Emergency Response Model as a part of the Smart Society

Jussi Simola[1,2], Martti Lehto[1], Jyri Rajamäki[2]
[1]University of Jyväskylä, Finland
[2]Laurea Universtiy of Applied Sciences, Finland
jussi.hm.simola@jyu.fi
martti.j.lehto@jyu.fi
jyri.rajamaki@laurea.fi
DOI: 10.34190/EWS.21.079

Abstract: Centralized hybrid emergency model with predictive emergency response functions are necessary when the purpose is to protect the critical infrastructure (CI). A shared common operational picture among Public Protection and Disaster Relief (PPDR) authorities means that a real-time communication link from the local level to the state-level exists. If a cyberattack would interrupt electricity transmission, telecommunication networks will discontinue operating. Cyberattack becomes physical in the urban and maritime area if an intrusion has not been detected. Hybrid threats require hybrid responses. The purpose of this qualitative research was to find out technological-related fundamental risks and challenges which are outside the official risk classification. The primary outcomes can be summarized so that there are crucial human-based factors that affect the whole cyber-ecosystem. Cybersecurity maturity, operational preparedness, and decision-making reliability are not separate parts of continuity management. If fundamental risk factors are not recognized, technical early warning solutions become useless. Therefore, decision-makers need reliable information for decision-making that does not expose them to hazards. One of the primary aims of hybrid influence is to change political decision-making. Practically, this means a need to rationalize organizational, administrative, and operative functions in public safety organizations. Trusted information sharing among decision-makers, intelligence authorities, and data protection authorities must be ensured by using Artificial Intelligence (AI) systems. In advanced design, protection of critical infrastructure would be ensured automatically as part of the cyber platform's functionalities where human-made decisions are also analyzed. Confidential information sharing to third parties becomes complicated when the weaknesses of crucial decision-making procedures have recognized. Citizens' confidence in the intelligent system activities may strengthen because of the decision-making process's reliability. Existing emergency response services are dependent on human ability.

Keywords: Critical Infrastructure Protection, cyber ecosystem, emergency response, public protection and disaster relief, artificial Intelligence

1. Introduction

As earlier researches (Simola & Rajamäki, 2015; Simola &Rajamäki, 2017) has shown, technical solutions need a deeper understanding of user needs. That means the infrastructure of a smart city environment cannot be developed separately from user requirements. There is also a need to design a common emergency response ecosystem for European public safety actors. Therefore, communication solutions used within public safety authorities must suit well in urban and rural area**s.**

Public safety actors like European law enforcement agencies need a common shared situational picture for the cross-boarding tasks so that operational cooperation is based on a reliable platform. Formal integration in the European Union and between member countries has developed rapidly. That does not mean that collaboration between organizations has developed in the same proportion. Digitalization cannot evolve in isolation from society. There are fundamental needs within public European safety organizations that should be at the same level in every country.

Decision-makers in Finland need to consider that cybersecurity maturity, operational preparedness, and decision-making reliability are integral parts of continuity management. Technical early warning solutions become useless to develop if crucial risk factors are not detected. Therefore, decision-makers need reliable decision-support information for decision-making that does not expose them to hazards. Technological development, infrastructure development, and legislation changes are inner-country challenges and everyday European needs concerning safety development agendas. State-level factors should be added to the European safety framework. There are many strategic plans at the European level concerning

safety functions, but national implementation realizes in a different order. As the report of the SAI (2017) indicates, Finland has a lot to do to improve the information exchange in significant accident situations.

Citizens choose political decision-makers, but the highest authorities are selected on selection criteria. Hybrid influencing can destabilize society in many ways, especially if threats accumulate or arise from within the society (Simola, 2020). One of the primary key aims is to influence political decision-making. In practice, this means a need to rationalize organizational, administrative, and operative functions (SAI, 2017). The flow of reliable information between decision-makers, intelligence authorities, and data protection authorities must also be ensured by using artificial intelligence systems. In an ideal model, national protection of vital functions would be ensured automatically as part of the cyber platform's functionalities where human-based decisions are also analyzed. When human weaknesses are left out of decision-making procedures, e.g., data leakage to third parties becomes more difficult. It could increase citizens' confidence in the smart system's activities and increase trust in government institutions.

Security and intelligence agencies in Europe have acquired new rights under the law. In Finland acceptation of Intelligence legislation package concerning civilian and military intelligence legislation has been approved. It will be seen in the future how prepared our state-level decision-makers are to develop the legislative base for the new cyber-physical ecosystem. A substantial part of Finland's intelligence legislation has been updated to the same level as in other European countries. The rest of this paper is divided as follows. Section 2 handles the overview of the theoretical framework. Section 3 proposes the central concepts of critical infrastructure and the framework of this article. Section 4 presents the research background, objectives, and methods. Section 5 presents the findings. Section 6 includes a discussion about the research area. Section 7 handles conclusions.

2. Theoretical framework and literature review

Member countries of the European Union and smart cities need cooperation because, without smart cities, the European Union's intelligent ecosystem cannot be created. Financial competition between countries creates the need for the development of intelligent technology. Thus, intelligent information systems are being developed; there must be an already digital ecosystem to connect the system. Every smart city should be constructed from a long-term view. A smart city needs an urban built technology-oriented environment where different kinds of intelligent systems communicate with each other. This case study aims to find out those fundamental technological-related risks that expose society to hybrid threats. These threats affect the protection of critical infrastructure and prevent the detection of threats. Implementation of the presented Hybrid Emergency Response Model is the primary purpose because there are separate situation centers, emergency response centers, and organizations fighting against cyber threats. Still, there is no common emergency response model for all kinds of hybrid-threats. The main author of this research has innovated the next-generation emergency response model (Simola & Rajamäki, 2017).

2.1 Development of Emergency Response system solutions

Emergency Response Center uses an Emergency Response system. It is one kind of decision support system. Decision support systems are used to track key incidents and the progress of responding units, optimize response activities and act as a mechanism for queuing ongoing incidents (Ashish et al., 2007; Endsley, 1988; Endsley, 1995).

In Finland, traditional emergency response functions have been modeled from other countries. However, we still have significant challenges related to the possibilities of transferring emergency data correctly and in time to the Emergency response center. There was a separate emergency response unit in the Police organizations until 1999. E.g., regional Radio Police consisted of their dispatch personnel who answered citizens' emergency calls and managed the use of emergency units to the site of an accident. Also, municipal rescue services handled their emergency calls. In the 21st century, separate emergency call units and functions were combined with emergency response centers. Very soon after the organization's changes, PPDR authorities found the need to manage their emergency resources. PPDR organizations established their situation centers to allocate emergency resources concerning field workers' cooperation.

The culture of the organization needs to be understandable when the purpose is to develop new technological solutions. Public safety organizations have a common working culture but also separate inner-organizational subcultures. That same issue concerning the meaning of the working culture relation to organizational reform also occurs in a different atmosphere and a different field. In practice, smart city infrastructure is the fundamental framework that governs minor factors inside it. It is impossible to create technological solutions in their separate entity regardless of the organizations' culture.

2.2 Smart nations and smart cities

Political power relations affect the national future of digitalization. Urbanization changes our lifestyle, and the digitized environment creates the base for the new safety culture. Citizens meet friends in public places, and they might go to the shopping center for shopping goods. Time has changed more dangerous; global terrorism has impacted people's behavior. Historical similarities between countries in northern Europe helps to understand the safety needs of neighboring countries. While separate European societies are evolving, societies are developing their cooperation on digitalization. It is essential to see the digitalization development of the north from the same perspective. There are different political aspects between European Union countries concerning energy and security policy. EU as the commercial operator brings its own needs into the discussion. Collaboration with Russian and China challenges our culture and western way of thinking. We need cooperation, but possibilities for cybersecurity threats emerge too often (Robertson & Riley 2018). Nord Stream2 and different kinds of 5G and cable projects may expose national security under cross-boarding hybrid risks (Buchanan, 2017; Shackelford et al., 2017; Buchanan, 2018; Hutchens, 2018).

It is impossible to create the entirety of a smart society without understanding the continuity management of society. If departments of the central government design separate digitalization projects without a common understanding of the future needs, society's expenses and digitalization management become complex. The governance of digitalization needs common goals for all participants. It means that the regional and local administrative operators need exact central steering concerning all municipal constructions of infrastructure.

3. Critical Infrastructure

The united states define critical infrastructure as physical or virtual systems and assets that are so vital that destructions of the above would have a crucial influence on security, national economic security, national public health, and safety, or any combination of those matters (The White House, 2013). According to the Secretariat of the Security Committee (2013), critical infrastructure comprises vital physical facilities, infrastructures, and electronic functions and services.

Critical Information Infrastructure comprises any physical or virtual information system that controls, processes, transfers, receives, or stores electronic information in any form, including data, voice, or video that is vital to the functioning of critical infrastructure (DHS 2011).

3.1 Fundamental elements of critical infrastructure in smart society

U.S Department of Homeland Security (2013) classifies 16 different sectors for the Critical Infrastructure as follows: “Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare, and Public Health, Information Technology, Nuclear Reactors, Materials and Waste, Transportation Systems and Water Wastewater System” (DHS 2013).

Department of Homeland Security categorizes, e.g., the communication sector closely linked to the Energy sector, the Information sector, the Financial services, the Emergency services, and the Transportation system sectors (DHS, 2013). Every government uses a different emphasis level between the importance of emphases. In this research communication sector, the energy sector, information technology, and emergency services sector have been chosen as selected sectors of critical infrastructure.

3.2 Risk management and preparedness

According to (NIST, 2018) the framework is used in U.S. suites well also in Finland. The risk management framework consists of three elements of critical infrastructure (physical, cyber, and human) that are explicitly identified and should be integrated throughout the steps of the framework. The critical infrastructure risk management framework supports a decision-making process that critical infrastructure actors or partners collaboratively undertake to inform the selection of risk management actions. It has been designed to provide flexibility for use in all sectors, across geographic regions, and by various partners. It can be tailored to dissimilar operating environments and applies to all threats (DHS, 2013).

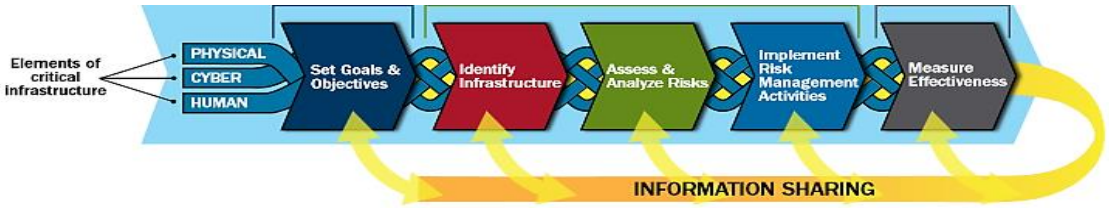

Figure 1: Critical Infrastructure Risk Management Framework

The risk management concept enables the critical infrastructure actors to focus on those threats and hazards that are likely to cause harm and employ approaches that are designed to prevent or mitigate the effects of those incidents. It also increases security and strengthens resilience by identifying and prioritizing actions to secure continuity of essential functions and services and support enhanced response and restoration (DHS, 2013).

According to the Department of Homeland Security (2013), the first point recommends setting infrastructure goals and objectives that are supported by objectives and priorities developed at the sector level. To manage critical infrastructure risk effectively, actors and stakeholders must identify the assets, systems, and networks that are essential to their continued operation, considering associated dependencies and interdependencies. This dimension of the risk management process should also identify information and communications technologies that facilitate essential services (DHS, 2013).

The third point recommends assessing and analyzing risks. Those Risks may comprise threats, vulnerabilities, and Consequences. A threat can be a natural or human-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. The vulnerability-based risk may occur physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. A consequence can be the effect of an event, incident, or occurrence. Implementing risk management activities means that decision-makers prioritize activities to manage critical infrastructure risk based on the criticality of the affected infrastructure, the costs of such activities, and the potential for risk reduction. The last element measuring effectiveness means that the critical infrastructure actors evaluate the effectiveness of risk management efforts within sectors and at national, state, local, and regional levels by developing metrics for both direct and indirect indicator measurement (DHS, 2013).

In this research, we have used a modified combination of NIST and Octave Allegro Risk Assessment Frameworks. According to Caralli & al. (2007), Octave allegro is a strategy for prioritizing and sharing information about security risks, e.g., information technology. According to (Zio & Pedroni, 2012) NASA risk-informed risk is the potential for performance shortfalls, which may be realized in the future, with respect to achieving explicitly established and stated performance requirements. As Figure 2 illustrates, Risk Management by NASA integrates two complementary processes, Risk-Informed Decision Making (RIDM) and Continuous Risk Management (CRM), into a single coherent framework. The RIDM process addresses the risk-informed selection of decision alternatives to assure effective approaches to achieving objectives, and the CRM process addresses the implementation of the selected alternative to ensure that requirements are met. These two processes work together to assure effective risk management as NASA programs (NASA, 2015).

Figure 2. Combined risk management processes.

3.3 Protecting vital society

According to (The Security Committee, 2018; Ministry of defence, 2010), threats can occur on the individual, national, and global levels. Individual threats primarily affect the individual, national threats primarily affect the state, society and population, global threats affect the earth and the population's future security. Figure 3 illustrates those levels relations. According to the Ministry of the Interior (2018) three top-level threat scenarios are severe disturbances in the power supply and cyber threats like severe disturbances in the telecommunications and information systems. Vital functions to the Finnish society contain the management of Government affairs, international and EU activities, Finland's defence capability, internal security, the functioning of the economy, infrastructure and security of supply, functional capacity of the population and services and psychological resilience to a crisis (Ministry of the Interior, 2018).

Figure 3: Threats on the individual, national, and global level

3.4 Artificial Intelligence helps continuing management

Artificial Intelligence (AI) is a part of the system that displays intelligent behavior by analyzing their environment and taking multiple actions with autonomy to achieve given purposes. Software-based artificial intelligence systems can act in the virtual world consisting of image analysis software and search engines. Also, it may be embedded in hardware devices, e.g., advanced robots, unmanned vehicles, or Internet of Things applications (European Commission 2018).

An intelligent Agent (IA) is an entity that produces decisions. It allows performing, e.g., specific tasks for users or applications. It can learn during the process of performing tasks. Two main functions consist of perception and action. Intelligent Agents form a hierarchical structure that comprises different levels of agents. A so-called multi-agent system consists of several agents that interact with one another (Wooldridge 2009). That combination may solve challenging problems in society. The agent may behave in three ways: reactively, proactively, and socially (Wooldridge 2009).

4. Research background, objectives, and methods

There have been many state-level discussions concerning digitalization among decision-makers in media. At present public safety authorities and decision-makers do not use cyber-threat information in their operative daily routine almost at all. The challenge is that public safety authorities have separate cybersecurity organizations in their administrations. Organizations that have responsibilities for cybersecurity operations act as separated entities from PPDR services. As a part of TRAFICOM, the National Cyber Security Centre Finland (NSCS-FI) produces and shares cyberthreats information for stakeholders. Still, shared data does not achieve emergency response centers or situation centers. Separate organizational cybersecurity functions, methods, and procedures prevent an effective response to cyber-physical threats. In addition to this, developed innovations, e.g., emergency response systems, are all useless if our ministers and other decision-makers are not faithful or decisions are made to advantage a foreign power. It is essential to realize the source and degree of threat. The innovative urban areas and information systems may be constructed on an unstable ground level that may consist, e.g., energy supply solutions and dicey communication equipment. Overall situational awareness enhances by combining Open Source Intelligence data and traditional intelligence data (Morrow and Odierno 2012). The cyber situational picture is needed because Hybrid threats need hybrid responses.

4.1 Method and Process

The multimethodological approach consists of four case study research strategies: theory building, experimentation, observation, and systems development (Nunamaker & al., 1990). 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 research is carried out with the guidance of Yin (2014). The research concentrates on sources of scientific publications, collected articles and literary material. The research subject comprises public safety organizations, procedures, and vital functions of Finland society.

The first purpose of this qualitative research was to collect and classify selected risks from different risk areas. In this research, we have used the Modified Risk Assessment Framework. The second purpose was to find out hidden technological-related state-level risks and challenges that are outside the official risk classification. A simple process model helps to identify those fundamental factors that are used in the creation of the scenarios. We have defined the research area concerning vital functions in four main sections; the Emergency services sector, the Communication sector closely linked to the Energy Sector, and the Information sector. Firstly, it is essential to find out technological-related risks and scenarios that expose society's vital functions to hybrid-threats and risks. It is easier to detect fundamental level risk factors when basic threats and risks are categorized and classified. These threats affect the protection of vital functions and prevent the detection of threats. We have used a combination of different methodologies to find out those factors that affect decision-making in society. As Table 1 illustrates, separate risks are divided into the main areas as follows: Administrative risks, conflict risks, emergency functions related risks, socioeconomic risks and infrastructure-related risks. The numbers A, B, C, D, and E indicate which main category the subcategories are also linked. Separate risks are categorized and ranked on a three risks level process. The first measure is valued "frequency of the phenomenon" (1 = phenomenon does not occur every year, 2 = phenomenon occurs yearly, and 3 = a phenomenon is permanent). The second value is titled "predictability and measurability of risks" (1= phenomenon is neither predictable nor measurable, 2= phenomenon is predictable. 3 = phenomenon is predictable and measurable.) The third value is named "impact of risk on overall security" (1= impact of the risk on one vital function, 2=impact of the risk on two to three vital functions, and 3 = impacts of risk to more than three selected vital functions.) Coefficients for variables are 1 to "frequency of the phenomenon," 2 to predictability and measurability of risks, and 3 to "Impact of risk on overall security.

Table1: Main risk classification

Main risk classification and subcategories								
A		B		C		D		E	
Aministrative risks		Conflict risks		PPDR services and functions related risks		Sosioeconomic risks		Infrastructure related risks	
Problems in local continuity management	C,D	Cyberattacks	A,C,E	Overloaded Emergency management system	B,E	Unemployment	A	Structural problems in the built urban area	A,B,C
Problems in cooperation between decisionmakers	B,C,D,E	Human made disasters or pandemia	E	Lack of human resources in PPDR services	A,D,E	Refugees	A,B	Structural problems in the rural area	A,B,C,D
Separate municipal activities	E	Cross-border radiation	C,D,E	Lack of resources in PPDR services/	A,D,E	Cultural change	A	Recovery problems	A,B,C,D
Organizational problems	B,C,	Physical war	A,C,D,E	Emergency event	D,E	Use of substances	B,C	Secrets cyber influences	A,B,C,D
Leadership problems in government	B,C,D,E	Hybrid warfare	A,C,D,E	Resource awareness of volunteers	A,D,E	Citizens poverty	A	Communicatio n problems	A,B,C
						Unidentified people	A,B,C,E		

The research aims to create a decision support subsystem solution for the proposed Hybrid Emergency Response system to assist politicians and public sector actors. That is an important issue because there is a need to detect sources of threats much earlier.

We have used the methodology model and framework by the National Aeronautics and Space Administration In designing the subsystem of Hybrid emergency response systems. The continuous Risk Management (CRM) process stresses the management of risk during implementation. The Risk-Informed Decision Making (RIDM) methodology is part of a systems engineering process that emphasizes the proper use of risk analysis in its broadest sense to make risk-informed decisions

that impact all mission execution domains, including safety, technical, cost, and schedule. RIDM helps ensure that decisions between alternatives are made with an awareness of the risks associated with each helping to prevent late design changes, which can be key drivers of risk and cancellation (NASA, 2016).

Figure 4 illustrated the risk analysis framework that helps to analyze the different alternatives and factors when decision-makers are making final decisions (Dezfuli et al.,2010; Zio and Pedroni, 2012).

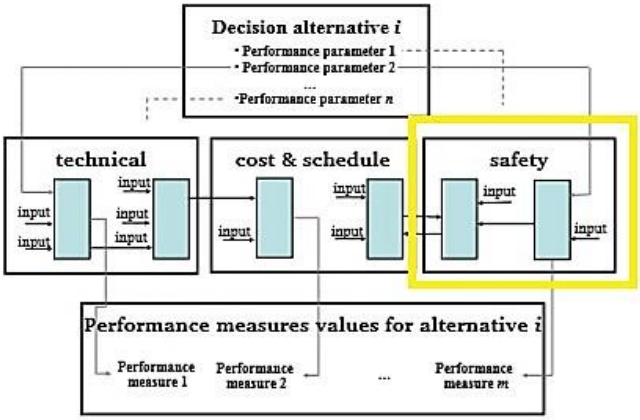

Figure 4: Risk analysis framework

The study's main goal is to find out fundamental societal factors that affect the effective protection of critical infrastructure. This research divides the types of risks into four sections. Ground Level indicates fundamental risks with scenarios that include factors, events, and actions of society. The scenarios' essential factors put all other societal factors, events, or actions into secondary threats level. Fundamental factors also make it possible to realize lower-level threats. This causes that the effective protection of critical infrastructure depends on external factors. The operator who controls external factors also dominates critical infrastructure. Therefore fundamental ground-level risk factors should be recognized and minimized.

5. Findings

Table 2 illustrates elements of society between risk levels. Higher risk levels are on the right, and these elements set the greatest threats to the vital functions. If ground-level threats are realized, the protection of critical infrastructure loses its meaning. E.g., the wide use of substances may indirectly harm society's overall security, but addiction cannot remain hidden for a long time. As a member of the EU, Finland gave away part of the national parliaments' sovereignty concerning national regulation. This kind of problem may happen when supranational legislation gives away the power of decision-making from the government to the commercial operators. E.g., change of ownership of the electricity transmission network.

Table 2: Classifications and impacts of risks

Classified by effetiveness of fundamental hidden risks and scenarios (red level) – Impacts and disruption on selected scenarios and consequences. Level of risks based on three values (frequency of the phenomenon, predictability and measurability of risks and impact of risk on overall security). Impact level 1-3 (1 =low, 2=average level, 3=high impact) 1 = impact on 1-2 scenarios, 2 = impact on 3-4 scenarios, 3 =impact on 5-6 selected scenarios. 1 = X, 2 = XX, 3 = XXX								
Classified basic risk levels. 1= low 4 =high	1		2		3		4	
	levels 6-10 –1		levels 11-13 –2		levels 14-16 –3		levels 17-18 – 4	
	Refugees	X	Overloaded Emergency management system	XX	Structural problems in the rural area	XX	Cyberattacks	XXX
	Cultural change	X	Lack of resources in PPDR services/	XX	Human made disasters or pandemia	XX	Separate municipal activities	XXX
	Use of substances	X	Resource awareness of volunteers	X	Structural problems in the built	XXX	Secrets cyber influences	XXX
	Unemployment	X	Emergency event	X	Leadership problems in government	XXX	Hybrid warfare	XXX
			Cross-border radiation	X	Lack of human resources in	XX	Unidentified people	XXX
			Organizational problems	XX	Communication problems	XXX		
			Problems in local continuity management	XX	Problems in cooperation between decision makers	XXX		
			Citizens poverty	X	Recovery problems	XXX		
					Physical war	XXX		

Findings indicate that lower-level risks of critical infrastructure do not cause problems to the ground-level risks. Higher-level risks also indicate structural governance problems in society. The effectiveness level indicates threats' impacts to the vital functions. Three x means that basic independent level risk becomes more dangerous due to connection ground level scenarios. As Table 3 illustrates, six scenarios were selected. At which impact level selected risks to affect to potential consequences of the scenarios? As illustrated in table 1 one X indicate impact on 1-2 scenarios, XX indicate impact on 3-4 scenarios, XXX = indicate impact on 5-6 selected scenarios. If higher (4) level risk support 4 or more scenarios and consequences, impact level is occasional for all vital functions. The domino effect causes this change of situation. E.g., a separate cyberattack is not so dangerous, but the event's danger will essentially change if it is due to a political decision.

Table 3*:* Scenarios and consequences (The table has been changed to match the original table of the research)

Ground-level – Scenario	Consequences
A) Legislation – Lack of possibilities to intervene in internal security	Lack of internal self-determination and internal sovereignty
B) Political decisions – Lack of continuity	Line changes in security policy - development of unstable decision-making culture
C) Energy solutions – Dependence on imported energy management, short-term political purposes	Exposure to extortion by an external actor
D) Equipment for Communication systems – E.g., 5g solutions devices, network equipment.	Foreign state spying and foreign country get a role in infrastructure
E) International public projects - Smart cable projects, gas pipeline projects	Vulnerability to sabotage - the foreign state may use cables and pipelines for hybrid influencing
F) Decision-makers credibility- corruption, discrimination, criminal contacts to foreign state	Ability to prevent disturbances will decrease. National overall security and resilience level decreases. As a result, management of overall security becomes uncontrollable**.**

Threats like severe disruptions to a power supply, severe disruptions to telecommunications and information systems risks are noticed in Finland's security strategy for society report. Still, the same fundamental risk types occur as the causes that have not been considered in decision-making.

6. Discussion

In Finland, existing solutions for public operators based on outdated technology and systems' life-cycles are short (DHS, 2018). Currently, the victim of an accident may have to wait long for the emergency response center's response because call center personnel have to exercise how the new Emergency Response Center system works (Saarenpää J. & Virtanen V. 2019). The handling of incoming and outgoing phone calls will lengthen.

Development towards the digital ecosystem starts with cultural understanding and process management. The subcultures of different PPDR authorities should be implemented through systems. Currently, all actors have their own separate operating model. E.g., if a complete emergency response system requires a significant additional workforce, designing has failed. Technological opportunities have not been exploited in Finland, such as in the U.S. The introduction of an immature system on holiday does not reflect the understanding of the situation in the operating environment (Rahko, 2018). A fully automated emergency response center can be a reality within a decade. An automated decision support system for the highest decision-makers can be a reality soon because vital functions require proof of political decisions.

7. Conclusions

As discussed above, we cannot hide our history and culture, but if we are developing a cyber-secure smart ecosystem, we need to make changes to the decision-making culture. The research has been shown that different kinds of structural fundamental-level threats may occur before any classified threat has been illustrated. Engineers, architects, and designers cannot develop anything new concerning smart solutions if the ground base is weak. An unsecured platform causes fundamental obstacles to designing solutions for an intelligent society. Legislation set challenges to the national politicians and authorities, but also power relations between union countries.

The micro and macro levels will be encountered if a foreign state party intervenes to interfere with data traffic functioning in maritime areas. E.g., there is a northeast cable project designed to connect networking activities between different continents. Nowadays, the problem is that fiber optic and power supply are transmitted through the same cable. So-called unexpected happenings influence all ecosystems. This kind of threat comes true and happens out of public safety control. In the future, it is an occasional issue to find the right balance between national security and warm bilateral relations.

Vulnerabilities and risks have increased, though formally, the goal is to harmonize Eastern and Western data cable functionalities (Buchanan, 2018; Shackelford et al., 2017). The study shows that the most troublesome and most significant threats to national security and vital functions are related to human factors, that are based on politicians' decisions and political projects. It is challenging to anticipate national policy's real direction at the macro level because good inter-state relations may indicate ignoring security issues. The study suggests that artificial intelligence-based solutions should be used enhancing to support decision-making. The subsystem could also operate as a part of the next-generation emergency response model. This model will work in two ways. Firstly, the framework consists of predictive and preventive elements that react when cyber-threat data fusion produces signals through the AI-agents and sensors that activate actuators, e.g., bollards or evacuation systems in smart cities infrastructure. Secondly, the system will output handled data for the decision-makers as politicians. This dimension uses the method that connects small pieces of data into a big view producing the situational picture. At present, state-level political decision-making culture may prevent the proposed smart hybrid emergency model's utilization and usefulness. Decision-makers of Finland need to consider if fundamental risk factors are not recognized, technical early warning solutions become useless.

References

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.

Buchanan, E. (2017). "From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and what to do about It." 96 (2).

Buchanan, E. (2018) Sea Cables in the Thawing Arctic. Lowy Institute, last modified 01.02.2018, accessed 20.08.2018, https://www.lowyinstitute.org/the-interpreter/sea-cables-thawing-arctic.

Caralli R. A., Stevens, J. F., Young, L. R., Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Technical report. U.S. Software Engineer Institute. Carnegie Mellon University

DHS, (2011). Blueprint for a Secure Cyber Future – The Cybersecurity Strategy for the Homeland Security Enterprise

DHS, (2013). NIPP 2013 - Partnering for Critical Infrastructure Security and Resilience.

DHS, (2018). Office of Emergency Communications: Cyber Risks to Next Generations 9-1-1.

Dezfuli, H., Stamatelatos M., Maggio G., Everett C., & Youngblood R. (2010). NASA Risk-Informed Decision Making Handbook: Office of Safety and Mission Assurance NASA Headquarters.

Endsley, M. R. (1988). "Design and Evaluation for Situation Awareness Enhancement. "Human Factors Society.

Endsley, M.R. (1995). "Toward a Theory of Situation Awareness. Human Factors." (37): 32-64.

European Commission (2018) Artificial Intelligence for Europe 237.

Hutchens, G. 2018 "Huawei Poses Security Threat to Australia's Infrastructure." The Guardian, last modified 30.10.2018, accessed 28.02.2019, https://www.theguardian.com/australia-news/2018/oct/30/huawei-poses-security-threat-to-australias-infrastructure-spy-chief-says.

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

Ministry of the Interior. (2018). National Risk Assessment 2018. 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.

NASA. (2015). Considering Risk and Resilience in Decision-Making. Hampton, Virginia: National Aeronautics and Space Administration.

NASA. (2016). Systems engineering handbook. Washington. National Aeronautics and Space Administration.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity: National Institute of Standards and Technology.

Nunamaker Jr. J., Chen M. & Purdin, T. (1990). Systems development in information system research. Vol 7 (3), 89–106.

Rahko, P. (2018) Uusi tietojärjestelmä otettiin käyttöön Oulun hätäkeskuslaitoksessa onnistuneesti, paikalla oli yöllä lähes kaksinkertainen henkilömäärä. Kaleva.

Robertson, J. and Riley, M. (2018) "The Big Hack: How China used a Tiny Chip to Infiltrate U.S. Companies?" Bloomberg, last modified 4.10.2018, accessed 2/28, 2019, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

Saarenpää J. & Virtanen V. (2019) Erica-hätäkeskustietojärjestelmä Käyttöönoton vaikutukset poliisin päivittäiseen kenttätoimintaan.

SIA. (2017). Turku stabbings on 18 August 2017/ Puukotukset Turussa, Safety Investigation Authority, Helsinki 18.8.2017

Secretariat of the Security Committee. (2013). Finland's Cyber Security Strategy - Government Resolution: Ministry of Defense.

Shackelford, S. J., Sulmeyer M., Graig Deckard, A. N., Buchanan, B. & Micic, B. (2017). From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and what to do about It. 96 (2): 321-337.

Simola J. & Rajamäki J. (2015) "How a real-time video solution can affect to the level of preparedness in situation centers," 2015 Second International Conference on Computer Science, Computer Engineering, and Social Media (CSCESM), Lodz, 2015, pp. 31-36, doi: 10.1109/CSCESM.2015.7331824

Simola, J. & Rajamäki, J. (2017). "Hybrid Emergency Response Model: Improving Cyber Situational Awareness." University, College, Dublin, Ireland, APCI, 29-30 June.

Simola, J. (2020). Privacy issues and critical infrastructure protection. In: V. Benson and J. McAlhaney, eds, Emerging Cyber Threats and Cognitive Vulnerabilities. Academic Press, pp. 197-226.

The Security Committee. (2018). Security Strategy for Society. Helsinki: The Security Committee.

The White House. (2013). Federal register – Improving Critical Infrastructure Cybersecurity

Wooldridge, M. (2009) An Introduction to Multiagent System, 2 ed. John Wiley & Sons, United States.

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

Zio, E. and Pedroni, N. (2012). Risk-Informed Decision-Making Process. Toulouse, France: Foundation for an Industrial Safety Culture.