To cite this Article: Simola, J. & Rajamäki, J. (2017) Hybrid Emergency Response Model: Improving Cyber Situational Awareness. In Mark Scanlon & Nhien-An Le-Khac (Eds.) Proceedings of the 16th European Conference on Cyber Warfare and Security, University College, Dublin, Ireland, 29-30 June, 2017, 442-451.

Laurea University of Applied Sciences
Ratatie 22, 01300 Vantaa, Finland
Phone +358 (0)9 8868 7150
Fax +358 (0)9 8868 7200
firstname.surname@laurea.fi
www.laurea.fi
Business ID 1046216-1
Domicile Vantaa

Hybrid Emergency Response Model: Improving Cyber Situational Awareness

Jussi Simola and Jyri Rajamäki
Laurea University of Applied Sciences, Research, Design and Innovations, Finland
simolajussi@gmail.com
jyrirajamaki@laurea.fi

Abstract: Cyber threats have increased in spite of formal integration in Europe and the world. Therefore, authorities need to respond to growing challenges. As major terror attacks, hybrid warfare and major accidents e.g. in USA, Belgium, Ukraine and France have shown preparation for different kind of threats is challenging. Finnish Public Protection and Disaster Relief (PPDR) authorities and politicians have recognized the importance of a common situational awareness in preparation for the future. Cyber situational awareness is a part of situational awareness which concerns the "cyber" environment. Such situational awareness can be reached, e.g., by using 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 in four situation and command centers of PPDR services located in Southwestern Finland. The main purpose of the study was to create smart hybrid emergency response -model based on intelligent emergency management system and find out local and state level factors which affect to utilization of 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 unclear allocation of responsibilities in government departments prevent authorities from fighting together against cyber and physical threats. Responsibilities for developing cybersecurity has also been shared for too many factors. The operational field work of the PPDR authorities should be more standardized and management should be more centralized. Unclear emergency procedures between authorities and lack of co-operation between situation centers with limited data transmission capacity prevent to create common situational awareness. In the future, a common cyber situational awareness is needed for both operating cyber physical system and for emergency and crisis management. PPDR services and decision makers In Finland need a common multifunctional hybrid emergency response-model to be able to prevent various threats until bureaucratic and organizational barriers have been removed. Need for common cyber ecosystem to control crossboarding threats is growing.

Keywords: cyber security, hybrid emergency response, PPDR, situational awareness, early warnings

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. *Also The military (MIL) and critical infrastructure protection (CIP) faces similar challenges.*

As major terror attacks, hybrid warfare and major accidents e.g. in USA, Belgium, Ukraine and France have shown preparation for different kind of threats is challenging. Recent major accidents have indicated that lack of human resources affects to disaster recovery.

The main purpose of the study was to create smart hybrid emergency response -model based on intelligent emergency management system and find out local and state level factors which affect to utilization of system. The aim was also to research the level of preparedness in regional administration including local PPDR departments.

Another topic is to find out different agencies' level of preparedness of applying new technologies, especially in the cyber domain.

2. Theoretical framework

2.1 Situational awareness

According to Endsley (Endsley 1988), 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 (Franke,

Brynielsson 2014). 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 (Franke, Brynielsson 2014). Referred to Endsley (1988, 2015), humans are not as good at processing large volumes of data, quickly and consistently, nor of sustaining attention for long periods of time. Figure 1 illustrates the level of autonomy increases as the capability of the system increases for performing various components of any given functions. Flexible autonomy should provide smooth, simple, seamless transition of functions between human and the system (Endsley 2015).

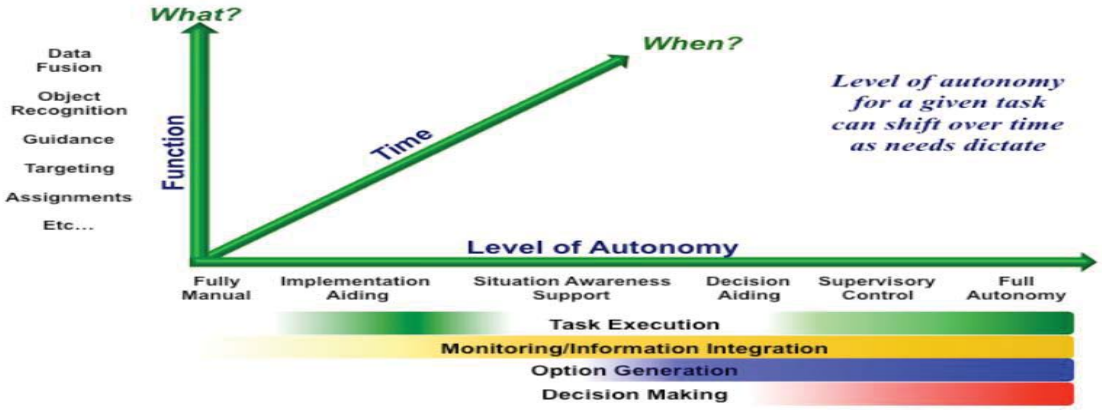

Figure 1: Level of autonomy

2.1.1 Cyber situational awareness

According to Franke and Brynielsson (Franke, Brynielsson 2014), 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 (Franke, Brynielsson 2014).

2.2 Structural and organizational changes in Finnish PPDR

The term public protection and disaster relief (PPDR) or Public Safety organizations are responsible for the prevention of and protection from events that could endanger the safety of the general public (Baldini 2010). According to Baldini (Baldini 2010), 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.

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 public sector employee´s work processes over the past ten years. In addition, technological development has occurred rapidly (Hanni 2013). Changes in PPDR organization´s due to legislation have developed a need to create special operational working methods (Aine et al. 2011). The Finnish Security Intelligence Service (Supo) is an operational security authority engaged in close cooperation with international security and intelligence services. Supo moved directly under the Ministry of the Interior in 2016. Earlier the Finnish Secure Intelligence Service operated under the National Police Board (The Finnish Security Intelligence Service 2015).

2.3 Command and control system

A Command Center is any place that is used to provide centralized command for some purpose. An Incident Command Center would be located at or near an incident to provide localized on-scene command and support of the Incident Commander. Mobile Command Centers may be used to enhance emergency preparedness and back up fixed command centers. Command Centers may include Emergency Operations Centers (EOC) or Transportation Management Centers (TMC) as well.

Supervisory Control and Data Acquisition (SCADA) systems are basically Process Control Systems (PCS) that are used for monitoring, gathering, and analyzing real-time environmental data from a simple office building or a

complex nuclear power plant. PCSs are designed to automate electronic systems based on a predetermined set of conditions, such as traffic control or power grid management (Gervasi 2010).

2.3.1 Distributed systems intercommunication protocol—DSiP

DSiP forms multiple simultaneous communication channels between the remote end and the control room: if one communication channel is down, other channels will continue operating. DSiP makes communication reliable and unbreakable by using various physical communication methods in parallel. Applications, equipment and devices can communicate over a single unbreakable data channel. Satellite, TETRA, 2G/3G/4G, VHF-radios and other technologies can be used simultaneously. DSiP is simultaneously a protocol-level and routing-level traffic engineering software solution for intelligently handling data routing, using all kinds of physical media, including IP and non-IP communication (Ahokas et al. 2010).

2.4 Critical infrastructure protection

Critical Information Infrastructure means any physical or virtual information system that controls, process, transmits, receives or stores electronic information in any form including data, voice or video that is vital to the functioning of critical infrastructure. Critical infrastructure (CI) includes energy production, transmission and distribution networks, ICT systems, networks and services (including mass communication), financial services, transport and logistics, water supply, construction and maintenance of infrastructure, waste management in special circumstances. That smart network will integrate information and communication technologies with the power-delivery infrastructure (Ministry of the Interior 2016, Ahokas et al. 2010).

2.5 Emergency communications

European authorities communicate with each other in Virve -network. There is a need to create new trusted network with wide bandwidth. The transmission capacity is often limited in an overload situation.

Enhancing common operational picture has been noticed also in The United States. Need to transmit live video but also different kind of sensor data from scene of the accident has become main areas for development of information systems. The 9-1-1 Center of the future with FirstNet systems will receive incoming Data calls from the machines and sensor systems including automatic crash notification (ACN), break-in alarms, and body health monitors. Use of both systems ensures multi-media capabilities throughout the entire call process (National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO) 2016, National Public Safety Telecommunications Council 2015).

2.6 A smart grid system and internet of thinks

Internet of Things connects systems, sensors and actuator instruments to the broader internet. IOT allows the things to communicate, exchange control data and other necessary information while executing applications towards machine goal (Electrical Technology 2016).

Cybersecurity risks should be addressed as organizations implement and maintain their smart grid systems (National Institute of Standards and Technology 2014). A smart grid system may consist of information technology which is a discrete system of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. A smart grid system may also consist of operational technologies (OT) or industrial control systems (ICS) like SCADA systems, distributed control systems (DCS), and other control system configurations (National Institute of Standards and Technology 2014, CHONG, KUMAR 2003).

Industrial Internet of Things (IIOT) collects data from connected devices (i.e., smart connected devices and machines) in the field or plant and then processes this data using sophisticated software and networking tools. The entire IIOT requires a collection of hardware, software, communications and networking technologies (Electrical Technology 2016).

2.6.1 Integration of safety functions

Decision Support Engine (DSE) is a facilitator intended to help authorities and other decision makers that compiles key information from raw data using system rules and knowledge. It captures data from different

sensors e.g. surveillance cameras (Ahmed et al. 2012). Face detection camera (FDC) is also one kind of decision support engine itself. Data processing for event detection follows next in order to identify events in current surveillance context (NEC Corporation). To understand the current surveillance state depends on the output of combined event detection units.

2.7 Situational awareness at national level

The Ministry of Finance of Finland is responsible for the steering and development of the state's information security (Ministry of defence 2010). Government situation centre ensure that the state leaders and central government authorities are kept informed continuously as illustrated in Figure 2. In Finland, the Government situation centre 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.

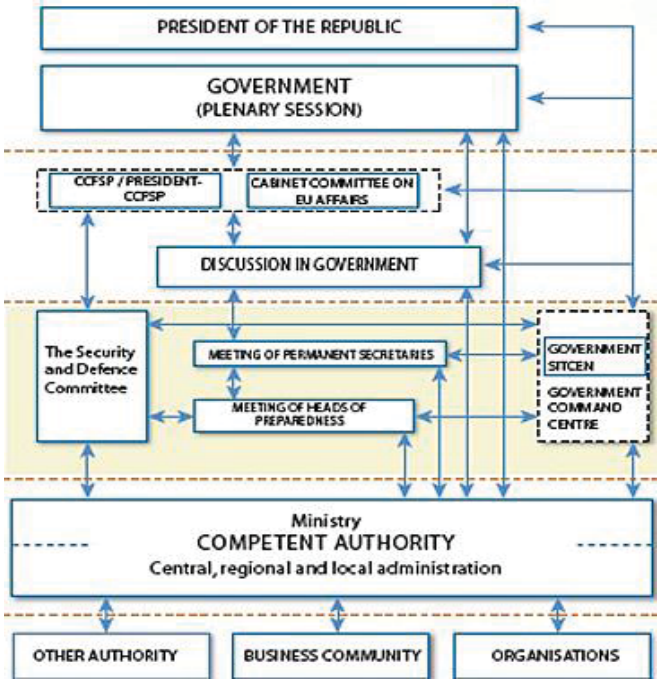

Figure 2: Management of disturbances in Finland

2.8 Cyber situational awareness at national level

Ministry of Transport and Communications is responsible for safeguarding the functioning of electronic ICT systems. The Ministry of Finance is responsible for safeguarding the state administration's IT functions, information security, and the service systems common to the central government (Secretariat of the Security Committee 2013). The Security Committee coordinates cyber security preparedness, monitors the implementation of the Cyber Security Strategy and issues recommendations on its further development. (Secretariat of the Security Committee 2013). The Finnish Communications Regulatory Authority (FICORA) working under steering control the Ministry of Transport and Communications. 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 (Finnish Communications Regulatory Authority 2014). 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 3. (Finnish Communications Regulatory Authority 2014).

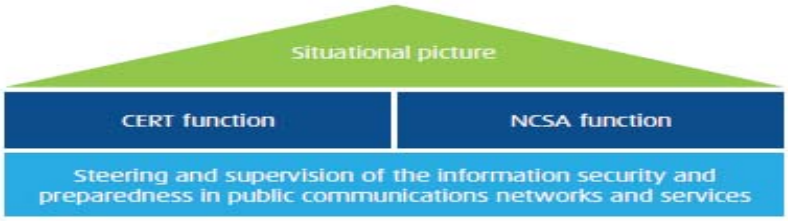

Figure 3: Producing of Finnish national cyber security situational picture (Finnish Communications Regulatory Authority 2014)

2.8.1 Alert and detection system HAVARO

HAVARO is an alert and detection system which FICORA has created in partnership with the National Emergency Supply Agency (NESA) in 2012. The National Emergency Supply Agency (NESA) is a public organization working under steering control the Ministry of Employment and the Economy. NESA is responsible for planning and measures related to developing and maintaining security of supply.

The system monitors information security incidents only, it is incapable of monitoring the communication of individual users. Red observations indicate that the system has observed harmful traffic, which points to a likely information security breach in the organization.

2.8.2 Cyber-Physical Systems

The term cyber-physical systems (CPS) was coined by Helen Gill at the National Science Foundation in the U.S. to refer to the integration of computation with physical processes. In CPS, embedded computers and networks monitor and control the physical processes. Feedback loops physical processes affect computations and vice versa. CPS are enabling next generation of "smart systems" like advanced robotics, computer-controlled processes and real-time integrated systems (Lee, Seshia 2015).

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 4. 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.

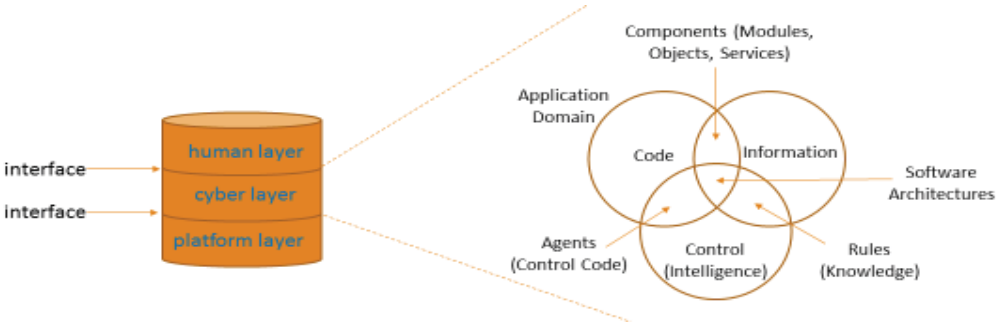

Figure 4: Layers of cyber-physical systems modified from (Hevner, Chatterjee 2010)

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.

2.8.3 Critical infrastructure and cyber threats

Cyber threats include denial of service (DoS), unauthorized vulnerability probes, botnet command and control, data exfiltration, data destruction or even physical destruction via alternation of critical software/data. These threats can be initiated and maintained by a mixture of malware, social engineering, or highly sophisticated advanced persistent threats (APTs) that are targeted and continue for long periods of time. Channel jamming is one of the most efficient ways to launch physical-layer DoS attacks, especially for wireless communications (National Institute of Standards and Technology 2014).

3. Research background, method, process

This case study is carried out by the guidance of Yin (2014). Case study illustrates the attempt to produce an profound and detailed information about the object under research.

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 situation/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 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 situation centers were interviewed in their own work environment.

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 (Viinamäki, Saari 2007), observation is made on the field and the results are recorded and saved as notes. One prominent data collecting method used was focus interviews (Brannen 2004). Eight emergency dispatch workers were interviewed.

4. Case study findings

Regional situation centers use different systems and therefore the same system can be used in two situation centers without cooperation with each other. None of the regional situation center has direct contact with the Government situation centre, but the connections are handled through intermediaries. For rapidly evolving situations access to the Government situation centres', data connection should be arranged to the essential situation centers.

As recent major accidents have indicated that lack of human resources affects to disaster recovery. PPDR-actors cannot start operations, if there is a human factor preventing the flow of information. Preventing post-accident after the disaster may be delayed. Recent violent acts at local and state level (from local to national level) have shown this to be reality. The communication activities of Intermediaries have been one of the major problems in recent major accidents. In Brussels, Belgium federal police request to close the metro and the main railway stations did not reach the responsible chief of the railway police because phone networks were down. A request to close railway station was sent to the responsible authority´s personal e-mail instead of work mail. Responsible authority did not see the message until after the attacks (McLaughlin et al. 2016). The November 2015 terror attacks also did not cause a total closure of the Paris Metro or other public arenas (The Guardian 2016, Steafel et al.). Therefore workable cyber environment with automated functions must be seen as a common objective of organized societies. The main issue regarding reliable decision support analysis to decision-makers is related to at which point in chain-reaction the human action is more harmful than useful (Endsley 1988, Endsley 2015, Endsley 1995).

4.1 Emergency situations

The lack of cooperation between situation centers prevent to create common situational awareness and picture. Starting cooperation at the scene of the accident, as Figure 5 illustrates, is not enough during a major accident in a modern cyber-physical system.

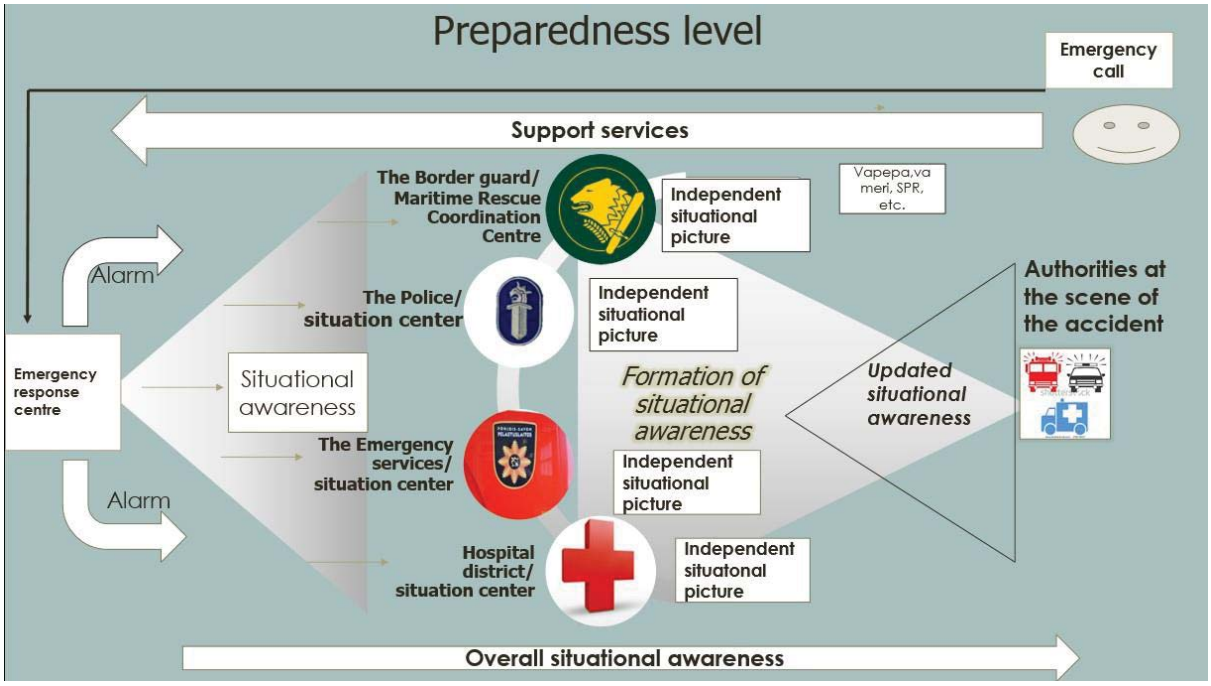

Figure 5: Formation of situational awareness

The officer in overall charge of the situation is responsible for maintaining the situational picture and for coordinating the operations. Unless otherwise agreed the officer in charge of the rescue operations comes from the rescue service region where the accident or dangerous situation occurred. Field commander and officer in charge of rescue operations decide together if it is necessary to make a major accident alert. For example The Turku University Hospital has its own command center which is set up in a case of a major accident. Leading medical director, managing dierector and other managing personnel get together in their command center depending on the type of a major accident. Communication between situation center and command center in the Turku University Hospital exists via online camera. This practice is too slow when there is a need to create a common situational picture. The differencies of rescue operations illustrate the facts that it would be important to see all the resources available. 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.

As shown in a picture of smart hybrid centre model 6. proactive accident/ incident management begins before any physical harm has occurred. Sensor networks consist cyber and physical elements. Cyber environment of Hybrid model works many ways. It detects intrusions and threats in critical infrastructure before any emergency call has been made. Data fusion analysis combine and produce important signal based on commands, which launch automatic process like isolating area under threat or robotic functions based on biometrics data like thermal imaging or face recognition. Data fusion also might help with the false alarms by fusing the information from multiple sources, also false alarms can be avoided by combining sensors. The processing device (controller) sends commands to a wireless sensor and actuator network (WSAN) which then converts them into input signals for the actuator, that acts with a physical process, thus forming a closed control loop.

The field tested DSiP solution with 4com routers (Simola, Rajamäki 2014) enables parallel use of different network technologies in a consistent and transparent way, enabling communications services platforms to be created. In cyber physical operations, this feature reduce network jamming. The hybrid model reduces necessary of communication with Virve phones between authorities. It also eliminates errors of human activity, when an accident situation is on. Automated safety measures can also bypass the problems related to the commandment of power relations. Hybrid emergency response system allows people to send pictures or video calls from the scene of the accident. Smart System allows crowdsourching software screens the images and videos automatically. Relevant data from the major accident will be directly shared to the field commanders and Governments command centre. To determinate discrepancies of limits is relevant to allocate additional reliable data. Combining pieces of information to ensure the correct and reliable information to be shared is of primary importance. The essential information is processed to the desired shape for the accident site command center.

The system is based on active operations and automated functions. Cyber defense operations are integrated and automated according to local capabilities, authorities and mission needs.

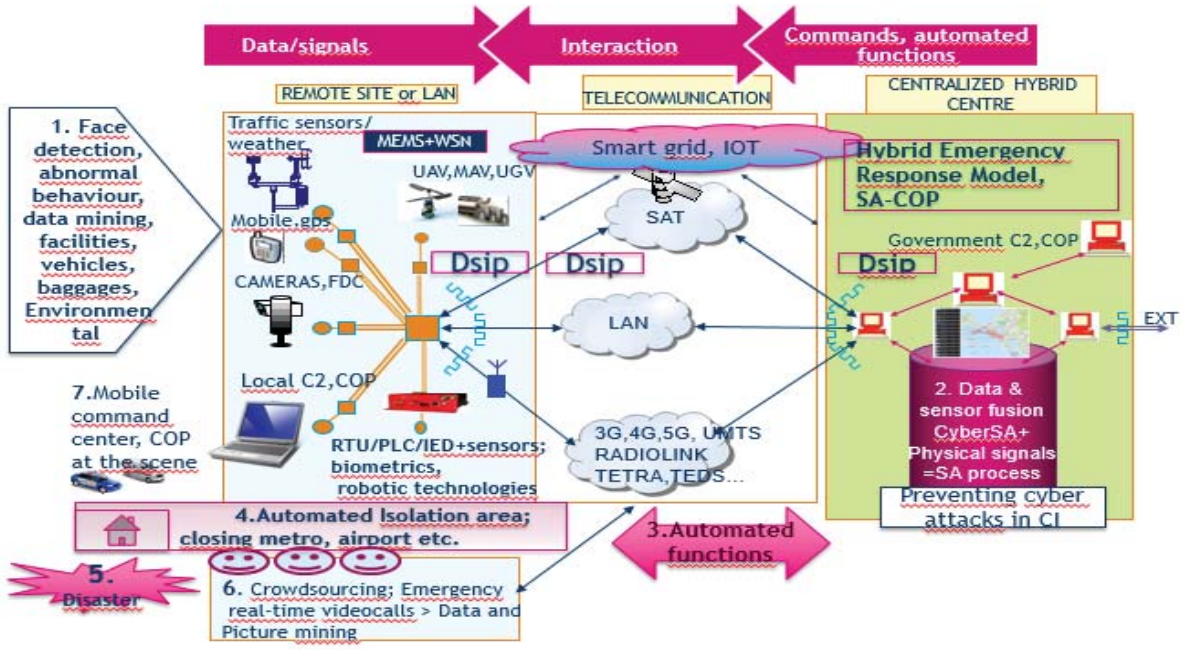

Figure 6: Smart hybrid centre model

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. 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. If there are too many hierarchy levels, information of situation does not flow or, at least, it is slow (Rajamäki, Viitanen 2014). Responsibilities for developing cybersecurity has been shared too many factors (Ministry of the Interior 2016, Ministry of defence 2010, Finnish Communications Regulatory Authority 2014, Kauppinen 2015, National Cooperation Network for Disaster Risk Reduction 2012).

5. Discussion

Both the European and the American regulations aim at achieving cyber resilience enhancing cooperation between public and private sectors in order to improve capacities, resources and processes to handle cyberphysical threats in critical infrastructures. But that´s not enough. There is a need for common cyber ecosystem to control crossboarding threats.

Traditional thought within Finnish decision-makers has been that the commercial operators must be kept separate from regulatory activities. In U.K. The Home Office-led Emergency Services Network (ESN) will replace the existing Airwave mobile radio system. ESN will be delivered using commercial network. The police communications network enabling officers to access key databases, to take electronic fingerprints and witness statements, and to stream live video while on the move (Nasir 2016, Travis 2015).

6. Conclusions

The need for a new type of hybrid emergency response model reflects the following factors; A human is an individual with limited observation capability. Overlapping and limited data transmission and lack of real time data capabilities prevents the effective cooperation between security authorities. No one of the situation centers of this case study has a possibility to direct communication connection to the Government situation centre. Fight against cyber threats is an essential part of the overall security in SA management. Instead of separate situation centers, there should be a common regional 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 in to account the equally vulnerable built infrastructures of modern urban areas. (Davis et al. 2006).

As Figure 7 shows, 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. According to Franke and Brynielsson (Franke, Brynielsson 2014), 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.

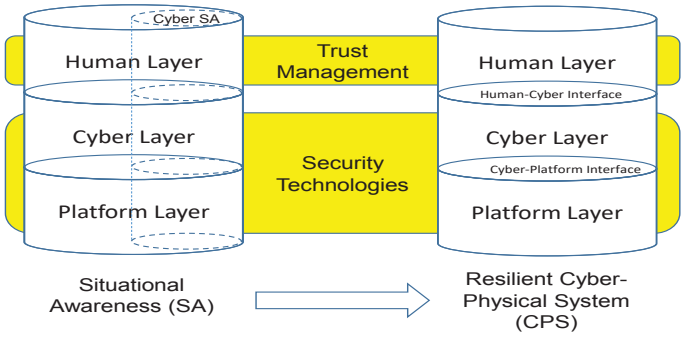

Figure 7: Situational awareness as a prerequisite of the resilience of a cyber-physical system

In the future centralized hybrid emergency model with emergency response functions is necessary. Shared common operational picture means that real time communication link from local level to state level exist. At the moment flow of real time data is not been transmitted to the Government command centre. E.g. if a cyber attack interrupted electricity transmission, telecommunication networks discontinue operating. Cyberattack become physical, if intrusion has not been detected. Hybrid warfare need hybrid responses. The government departments of Finland must take into considerations that cyber preparedness is not a separate part in the continuity management. In practice this means that there is need to integrate e.g. Emergency Response Centre and National Cyber Security Centre Finland emergency functions.

References

Ahmed, D.T., Hossain, M.A., Shirmohammadi, S., Alghamdi, A., Pradeep, K.A. and El Saddik, A. (2012) Utility based decision support engine for camera view selection in multimedia surveillance systems DOI 10.1007/s11042-012-1294-7.

Ahokas, J., T. Guday, T. Lyytinen and J. Rajamäki (2010) Secure and Reliable Communications for SCADA SystemsAnonymous *INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS*.

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

Baldini, G. (2010) *Report of the workshop on "Interoperable communications for Safety and Security" with recommendations for Security research.* Publications Office of the European Union DOI 10.2788/19075.

Brannen, J. (2004) Working qualitatively and quantitatively. In: Seale C., Gobo G., Gubrium J.F. and SILVERMAN D. eds., *Qualitative Research Practice* London: Sage Publications, pp. 312-326.

Chong, C. and KUMAR S. (2003) Sensor Networks: Evolution, Opportunities and Challenges, *IEEE*.

Davis, R., Ortiz, C., Rowe, R., Broz, J., Rigakos, G. and Collins, P. (2006) An assessment of the preparedness of large retail malls to prevent and respond to terrorist attack. (No. 216641).

Electrical Technology (2016) *Internet of Things (IOT) and Its Applications in Electrical Power Industry.* ET. [viewed 11/8/2016]. http://www.electricaltechnology.org/2016/07/internet-of-things-iot-and-its-applications-in-electrical-power-industry.html.

Endsley, M.R., (1995) Toward a theory of situation awareness. Human Factors, no. 37, pp. 32-64.

Endsley, M.R. (1998) Design and evaluation for situation awareness enhancement. Anonymous *Proceedings of the Human Factors Society 32nd Annual Meeting*.

Endsley, M.R. (2015) *Autonomous Horizons, System Autonomy in the Air Force – A Path to the Future.* Air Force Office of the Chief Scientist.

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

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

Gervasi, O. (2010) Encryption Scheme for Secured Communication of Web Based Control SystemsAnonymous *Encryption Scheme for Secured Communication of Web Based Control Systems*.

Hanni, J. (2013) *The quality and amount of information for emergency situations management.*

Hevner, A. and Chatterjee, S. (2010) *Design science research in information systems*. In: *Design Research in Information Systems: Theory and Practice.*Springer Science and Business.

Kauppinen, T. (2015) *CYBER SECURITY OF SUPPLY, FIIF JAM SESSION.* National Emergency Supply Agency, 22nd September 2015.

Lee, E., Ashford and Seshia, S., Arunkumar (2015) *Introduction to Embedded Systems, A Cyber-Physical Systems Approach.* 2nd ed. Lee&Seshia ISBN 978-1-312-42740-2.

Mclaughlin, E., Haddad, M. and Hume, T. (2016) *Brussels attacks: Order to close metro sent to wrong address - CNN.com.* Available from: http://edition.cnn.com/2016/05/12/europe/belgium-brussels-attacks-metro-email/.

Ministry of the Interior (2016) *National Risk Assesment 2015.* Helsinki: Ministry of the Interior ISBN 2341-8524/ISBN 978-952-324-060-5 (PDF).

Nasir, R. (2016) LTE to replace TETRA network for UK emergency services – Networking.

National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO) (2016) *NENA/APCO Next Generation 9-1-1 Public Safety Answering Point Requirements.* USA: NENA and APCO.

National Cooperation Network for Disaster Risk Reduction (2012) *National Platform for Disaster Risk Reduction.* Helsinki: Ministry of the Interior.

National Institute of Standards and Technology (2014) *Guidelines for smart grid cybersecurity National Institute of Standards and Technology, Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements.* U.S. Department of Commerce DOI. DOI 10.6028/NIST.IR.7628r1.

National Public Safety Telecommunications Council. (2015) *FirstNet and Next Generation 9-1-1 High-Level Overview of Systems and Functionality.*

NEC Corporation. *Face Recognition: Technologies: Biometrics: Solutions & Services | NEC.* [viewed:11/15/2016]. Available from: http://www.nec.com/en/global/solutions/biometrics/technologies/face_recognition.html.

Ministry of defence (2010) *Security strategy for society, Government resolution.* Helsinki: Ministry of Defence; ISBN ISBN: 978-951-25-2235-4 pdf.

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

Secretariat of the Security Committee (2013) *Finland´s Cyber Security Strategy - Government resolution.* Ministry of Defense.

Simola, J. and Rajamäki, J. (2014) Using a real-time video to allocate public protection and disaster relief resources in rescue service process - Natural diaster in Young voluntary firefigter´s camp *5th European Conference of COMPUTER SCIENCE (ECCS '14) 72007-127*. Geneva, Switzerland.

Steafel, E., Mulholland, R., Sabur, R., Malnick, E., Trotman, A. and Harley, N. Paris terror attack: Everything we know on Saturday afternoon - Telegraph. *The Telegraph* (11/27/2016).

The Finnish Security Intelligence Service (2015) *The Year Book.* Helsinki: Ministry of the Interior.

The Guardian (2016) Paris attacks inquiry finds multiple failings by French intelligence agencies.

Travis, A. (2015) Questions over limited range of new £1bn emergency services network. *The Guardian*.

Viinamäki, L. and Saari, E. (2007) *Polkuja soveltavaan yhteiskuntatieteelliseen tutkimukseen.* Helsinki: Kustannusosakeyhtiö Tammi.

Yin, R.K. (2014) *Case Study Research, Design and Methods.* 5th ed. Thousand Oaks: Sage Publications.