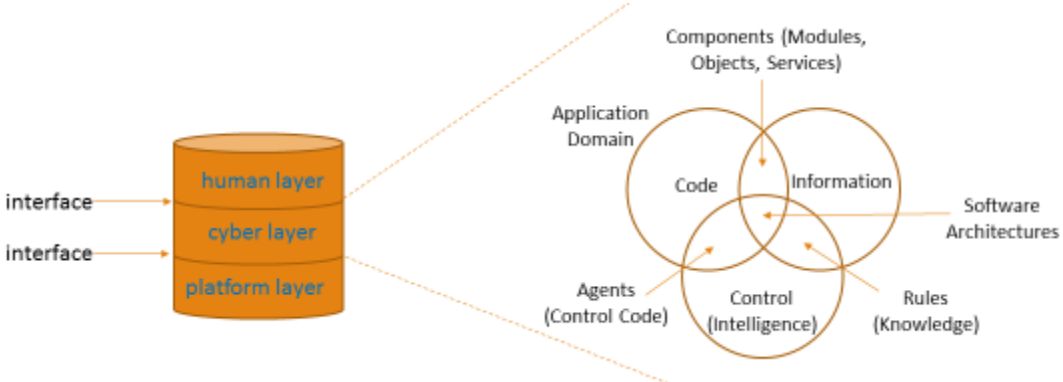

Fig. 3. Layers of Cyber-Physical Systems (modified from [7])

ISBN: 978-1-61804-365-8

Finnish Border Guard are managed by the state. Southwest Finland Emergency Services and Hospital District of Southwest Finland act under the municipality. The field commanders of the situational centers were interviewed in their own work environment.

The case study´s empirical ethnographic research approach is due to the fact that the researcher had to study more deeply the culture of the situational centers and the actual working environment of employees working in the field, because there were differences in literature -references regarding public safety organizations information systems.

The materials collected for this case study are based on observations, interviews, scientific publications, collected articles and literary material. Participant observation makes it possible to get close to the actors. It illustrates the identities of actors' diversity [9], observation is made on the field and the results are recorded and saved as notes. One prominent data collecting method used was focus interviews. Eight emergency dispatch workers were interviewed. Questions were sent to participants in advance. In addition four public safety specialist were interviewed. The focus interviewees were designated based on their expertise on their specialist role. Semi-structured interviews had a flexible and fluid structure. The interviewees operates or have been operated in the public safety organizations. Observing emergency dispatch workers work in their real work environment give the better way to understand work procedures. The interviews were recorded and analyzed with qualitative content analysis methods [10].

4 Case Study Findings

One way of gaining increased cyber situational awareness is to exchange information with others. However, regional situational centers use different systems and therefore the same system can be used in two situational centers without cooperation with each other. None of the regional situational centre has direct contact with the Government situational center, but the connections are handled through intermediaries. For rapidly evolving situations access to the government situational centers', data connection should be arranged to the essential situational centers.

At present, Finnish PPDR authorities do not have common command and control center with regular personnel. The lack of cooperation between situational centers prevent to create common situational awareness and picture. Starting cooperation at the scene of the accident, as Figure 4 illustrates, is not enough during a major accident in a modern cyber-physical system. However, a reliable and correct common situational picture should be created before arriving to scene of the accident. If the scene is a modern CPS, also a cyber situational picture is needed.

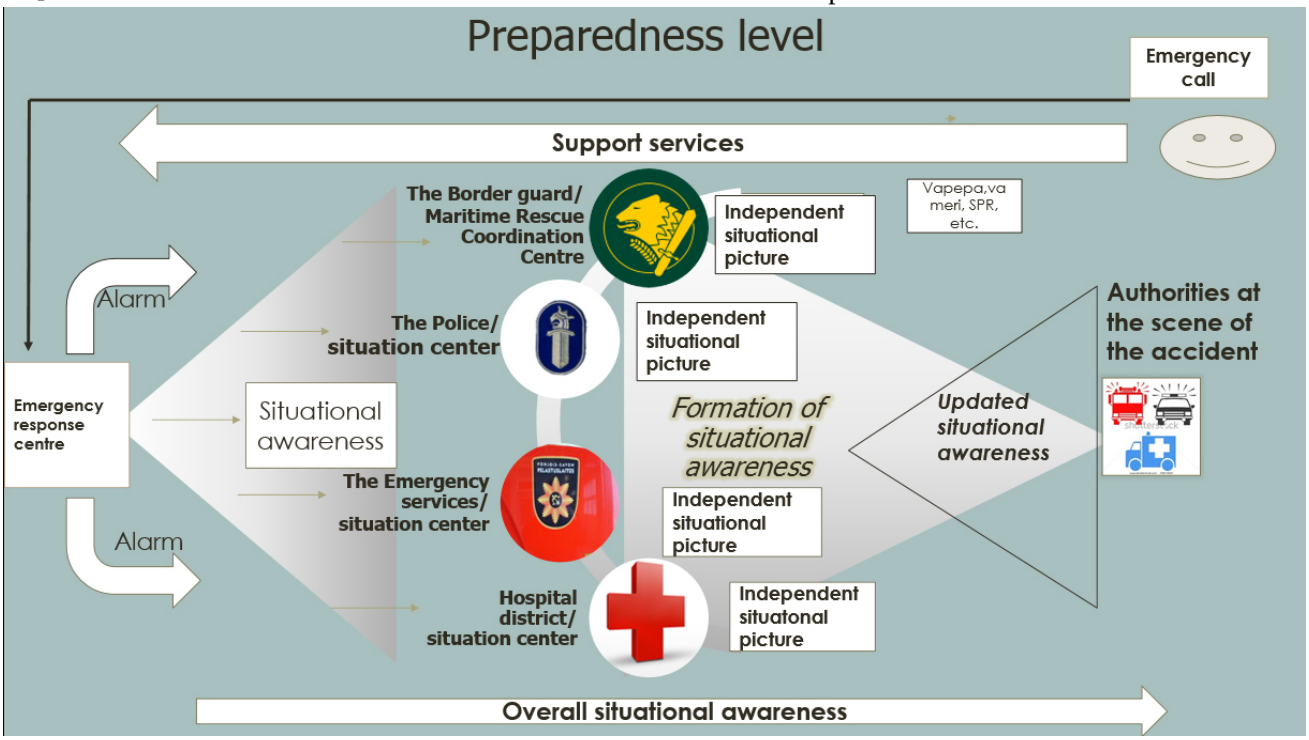

Fig. 4 Formation of situational awareness [11]

ISBN: 978-1-61804-365-8

Lack of preparedness plans affect to cooperation within PPDR authorities at the field of a major accident. Reforms in public sector and changes in PPDR organizations with legislative amendment require changes in preparedness plans. Unclear tasks descriptions in a case of a major accident prevent allocating resources. Clear instructions cards are only a part of the preparedness. In case of a major accident, there should be a common command center having liaison officers in the process of creating a common situational picture. At present managerial personnel get together at each other's command centers depending on the type of the accident.

Today, too many hierarchy levels in and between organizations exist. Therefore, settling new technology faces challenges. It must be understood that individuals, groups and work environments form an entity. If there are too many hierarchy levels, information of situation does not flow or, at least, it is slow [12].

5 Discussion and Conclusions

In a case of a major accident, organization´s own tasks help them to concentrate on their own field of PPDR operation. But on the other hand, their own tasks prevent them from seeing what other authorities are doing. No one of the situational centers of this case study has a possibility to direct communication connection to the Government situation center. This prevent information flow from local level to higher level and also prevents to get higher level of preparedness. Instead of separate situation centers, there should be a common situation center where different state and municipality PPDR actors and decision-makers could get together when a major accident occurs.

Often, urban built infrastructures represent a critical node within the intertwined networks of an urban area. Substantial part of our CPS today relies on complex systems of communication networks. There is just as much of a need to take into account the equally vulnerable built infrastructures of modern urban areas. Many of these, be it transport systems of different kinds, large school/university campus areas, sports arenas or shopping malls have already been evaluated regarding their resilience against major terrorist attacks, school-shootings or disruptions of other natures. However, shortages in the emergency preparedness are common, e.g. bit money has been spent to upgrade security; training

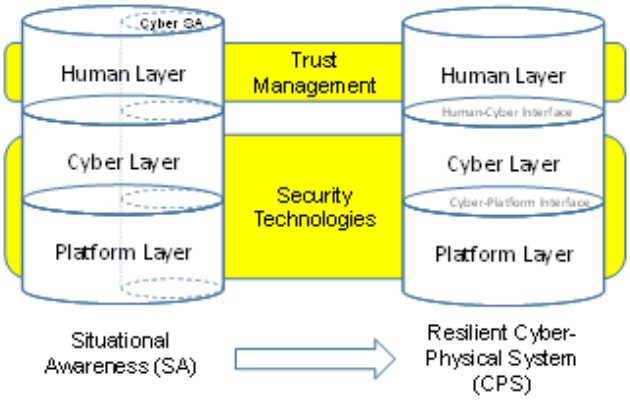

Figure 5. Situational awareness as a prerequisite of the resilience of a cyber-physical system

of security staff on preventing and responding to attacks remain inadequate; hiring standards for prospective security officers have not changed substantially; and risk assessments are rare and emergency management plans are developed without the input or participation of first responders [13]. Making large-scale built infrastructure in urban areas more resilient against attacks and disruptions of different kinds is an endeavor that requires multifaceted and multifunctional cooperation between various players of the security sector [13], [14]. Alert mechanisms should be multimodal (not just on operator screens), and the control system functions and communications that generate them must be designed in a manner that they cannot be bypassed by cyber-attacks. A common cyber situational awareness is needed for both operating CPS and for emergency and crisis management. Some national strategies already note the connection between cyber situational awareness and emergency management, for example the Canadian: "Cyber attacks that disrupt emergency response and public health systems would put lives in danger" [15].

According to Franke and Brynielsson [2], cyber SA cannot be treated in isolation, but it is intertwined with and a part of the overall SA. Cyber SA indeed concerns awareness regarding cyber issues but these need to be combined with other information to obtain full understanding regarding the situation. Figure 5 illustrates that a situational awareness (SA) system itself is a CPS, cyber SA being a subset of it. Situational awareness is a prerequisite for CPS to be resilient.

ISBN: 978-1-61804-365-8

References:

[1] Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. Human Factors Society 32nd Annual Meeting, 97-101.

[2] Franke, U., & Brynielsson, J. (2014). Cyber situational awareness: A systematic review of the literature. *Computers & Security*, 46, 18-31. doi:10.1016/j.cose.2014.06.008

[3] Baldini, G. (2010). *Report of the workshop on "Interoperable communications for safety and security"*. Publications Office of the European Union.

[4] Hanni, J. (2013). The quality and amount of information for emergency situations management (Master's Thesis. Oulu University of Applied Sciences).

[5] Aine, A., Nurmi, V., Ossa, J., Penttilä, T., Salmi, I., & Virtanen, V. (2011). *Moderni kriisilainsäädäntö.* Helsinki: WSOYpro.

[6] Finnish Communications Regulatory Authority. (2014). National cyber security centre: Action plan 2014-2016

[7] Hevner, A., & Chatterjee, S. (2010). *Design science research in information systems*. Springer.

[8] Yin, R. K. (2009). *Case study research design and methods* (4th ed.). Thousand Oaks: Sage Publications.

[9] Viinamäki, L., & Saari, E. (2007). *Polkuja soveltavaan yhteiskuntatieteelliseen tutkimukseen.* Helsinki: Kustannusosakeyhtiö Tammi.

[10] Brannen, J. (2004). Working qualitatively and quantitatively. In C. Seale, G. Gobo, J. F. Gubrium & D. Silverman (Eds.), *Qualitative research Practice* (pp. 312-326). London: Sage Publications.

[11] Simola, J. (2015) The effects and factors of the real-time video in PPDR services (Master's Thesis. Laurea University of Applied Sciences).

[12] Rajamäki, J., & Viitanen, J. (2014). Near border information exchange procedures for law enforcement authorities. *International Journal of Systems Applications, Engineering & Development*, 8, 2015-2020.

[13] Davis, R., Ortiz, C., Rowe, R., Broz, J., Rigakos, G., & Collins, P. (2006). *An assessment of the preparedness of large retail malls to prevent and respond to terrorist attack*. (No. 216641). Washington: The U.S. Department of Justice.

[14] Kreus, J., Pelkonen, N., Ranta, T., Turunen, T., Viitanen, J., & Vuoripuro, J. (2010). *Korkeakoulun turvallisuuskäsikirja – vakavien henkilöriskien hallinta*. Helsinki: Edita Prima Oy.

[15] Government of Canada. (2010). *Canada's cyber security strategy: For a stronger and more prosperous canada* (No. PS4-102/2010E-PDF).