Effects of Cyber Domain in Crisis Management

Jussi Simola and Martti Lehto
University of Jyväskylä, Faculty of Information Technology, Finland
juhemisi@student.jyu.fi
martti.j.lehto@jyu.fi

Abstract: There is fundamental need in EU-level to develop common alarm procedures and emergency response models with preventive functions which work well from local to national level and from national to international level. European Public Protection and Disaster Relief (PPDR) services such as law enforcement, firefighting, emergency medical and disaster recovery services have recognized that lack of interoperability of technical systems limits cooperation between the PPDR authorities. Also, the military (MIL) and critical infrastructure protection (CIP) faces similar challenges. 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 a domino effect after a disaster may be delayed. There is a need to understand how public safety authorities can act in a preventive manner so that a potential accident or offense can be prevented in advance. This paper´s goal is to find out main factors which affect to implementing of the next generation hybrid emergency response system for critical infrastructure protection. Early detection of any threat and rapid response to neutralize the threat may help to save human lives and vital functions before any disaster occurs. By comparing present emergency response processes to the next generation Smart hybrid emergency process model, it can be found effects and factors which prevent to implement this architecture. For example, legislation, organizational changes, lack of using cyber dimension and emergency procedures effects to combine different kind of PPDR -functions. Cyber dimension as a part of situational awareness raises its value for the continuity management. For traditional purposes, PPDR services are being seen as separate physical operational functions. This study proposes to solve the problems of development needs through technical, organizational and structural alternatives. The main issue regarding dividing reliable decision support information to decision-makers is related to at which point in chain-reaction a human action is more harmful than useful. It has been seen in earlier empirical studies that human activities may prevent to manage functions of essential emergency response procedures during a disaster. It´s necessary to create emergency response model, that will be functionally capable and modern combining cyber and physical elements in a right proportion.

Keywords: critical infrastructure protection, cyber-physical threats, emergency response, PPDR, continuity management

1. Introduction

European decision-makers like politicians have recognized, that it´s not enough to start emergency response procedures in traditional way at the scene of an accident or a catastrophe. Nowadays hybrid attacks against critical infrastructure are based on combination of different kind of threats. Human factors, technological communication problems and lack of interaction between different PPDR actors show challenges at the scene of an accident. It´s necessary to take into account these things before starting to build the next generations emergency response model.

Thanks to the rapid development of information systems, national legislation has also faced new challenges. On the other hand, practiced policy in Europe has been based on the image of the world that free movement between countries should be facilitated in Europe. The obstacles to free movement were reduced in the Schengen area until the terrorism that came with the Middle East refugee wave forced the European decision-makers to change the political lines. Terrorist attacks in the United States, Australia, France, Belgium, Germany, Sweden and Finland have changed the weighting of security issues.

The EU's internal and external border control have been intensified and the conditions for asylum applications have been revised. EU information systems projects have become increasingly multinational. Security has been perceived as a common EU affair, no longer a separate national task. The importance of legislation is emphasized when building common IT structures and platforms for information systems. National legislation may become an obstacle, especially in situations where other partner countries have implemented laws that support new IT solutions. The outline of the paper is as follows. After the introduction section 2 presents theoretical framework and central concepts of the paper. Section 3 handles research background, objectives and methods. Section 4 handles findings. Section 5 include discussion and section 6 conclusions.

2. Theoretical framework and literature review

In the future it´s not enough to develop separate technological solutions for critical infrastructure protecting. In EU-level there is a need to reach common situational picture when cross-boarding threat like cyberattack has occurred. Smart nations or European union needs cooperation between smart cities, because without smart cities smart nation cannot form. Thus smart information systems are being developed, it´s important that there is already infrastructure where to connect the system. Every smart city should be construct from a long-term view. Smart city needs urban built environment. This case study aims to find out those factors which affect to implementation of the Hybrid Emergency Response Model. There are separate situation centers, emergency response centers and organizations fighting against cyber threat´s, but there is no common emergency response model for all kind of hybrid-threats. The author of this research has innovated next generation emergency response model (Simola & Rajamäki, 2017). It´s necessary to research things that are setting barriers to implementation process.

The proposed cross-boarding intelligent emergency management system will provide next generation emergency response model for state decision-makers and PPDR-authorities. The model will combine different data sources, analyze them and produce predictive emergency actions before an alarming accident has occurred. Developed Hybrid Emergency Response -model is one kind of concept which can be expanded to the maritime surveillance environment.

2.1 Data protection regulation in EU countries

The EU General Data Protection Regulation (GDPR) harmonize data privacy laws across Europe. The law is technology neutral and applies to both automated and manual processing if the data is organized in accordance with pre-defined criteria (European Commission, 2016b). The purpose is to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. GDPR applies to all businesses offering goods and/or services to EU. That means that the organizations do not have to reside in the EU area or even in Europe. If you are holding private information about an EU citizen whom you provide services, GDPR applies (European Commission, 2016b).

Personal data cover e.g. name, address, email address, an internet protocol address, location data on a mobile phone and a cookie ID, the advertising identifier of your phone. In some cases, there is a specific sectoral legislation regulating for instance the use of location data or the use of cookies. Directive presents mostly a continuation of earlier Data Protection Directives efforts (European Commission, 2016b).

Eu directive named the ePrivacy 2002/58 has been amended by Directive 2009/136, which introduces several changes, especially in what concerns cookies, that are now subject to prior consent. The directive does not apply to issues concerning criminal law and state security, public security and defense. The interception of data is covered by the new EU Data Retention Directive the purpose of which is to amend E-Privacy Directive (IBP, 2014)

The EU Data Protection Directive 2016/680 or Law Enforcement Directive regulates on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. This proposal applies cross-border and national processing of data by member states' competent authorities for the purpose of law enforcement. This comprise e.g. the prevention, investigation, detection and prosecution of criminal offences, the safeguarding and prevention of threats to public security (European Commission, 2016a).

2.2 Central concepts

2.2.1 Smart city, nation and infrastructure

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). Fig. 1. Illustrates secure communication flows, electrical flows and different domains (Updated NIST Smart Grid Framework 3.0, Feb 2014).

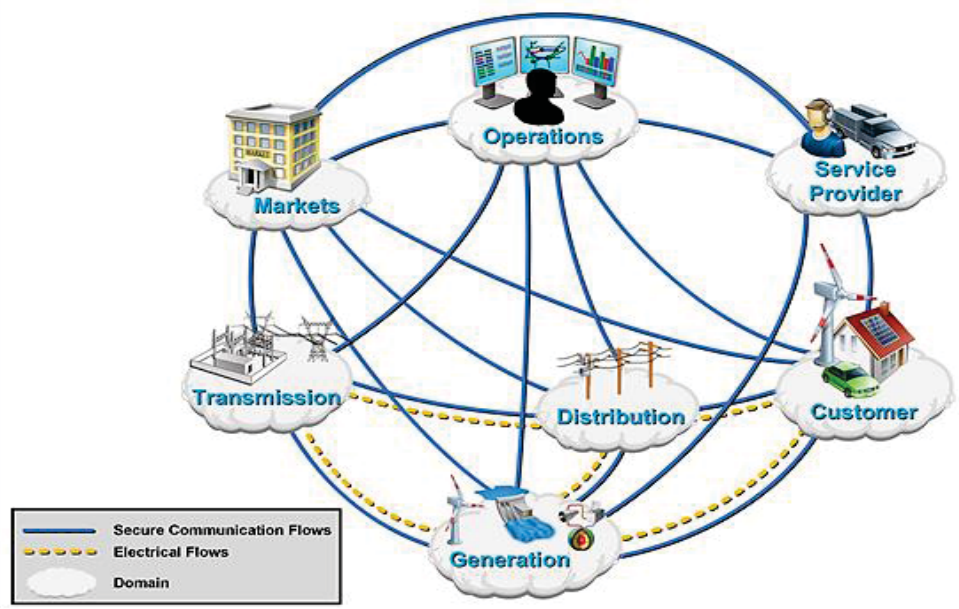

Figure 1: Interaction of actors in different smart grid domains

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 (CHONG & KUMAR, 2003; National Institute of Standards and Technology, 2014). 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).

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 (Ahokas, Guday, Lyytinen, & Rajamäki, 2010; Ministry of the Interior, 2016).

2.2.2 Sensors for monitoring, buildings, bridges and other structures

The development of more robust and advanced smart sensors could help provide valuable information about the health of various structures, including bridges, tunnels, buildings like shopping malls and water distribution systems. Sensors can provide valuable insight on the structural health and condition of bridges or buildings. In the future building can monitor the activities of all individuals inside the building. In the future buildings, bridges and shopping malls are part of smart city and smart grid (NIST, 2012).

2.2.3 Location based sensors

Retailers of malls may use indoor or/and outdoor navigation technologies to provide location-based services using mobile ‘‘push’’ notifications to provide advertisements. Technologies are currently available to not only locate a customer but are also be able to establish history of a path taken by a typical customer during the day (Kini & Suomi, 2018; Rachel, 2013). Advertisement networks are able to locate and custom-deliver an advertisement to customer with or without customer’s permission. With this technology it is possible to provide personalized marketing based on the consumer’s location. If mobile users give permission (opt-in) to the companies whose brand, products and services they like, companies send them personalized advertisements when they are shopping (Yiu, Jensen, Møller, & Lu, 2011).

2.2.4 Cyber infrastructure and 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. CPS are enabling next generation of "smart systems" like advanced robotics, computer-controlled processes and real-time integrated systems (Lee & Seshia, 2015). Cyber Infrastructure Includes electronic information, communications systems, services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information or any combination of all of these elements. Processing includes the creation, access, modification and destruction of information. Storage includes paper, magnetic, electronic, and all other media types (National Institute of Standards and Technology, 2014). According to Franke and 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, e.g. 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). Communications include sharing and distribution of information, e.g. computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) which are part of cyber infrastructure.

2.2.5 Cyber and hybrid threats

According to DHS & Office of Emergency Communications (2016) cyber threats can be illustrated in many ways. Potential Risks to emergency response system components may be formed from devices or equipment, network infrastructure and connections or data applications and services. In spear-phishing attack means that a criminal finds a webpage for his target organization that supplies contact information for the company. Using available details to make the message seem authentic, the criminal drafts an email to an employee on the contact page that appears to come from an individual who might reasonably request confidential information, such as a network administrator. The email asks the employee to log into a false page that requests the employee's username and password or click on a link that will download spyware or other malicious programming (Rouse, 2017). Data breaches mean data has stored on user device and it is accessed, manipulated or stolen. Users may download malicious software "malware" (e.g., botnets, viruses, spyware, trojans and rootkits). It is called "Man-in-the-middle attack" when wireless link between the user device and the tower may be susceptible and allow attackers to steal data or monitor conversations. In Denial-of-service (Dos) attack, criminals overload towers or other key network resources with requests for network access, damaging or destroying the operability of the targeted infrastructure and straining the capacity and resiliency of the network. Insider threats: Employees or other authorized personnel may produce insider threats when they use their access to steal, corrupt, or destroy data. In malicious applications attackers create applications that appear to be safe but allow them to steal, corrupt or modify data, eavesdrop on conversations, or acquire data on the location of victims and/or first responders (DHS & Office of Emergency Communications, 2016). Hybrid threat means for example combination of different kind of physical and cyber threats.

2.2.6 PPDR services

The term "Public Protection" is used to describe critical public services that have been created to provide primary law enforcement, firefighting, emergency medical and disaster recovery services for the citizens of the political subdivision of each country. The term Public Safety and Disaster Response, within certain regions, can also be construed as PPDR. The military (MIL) and critical infrastructure protection (CIP) are also included in the term (Baldini, 2010).

The Emergency Response Centre Administration provides emergency response center services throughout Finland. The duty of the Emergency Response Centre Administration is to receive emergency calls from all over the country for the rescue, police and social and health services; handle communications relating to the safety of people, property and the environment; and relay the information they receive to the appropriate assisting authorities or partners (National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO), 2016; The emergency response act, 2010).

2.2.7 Emergency response management information systems

Traditional Emergency Response System should consist of at least basic components like a database, data analysis capability, normative models and interfaces. E.g. personnel in Emergency Response Center use Emergency Response system. It is one kind of DSS system. Decision support systems are used to track key incidents and the progress of responding units, to optimize response activities and to act as a mechanism for queuing ongoing incidents (Ashish et al., 2007; Endsley, 1988; Endsley, 1995).

Situation center means the place where PPDR authorities make decisions to allocate resources to the right proportion. The words Command and Control individually and collectively mean different things to different communities (Alberts & Hayes, 2006). C2, situation center or Emergency Operation Room is a physical or virtual location designed to support emergency response, business continuity and crisis communications activities. PPDR authorities meets at the C2 -room to manage preparations for an impending event or manage the response to an ongoing incident. By gathering the decision makers together and supplying them with the most current information can be made better decisions (Ashish et al., 2007). In systems engineering, monitoring means a process within a distributed system for collecting and storing state data. A PPDR monitoring station is a workstation or place in which sensor information accumulates for end users who need it. Monitoring systems include information collection, analysis and provision for end-users, which is front-deployed knowledge. Government Situation Centre ensure that the state leaders and central government authorities are kept informed continuously (Ministry of defence, 2010).

2.2.8 Open Source Intelligence as a part of the HERM

OSINT is defined as the systematic collection, processing, analysis and production, classification and dissemination of information derived from sources openly available to and legally accessible by the public in response to particular government requirements serving national security. It is any unclassified information, in any medium, that is generally available to the public, even if its distribution is limited or only available upon payment (Glassman & Kang, 2012; Morrow & Odierno, 2012; Nurmi, 2015).

3. Research background, objectives and methods

At present public safety authorities (PPDR) do not use cyber dimension in their daily routine at all. The problem is that public safety authorities have separate Cyber security organizations with own administrations. Organizations which have responsibilities for cyber security operations are separated from PPDR services. As a part of FICORA, The National Cyber Security Centre Finland (NSCS-FI) produce information of Cyber threats for stakeholders, but that data does not reach e.g. emergency response centers or situation centers. Separate organizational cyber security functions, methods and procedures prevent effective response for cyber physical threats. Combining Open Source Intelligence data (Morrow & Odierno, 2012) and traditional intelligence sources overall situational awareness arises. Hybrid threats need coordinated hybrid responses, therefore also a cyber situational picture is needed.

3.1 Method and process

3.1.1 Case study research strategy

Empirical approach helps to understand PPDR authorities´ entity. Choosing a case study research strategy enables investigation of interaction between the different factors. The multimethodological approach consists of four case study research strategies: theory building, experimentation, observation and systems development (Nunamaker, Minder Chen, & Purdin, 1991). Yin (2014) identifies five components of research design for case studies: (1) the questions of the study; (2) its propositions, if any; (3) its unit(s) of analysis; (4) the logic linking the data to the propositions; and (5) the criteria for interpreting the findings. This case study is carried out with the guidance of Yin (2014). This research concentrates in sources of scientific publications, collected articles and literary material.

3.1.2 Analyzing vulnerabilities

We can divide research-area in four sections; local, regional, national and European level. Local PPDR-area consists of one city or municipalities, regional area is wider area including organizations like regional administration with PPDR-authorities, cities and municipalities. The focus of the research is on the protection of

critical infrastructure at local and regional level and how the current EMS system could be developed to be able to respond to the future challenges of cross-border cooperation between PPDR authorities. This is an important question, because there is a common need to develop interoperability between information systems within European Union member countries. Firstly, next generation emergency response system should work in lowest local level before it can be connected to the next level.

We have used combination of different methodologies to find out those factors which affects to introduction of the next generation emergency response model. The Framework by National Institute of Standards and Technology focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework will help an organization to understand, align and prioritize its cybersecurity activities with its mission requirements, risk tolerances and resources. The Tiers or levels provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives (DHS & Office of Emergency Communications, 2016; National Institute of Standards and Technology, 2018).

A prescriptive metric known as Technology Readiness Level (TRL) has being used mainly by NASA, the DoD, the DoE and the Department of Homeland Security to address the readiness of systems under development. TRLs have been adapted for biomedical systems, modeling and simulation technologies, learning systems and software intensive systems, among others. Additional readiness levels (RLs) were developed to meet specific needs. Proliferation does emerge as a problem when the tendency is to add new undefined RLs that did not have the quality control in their construction as the original (Perseus, 2013).

To address integration, another metric called Integration Readiness Level (IRL) was introduced by the Systems Development & Maturity Laboratory (SysDML) at Stevens Institute of Technology. The introduction of an IRL to the assessment process not only provides a check as to where a technology is on an integration readiness scale but also presents a direction for improving integration with other technologies. Combining both TRL and IRL scales it is possible to form a knowledge base on the technological maturity level of the emergency response services infrastructure. Tier levels 1-3 are used instead of 1-9 in this research. Two emergency response systems were compared with each other; present system and the next generation hybrid emergency response model.

Three main categories have been chosen to classifications:

- Legislation concerning the smart hybrid model
- Technological maturity Level
- Readiness Level of organizational and political view

The approach of the research is at the local and regional level and it includes the intelligent city area with its authorities and operational functions of situation centers and emergency response information system.

4. Results

4.1 Emergency response model for critical infrastructure protection

The highest state decision-makers, such as members of the Finnish government or highest public safety officers must understand digital entity of the environment where citizens are living. As figure 2 illustrates, formation of cyber-physical threats is gathered from different sources and separate organizations handle those threats. There is no common preventive cyber functionalities or connection between emergency response administration and National Cyber Security Centre Finland which acts under the Finnish Communications Regulatory Authority.

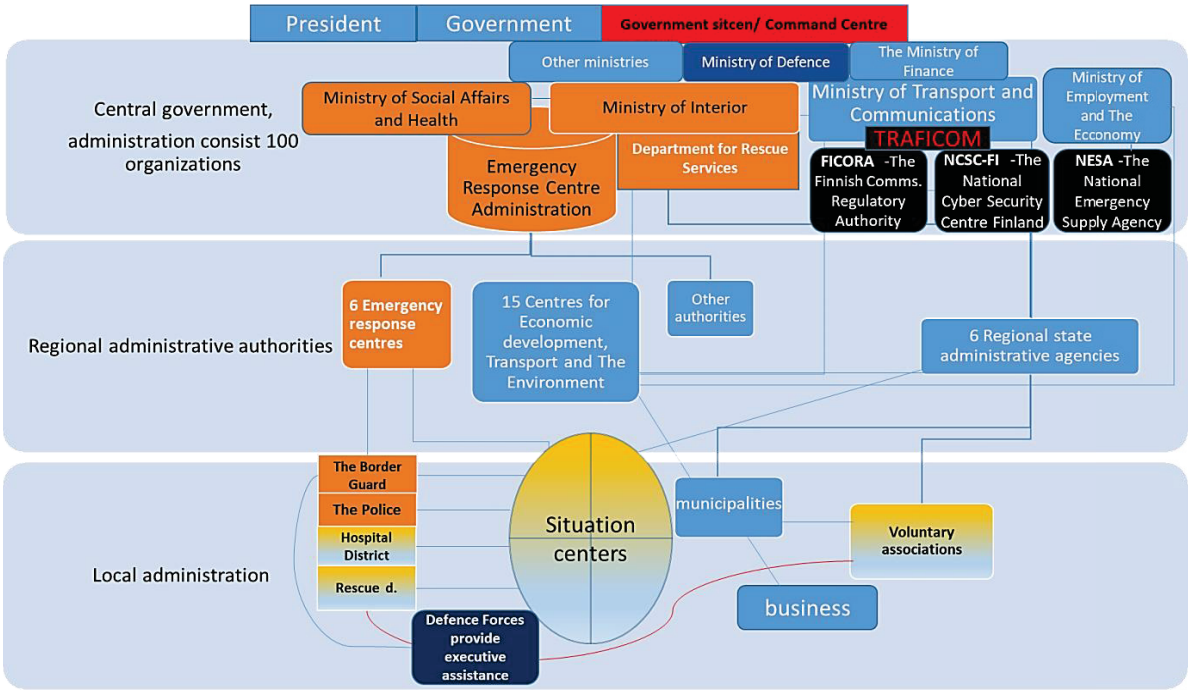

Figure 2: Organizations responsibilities of cyber security

Hybrid emergency response model as a part of smart society and smart city will create a secure framework with efficient procedure to identify and assess national and cross-boarding threats in critical infrastructure. It will provide efficient decision support solution for decision-makers and PPDR authorities how to protect critical infrastructure, but there are fundamental factors which prevent to start implementation of the system. When present national and European development concerning developing next generation emergency response model are taken into consideration the difference of new and the old model illustrated as fig.3.

Maturity level	**Low**	**Med**	**High**	
	1	2	3	
Low (red 1) presents that the maturity level of the system does not correspond the research area. Medium (green 2) presents that the maturity level is average. High (blue 3) presents that the maturity level of the system is ready for the implementation.				
Research areas	**Present system**		**Next gen. HERM syst**	
European legislation	1		2	
Legislation concerning technology	3		1	
Legislation concerning privacy issues	3		2	
Legislation concerning the smart hybrid model	sum	7		5
Technological maturity	2		3	
Smart city maturity	1		3	
Maturity of organizational Integration	1		2	
Opportunities to use smart devices	1		3	
Opportunities to integrate sensor tech.	2		3	
Maturity to integrate it-systems	1		3	
Operational reliability	2		2	
Technological maturity Level	sum	10		19
Organizations maturity level	3		1	
The political readiness at national level	3		1	
European policy	1		2	
Readiness Level of organizational and political view	sum	7		4
Total	24		28	

Figure 3: Maturity level of emergency response systems

Firstly, there are organizational factors which prevent to implement new system. Those factors are closely related to legislation, because there is PPDR administration like emergency services which act under the municipalities. Emergency Response Centre acts under Ministry of Interior. On the other Coast guard acts under the Ministry of Interior, but Defense forces act under The Ministry of Defence. There is a lot to do that the operating environment would be favorable to the next generation emergency response system. In Finland the legislation does not give permission for law enforcement to trace citizens digital behavior in real time. Tools like OSINT, Geo-targeting, Geo-fencing with Wi-Fi, Cell Towers and Beacons create a privacy-restricting advertisement and surveillance circuit that aims to trace consumer behavior. These tools are possible to use only with new Hybrid Emergency Response model. Therefore, maturity level for using mobile technologies is so low.

5. Discussion

In democratic society, it must be taken into consideration that privacy concerns and public safety functions both effect to our quality of life. No one wants to live in an environment where citizen´s rights and responsibilities are unclearly defined. Important things for us, such as the data privacy issues, can be more relieved on the grounds that the "common good" requires it. How can we then define the common good? This issue has been controversial in Europe. Determining the public interest or limiting the need to protect society has sometimes caused difficulties. The problem is related to situations where protected legal intresses are incompatible. Government agents, utility executives, policymakers and technology providers must agree about a common goal and take actions to accelerate the process towards final deployment, legal and organizational barriers have to be removed. Given the scale of the effort required and the enormity of the challenges ahead, collaboration among different sectors is essential and should be developed through various channels in order to ensure and accelerate the success of the future smart control centers. In a society where the limits of public and private commercial players have become obscured, the risks are also increasing. Citizens should be able to trust decision-makers, authorities, and society that they do not have to constantly think about what kind of digital footprints they are left behind in any department store control unit. As a single datum, separate information of human life is not significant, but if data is combined from the different sources, the position of a citizen as a manager of his or her own life may change significantly.

6. Conclusions

The new intelligence legislation package proposed by the Finnish government would include provisions on the principles of intelligence activities. If the legislation package will be approved, it is expected to enhance the ability of the PPDR authorities to respond on major national and international hybrid threats, because it also allows wider use of new decision support system technologies. It requires clarification of common rules. In other words, in a public place, e.g. in shopping centers privacy protection should be facilitated if citizen accept common rules which have been created in the form of legislation.

People have been irritated by the fact that people's behavior has been collected much more widely, what has been told and uses that are not known. Therefore, it might be important to look at the big picture of the protection of critical infrastructure. What kind of elements can be included in the framework which protect the vital functions of society? When all the things we do leave some data to tracking systems, people have the right to know what information is collected and for what purpose it has been collected. Perhaps even more important thing is to know who is the holder of the personal data and what is the storage time of the data.

The next generation hybrid model will integrate existing surveillance systems and networks with new ones and it based on active operations and automated functions. There is a need to strengthen the entire intelligence ecosystem in maritime and inland. There is also a need in command and control functions to design a combination of a new kind of hybrid sensor technology that uses location based solutions and OSINT tool in order to detect threats in advance because common cyber situational picture is needed. Location based intelligence is an applicable emergency response tool for public safety authorities in shopping malls and in city areas. The presented hybrid model will offer an updated emergency response management model to PPDR services. Effective cooperation between public safety authorities needs a common technology for all authorities and organizational cooperation requires a common infrastructure and clearer and faster connections.

A dynamic cyber-physical infrastructure is needed in order to respond to a rapidly evolving alert situation. The local and state level PPDR -atmosphere can no longer be separated in the traditional sense. Threats have

changed into combinations of threat types and, as a consequence, public safety organizations like the Police or Finnish Border Guard must be able to prevent new kinds of hybrid threats and respond to them. Improving the flow of information between the public sector and citizens, including volunteer associations, is also a relevant part of this framework. It must be possible to prevent and respond faster to the realization of threats. Municipal actors relying on municipal technical resources is not sustainable because cooperation between the Police, Finnish Border Guard and emergency services has developed. A modelling platform for a smart emergency response model can lead to important new results. The cyber domain can be used as a powerful dimension to enhance data fusion to more accurate overall situational awareness. By processing raw data on anomalous behavior in advance, PPDR services can use smart emergency response functions before any threats have occurred.

References

Ahokas, J., Guday, T., Lyytinen, T., & Rajamäki, J. (2010). Secure and reliable communications for SCADA systems. Paper presented at the *International Journal of Computers and Communications,6*(3)

Alberts, D. S., & Hayes, R. E. (2006). *UNDERSTANDING COMMAND AND CONTROL. DoD command and control research program.* Center for Advanced Concepts and Technology (ACT).

Ashish, N., Kalashnikov, D. V., Mehrotra, S., Venkatasubramanian, N., Eguchi, R., Hegde, R., & Smyth, P. (2007). Situational awareness technologies for disaster response. In H. Chen, E. Reid, J. Sinai, A. Silke & B. Ganoz (Eds.), *Terrorism informatics: Knowledge management and data mining for homeland security*. Springer.

Baldini, G. (2010). *Report of the workshop on "interoperable communications for safety and security" with recommendations for security research.* (No. JRC60381). Publications of Office of the European Union. doi:10.2788/19075

CHONG, C., & KUMAR, S. (2003). Sensor networks: Evolution, opportunities and challenges. Paper presented at the *IEEE, 91*(8) 1247-1256.

DHS, & Office of Emergency Communications. (2016). *Cyber risks to next generation 911.* Department of Homeland Security.

Electrical Technology. (2016). Internet of things (IOT) and its applications in electrical power industry. Retrieved from http://www.electricaltechnology.org/2016/07/internet-of-things-iot-and-its-applications-in-electrical-power-industry.html

The emergency response act 692/2010, (2010).

Endsley, M. R. (1988). (1988). Design and evaluation for situation awareness enhancement. Paper presented at the *Proceedings of the Human Factors Society 32nd Annual Meeting,* 97-101.

Endsley, M. R. (1995). Toward a theory of situation awareness. human factors. (37), 32-64.

EU data protection directive 2016/680, Directive U.S.C. (2016a).

General data protection regulation (EU) 2016/679, Regulation U.S.C. (2016b).

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

Glassman, M., & Kang, M.,Ju. (2012). Computers in human behavior; intelligence in the internet age: The emergence and evolution of open source intelligence (OSINT).*28*(2), 673-682.

IBP. (2014). *European union cyber security strategy and programs handbook. strategic information and regulations.* Washington DC, USA: International Business Publications.

Kini, R., B, & Suomi, R. (2018). Changing attitudes toward location-based advertising in the USA and Finland, journal of computer information systems.*58* doi:10.1080/08874417.2016.1192519

Lee, E., Ashford, & Seshia, S., Arunkumar. (2015). *Introduction to embedded systems, A cyber-physical systems approach* (2nd ed.) Lee & Seshia.

Ministry of Defence. (2010). *Security strategy for society, government resolution*. Helsinki: Ministry of Defence;

Ministry of the Interior. (2016). *National risk assessment 2015*. Helsinki: Ministry of the Interior.

Morrow, J., & Odierno, R. (2012). *Open-source intelligence, ATP 2-22.9, army techniques publication.* (). Washington: Headquarters, Department of the U.S. Army.

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. Retrieved from https://www.nena.org/resource/resmgr/Standards/NENA-APCO-REQ-001.1.1-2016_N.pdf.

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:10.6028/NIST.IR.7628r1

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity.* (No.1.1). NIST.

NIST. (2012). *Cyber-physical systems: Situation analysis of current trends, technologies and challenges.* (). Maryland, USA: National Institute of Standards and Technology.

Nunamaker, J., Minder Chen, J. R., & Purdin, T. (1991). Systems development in information system research. (3), 89-106.

Nurmi, P. (2015). *OSINT - avointen lähteiden internet-tiedustelu*. Helsinki: Aalto yliopisto.

Perseus. (2013). *Protection of European seas and borders through the intelligent use of surveillance D26.12 working document: Assessment report.*

Rachel, M. (2013). MIT Technology review. Retrieved from https://www.technologyreview.com/s/510491/every-step-you-take-tracked-automatically/

Rouse, M. (2017). Spear phishing. Retrieved from https://searchsecurity.techtarget.com/definition/spear-phishing

Simola, J., & Rajamäki, J. (2017). Hybrid Emergency Response Model: Improving Cyber Situational Awareness. Paper presented at the *16th European Conference on Cyber Warfare and Security,* University, College, Dublin, Ireland. 442-451.

Yin, R. K. (2014). *Case study research, design and methods* (5th ed.). Thousand Oaks: Sage Publications.

Yiu, M., L., Jensen, C. S., Møller, J., & Lu, H. (2011). Design and analysis of a ranking approach to private location-based services. *ACM Transactions on Database Systems, 36*(2), 10:1-10:42. doi:10.1145/1966385.1966388

Sylvain (Sly) Leblanc is an Associate Professor and Interim Chair for Cyber Security at the Royal Military College of Canada (RMC). Sly was a Canadian Army Signals Officer for over 20 years, where he developed his interest in computer network operations. His research interests are in computer security, cyber operations development and cyber education.

Wai Sze Leung is an associate professor at the Academy of Computer Science and Software Engineering at the University of Johannesburg. Her current research interests include digital forensics and the application of Artificial Intelligence in enhancing cyber security.

Dr. Andrew N. Liaropoulos is Assistant Professor in University of Piraeus, Department of International and European Studies, Greece. His research interests include international security, intelligence reform, strategy, foreign policy analysis, European security policy and cyber security. Dr. Liaropoulos is also a member of the editorial board of the Journal of Information Warfare (JIW).

Jarno Limnéll is the Professor of cybersecurity in Aalto University, Finland. Martti Lehto is the Professor of cybersecurity in University of Jyväskylä, Finland.

Christoph Lipps graduated in Electrical and Computer Engineering at the University of Kaiserslautern. Born in Pirmasens, Germany in 1986, he started working as a Researcher and Ph.D. candidate at the German Research Center for Artificial Intelligence (DFKI) in Kaiserslautern. His research focuses on Physical Layer Security (PhySec), Physically Unclonable Functions (PUFs) and entity authentication.

Dr. Leandros A. Maglaras received the B.Sc. degree from Aristotle University of Thessaloniki, Greece in 1998, M.Sc. in Industrial Production and Management from University of Thessaly in 2004, and M.Sc. and PhD degrees in Electrical & Computer Engineering from University of Volos, in 2008 and 2014 respectively. In 2018 he was awarded a PhD in Intrusion Detection in SCADA systems from University of Huddersfield. He is the head of the National Cyber Security Authority of Greece and a part time Senior-Lecturer in the School of Computer Science and Informatics at De Montfort University, U.K. He serves on the Editorial Board of several International peer-reviewed journals such as IEEE Access and Wiley Journal on Security & Communication Networks. He is an author of more than 100 papers in scientific magazines and conferences and is a senior member of IEEE.

Nnana Mogano is a professor of computing at University of Pretoria, South Africa. She received her Bachelor of Science in Statistics and Computer Science and Honours in Statistics from the University of Limpopo, South Africa in 2014. Her main interests are data analytics to enhance business models and operations.

Potsane Mohale is a master's student of the Academy of Computer Science and Software Engineering at the University of Johannesburg. He works as a software engineer based in Johannesburg, South Africa.

Pardis Moslemzadeh Tehrani is a Senior Lecturer in the Faculty of Law, University of Malaya where she has been a faculty member since 2015. Her research interests lie in the area of Cyber Terrosim, Human Right, International Humanitarian Law, Cloud Computing in Law. Pardis has widely published papers in a number of national and international Conferences.

Dr Jabu Mtsweni is a Research Group Leader for Cyber Defence at the Council for Scientific and Industrial Research (CSIR), Research Fellow at University of South Africa, and Advisory Board Member at ITWeb Security Summit. His research interests and technical expertise are in cyber warfare, cybersecurity, and cybercrimes. He has over 15 years academic and industry experience with over 60 peer-reviewed conference and journal articles.

Julie Murphy has over 10 years of experience in telecommunications working primarily with Fortune 500 companies, and currently works as a Security Expert with IBM X-Force Red. Julie lectures part-time in the Technological University Dublin and is actively involved in promoting cybersecurity awareness and training.

Abdalmuttaleb M.A. Musleh Al-Sartawi is the Editor-in-Chief of the International Journal of Electronic Banking (IJEBank). He received his PhD in Accounting, from UBFS. He has chaired as well as served as a member in various editorial boards and technical committees in international refereed journals and conferences.

Youngsup Shin is a researcher in Agency for Defense Development, South Korea. He is in an integrated PhD program in Korea University. His main research areas are cyber situational awareness and cyber warfare.

Ph.D. Petteri Simola is a senior psychologist at the Finnish Defence Research Agency, Human Performance Division. His work involves human aspects of information security, Human Factors (especially sleep) and aptitude testing in recruitment.

Jussi Simola is a PhD student of cyber security in University of Jyväskylä. His area of expertise includes decision support technologies, SA systems, information security and continuity management. His current research is focused on effects of cyber domain as a part of Hybrid Emergency Response Model.

Mr Veikko Siukonen is a research officer at Finnish Defence Research Agency (FDRA). He resieved his Master's Degree in Military Sciences from The National Defence University in 2007. He is a master of science student (cyber security program) in University of Jyvaskyä. His main research areas are cyber warfare and cyber threat intelligence.

Tiia Sõmer is early stage researcher at Tallinn University of Technology. She is conducting PhD level studies, focusing on modelling cyber criminal journey mapping. In addition to research she does teaching and has co-authored educational materials for general education. Before starting academic career, she served for more than twenty years in the Estonian defence forces.

Lee Speakman, Lee gained his PhD in the area of Mobile Ad hoc Networks from Niigata, Japan, in 2009. Since then Lee worked in the area of networks, network security, and software exploitation and protection measures in Defence. Lee joined the University of Chester in 2015 to develop and deliver the University's new Cybersecurity programmes and research.

Ilona Stadnik is a PhD student at the School of International Relations, Saint-Petersburg State University, Russia. During 2018-2019 academic year she was a Fulbright visiting researcher at Georgia Institute of Technology, USA, working with Internet Governance Project. She has been a regular participant and speaker at major cybersecurity events such as the United Nations Internet Governance Forum (IGF), CyFy conference, European Dialogue on Internet Governance (EuroDIG). Her research covers international cyber norm-making, Russia-US relations in cybersecurity, and global Internet governance.

Dr. Nikolai Stoianov is Colonel in the Bulgarian armed forces, Deputy Director of the Bulgarian Defence Institute "Prof. Tsvetan Lazarov" and principal member of NATO's Science and Technology Board. He is also associate professor and leads several international research projects on cybersecurity and related issues.

Mr Marcel Stolz is a doctoral student in cyber security at the University of Oxford, UK. He has a background in Computer Science and has served as a First Lieutenant in the Swiss Armed Forces. His research interests lie in global cyber security and regulation of data companies, such as Facebook.

Dr. Steven Templeton is a researcher at the University of California, Davis, USA. Since 1999 he has operated a consulting firm specializing in ICS security and compliance. Originally a wildlife biologist, in 2018 he received his PhD in computer science. His research spans multiple area of computer security, in particular intrusion detection, monitoring, and attack modelling.

Dr Ben Turnbull is a Senior Lecturer for the University of New South Wales, Australia. He is an expert in cyber security and digital forensics with 16 years in the industry. He is also a Certified Information Systems Security Professional (CISSP). He has previously worked as a research scientist for the Defence Science and Technology Organisation in the field of cyber network defence and analysis. In his spare time, Ben plays too many card and board games.

Maija Turunen is a PhD Student at the Finnish National Defense University. Her main research areas consist of cyber warfare, Russia and strategic communication. Maija Turunen works as a legal counsel at the Finnish Transport Infrastructure Agency.