Saving Lives in a Health Crisis Through the National Cyber Threat Prevention Mechanism Case COVID-19

Jussi Simola

Faculty of Information Technology,

University of Jyväskylä, Jyväskylä, Finland

e-mail: jussi.hm.simola@jyu.fi

Abstract Today's ongoing coronavirus pandemic has shown that our overall public security mechanism in Finland requires a more coherent system that combines different types of sensors with artificial intelligence-based systems. Various states may have a crucial task: creating a common early warning system with a cyber dimension. But first, the decision-making process for public safety administration must be enhanced at the national level. COVID-19 has demonstrated the difficulty of predicting the progression of a pandemic, and nearly every country on earth has faced remarkable challenges from the spread of disinformation. False information has been shared around many public health and safety-related issues—such as how the virus is spread, the usefulness of self-protection, and the side effects of vaccines. Effective early warning tools are needed to prevent the domino effect of misinformation and to ensure the vital functions of society. This research will demonstrate the need for a common emergency response model for Europe to ensure national public safety—along with a technical platform at least for the interface between the countries. Hybrid-influenced incidents require a hybrid response.

Keywords Pandemic · Emergency response · Early warning · Information sharing Situational awareness

1 Introduction

In Finland, the Ministry of Social Affairs and Health (STM) and the Finnish Institute for health and Welfare (THL) are the organizations responsible for ensuring the virus does not spread. Finland's Emergency Response Administration is responsible for the crucial administrative functions around warning and alerting the public.

It is vital to note that the ongoing COVID-19 pandemic crisis constitutes just one version of the emerging viruses that are spreading. In Finland, official reports have shown no crucial weaknesses in the national preparedness level; the society's current state of vital functions is stable. Yet there is a need to enhance, for example, strategic management, political commitment, international activities, situational awareness, the protection of vital functions, legislation, and strengthening cyber security as a national competitive advantage, and as a part of overall security [32]. The vital functions of society allow it to maintain its resiliency. Meanwhile, the problems that now have emerged in central administration and middle-level administration reflect challenges around reliable information sharing and the use of evidence-based information.

Situational awareness has been lacking, for nearly the entire period of response to the COVID-19 crisis. A concise and easy-to-understand summary of the general guidelines has not been provided to citizens. This is compounded by other challenges. First, legitimate jurisdictional issues have caused political confrontation; the responsibilities of officials and politicians have been unclear for some time. Second, pandemic preparedness plans and action plans will not produce added value if they are not implemented. The political and administrative debate around separation of powers between government ministries has caused major problems in the coordination of decision-making. It is not enough merely to attempt to survive the daily challenges around the virus pandemic, while the potential for new incidents of misinformation, cybercrime incidents or public health crisis increases [50]. For example, the limited patient care capacity of hospitals makes it difficult to cope with a simultaneous accident. Yet government resources are insufficient to be distributed everywhere they are needed.

At present, Finland's social and healthcare system is overloaded. Tens of thousands of patient records were stolen from the Finnish therapy center Vastaamo [33]. The patient records of several officials and politicians have been leaked to the secret Tor network, and victims of such crimes have been subjected to blackmail [33]. Sensitive and personal data must be protected in the Finnish healthcare system and in addition at the European level. Along with grave privacy breaches like these, nearly every country has faced massive challenges due to the spread of misinformation through media and social media. Such misinformation has driven a divergence in people's perceptions and understanding of critical facts around the pandemic—as well as around the response chosen by decision-makers. False information has been shared around crucial public health and safety-related issues, including how the virus is spread, the benefits of self-protection, and vaccinations.

In this chapter, our research problem is formulated in Sect. 2.2. Section 2.3 discusses basic problems around the formation of situational awareness in a pandemic situation. Section 2.4 handles the central concepts of our review. Section 2.5 describes previous studies conducted by the researcher. Section 2.6 presents the findings and Sect. 2.7 provides discussion and conclusions.

2.2 Problem Formulation

The public debate on COVID-19 has pitted economic development and security against each other. Good economic development can help create security, because sufficient wealth provides an opportunity to create well-being and security. Lack of wealth will increase insecurity.

How can we find a balance in the flow of information? Information warfare has created barriers to forming a coherent situational picture of the COVID-19 pandemic. Figure 2.1 illustrates the formation of crisis information nationally among citizens, media (including social media), and states' decision-makers. It also shows the second crucial element: foreign influencers, including the press, scientific researchers, authorities, and politicians.

The overall formation of a situational picture has been notably difficult. Finland's government officials and members of the government have relied heavily on the World Health Organization's (WHO's) statements about the global spread of the COVID-19 pandemic. Yet is it sufficient to use one or two international organizations as sources, to support decision-making at the state level? The WHO predicted an ongoing pandemic a year ago [15]. It has been argued that WHO executives' connections with the Chinese administration would have prevented a rapid, transparent, and effective information exchange with other countries [3]. This is why we need an early warning system, at least at the European level—one that more quickly takes into account changing threat factors across the world. We need to be able to analyze raw data more quickly, we need to be able to find health abnormalities faster.

The fight against cross-border health threats requires excellent preparation and coordinated action—before, during, and after the crisis. We must be able to process and analyze scientific research more quickly. We must also be able to compile data into a sensible map of measures to be taken, and these strategic measures must be implemented quickly enough to suppress crises like pandemics on time. Solutions

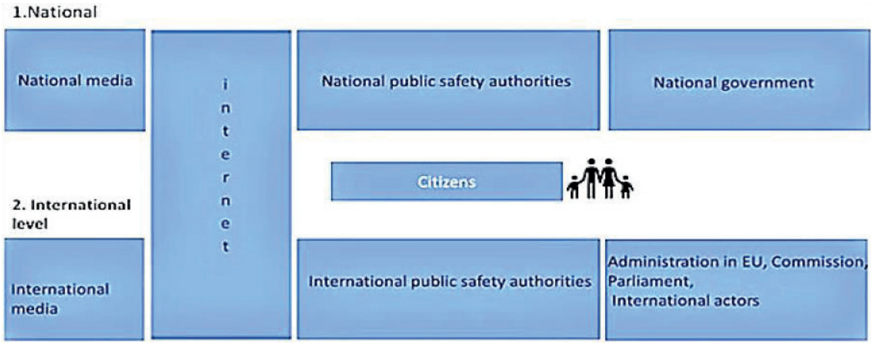
1.National
National media
internet
National public safety authorities
National government
Citizens
2. International level
International media
International public safety authorities
Administration in EU, Commission, Parliament, International actors

Fig. 2.1 Formation of crisis information

utilizing artificial intelligence can help enormously, in such a rapidly evolving event process.

It is problematic that no separate operational "power team," or even national science adviser, has been used to advise the government of Finland. Italy was left nearly alone in its struggles against COVID-19, despite claims that the EU was acting as one front. While the European Union did not effectively work towards a common goal, it did coordinate some issues concerning all member states and placed a joint order on masks. Yet Finland was left out EC [10]. The availability of protective equipment created an almost warlike situation among different European countries.

The purpose of this publication is to look for those factors and influences that pose obstacles to our preventing the spread of a pandemic. Our focus is on a proposed hybrid model of alarm functions—as seen in Fig. 2.2—taking advantage of the scope of a cyber early warning system [53]. The study particularly emphasizes the decision-making capacity and formation of situational awareness of the Finnish government, the National Institute for Health and Welfare, and the Ministry of Social Affairs and Health. Specifically, we tackle the question of how to reduce the role of disinformation and misinformation in the state-level decision-making process. We explore how it is possible to use a hybrid emergency response model to solve multiple problems around crisis management, especially when several threats occur at the same time. For example, the combined crises of a coronavirus pandemic and cyberattacks can easily overload public safety organizations' workflow. Preventing the domino effect can become still more challenging, if separate or overlapping problem-solving methods are used in crisis management.

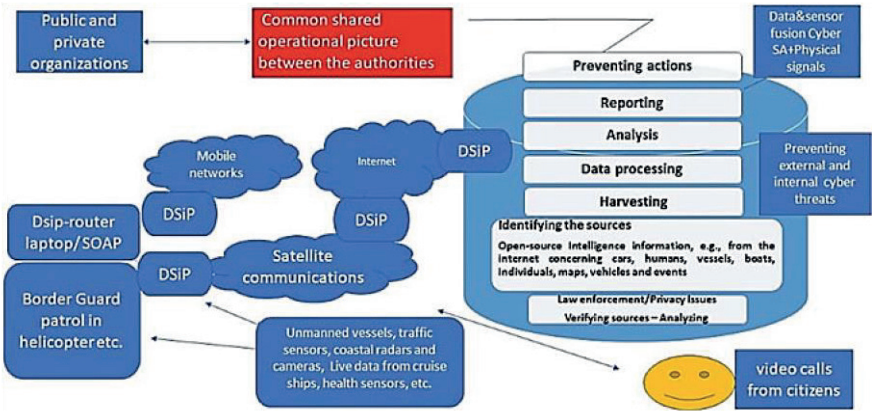
Public and private organizations
Common shared operational picture between the authorities
Data&sensor fusion Cyber SA+Physical signals
Preventing actions
Reporting
Analysis
Data processing
Harvesting
Mobile networks
Internet
DSiP
DSiP
DSiP
DSiP
Dsip-router laptop/SOAP
Satellite communications
Preventing external and internal cyber threats
Identifying the sources
Open-source Intelligence information, e.g., from the internet concerning cars, humans, vessels, boats, individuals, maps, vehicles and events
Law enforcement/Privacy Issues
Verifying sources – Analyzing
Border Guard patrol in helicopter etc.
Unmanned vessels, traffic sensors, coastal radars and cameras, Live data from cruise ships, health sensors, etc.
video calls from citizens

Fig. 2.2 Hybrid emergency response model (HERM)

2.3 Challenges in the Decision-Making Process with COVID-19

As the COVID-19 pandemic has shown, an international cross-border crisis can spread very quickly. It is thus crucial that decision-makers effectively share information—including around the fact that public safety organizations' preparedness levels are not sufficiently high.

2.3.1 *Situation in Finland*

Finland's citizens noted an enormous lack of correct information around COVID19 at the end of February 2020 [62, 65]. Ministers and responsible authorities failed to immediately offer guidelines for controlling COVID-19. In March 2020, the ministers of social affairs and health did not know how the tasks should be divided between them [20, 31]. Several countries recommended the use of protective masks. Following this, the National Emergency Supply Agency argued that it did not have enough protective masks in stock. Finland did not recommend the use of masks [28], and the masks were later reported to be out of date [35]. Eventually, the Ministry of Social Affairs and Health began to order the masks, but they did not pass the test carried out by VTT Technical Research Centre of Finland [61]. The manager of the Ministry of Social Affairs and Health and The Finnish Institute for Health and Welfare (THL) also held a different view, regarding the benefits of using masks [39, 44]. THL recommended the use of masks, but the Ministry of Social Affairs and Health doesn't.

At present, our government employs more political assistants than ever before [56]. Managing the administration is thus becoming cumbersome. State leaders need decision-making support, such as via artificial intelligence tools, to enhance administrative efficiency. External pressure has had marginal effects on the overall decision-making process, except for in the case of a few decision-makers [64]. Information about the pandemic has been made available for the decision-makers, but the response has been slow and little scientific information from abroad has been shared with the public.

In Finland, the guidelines set by the WHO have been interpreted from a national political perspective. Exceptional conditions were imposed, including a separate regional movement restriction, on the Uusimaa region. The purpose was to prevent the COVID-19 from spreading outside the metropolitan area. Despite that, it was possible to fly relatively freely between Finland and other countries for months. The classification of pandemic countries, based on disease quantity, was incomplete. Statements made by a few doctors about the development of the COVID-19 pandemic have also posed challenges to forming a coherent picture of the situation [18, 34]. They believe that by letting the coronavirus rip through the population to infect people, it is possible to achieve so-called herd immunity.

The decisions made by various Nordic countries to prevent the spread of COVID19 have differed and continue to differ. This is also true amongst EU member countries. Sweden began to seek herd immunity for its citizens and allowed the disease to spread almost freely [21]. Finland started by following the Swedish COVID-19 strategy, but its selected strategy changed after the president intervened in the government's decision-making process [64]. After considering the situation—as well as the grounds for declaring a state of emergency by the President of the Republic and the government—the government announced a state of emergency in Finland on 16 March, 2020 [23]. The Finnish Parliament applied the Emergency Powers Act on 18 March, 2020. Regional restrictions were then put into effect, preventing needless travel among the country's regions [60].

Only one technical solution is currently in use for COVID-19 prevention. The Finnish Corona Blinker, "Koronavilkku"—an application developed by Solita and the Finnish Institute for Health and Welfare—was released in August 2020 [54]. Soon after, crucial problems were found in the app's ability to track infected people. When a person infected with coronavirus reported their infection to the app, the warning failed to reach other users of the app. Another crucial problem was the delay between a user reporting an infection and the app's recording of it. A one week delay slows or prevents infection chain tracing [63]. Another challenge to infection tracing is that users do not have to inform the app when they learn they have COVID-19.

There is also an online service called "omaolo". You can do an online medical check-up for COVID-19 symptoms on the internet, if you suspect you have a coronavirus infection [8]. It is free of charge and the service guides the patient to take a test or go to a hospital, if there is a need.

2.3.2 Case Vastaamo

As mentioned above, tens of thousands of patient records were stolen from the Finnish psychotherapy center Vastaamo [40]. Criminals can use stolen personal data in many ways. For example, they can try to blackmail or otherwise influence the victims. Finland's National Bureau of Investigation (KRP) has received over a thousand reports of offenses connected to the hacking and blackmailing case revolving around Vastaamo [41].

Kanta produces digital services for the social welfare and healthcare sector in Finland. According to [30], each organization associated with Kanta services has at least one Kanta-access point. Access to the service can either be carried out as an organization's activity or implemented by the organization. That means, the Kanta subscriber has an integration solution through which several systems, organizational units, or organizations are connected to the Kanta services. The purpose of the integration solution is to route messages to application servers that may be located in different organizational units or organizations. It is also possible to connect to the service via an external access point. In this model, the organization has joined the Kanta services through a Kanta access point implemented by an intermediary.

The organization may have externalized information system (e.g., a shared information system as a SaaS), messaging, and/or communications to an intermediary. There can be several access points (and server certificates) if, for example:

- the organization's units are directly connected to Kanta services from different information systems, without a centralized integration solution (messaging solution);
- the organization's reception services (for example, receipt of renewal requests) are located on a server other than that from which its systems connect to Kanta services [30].

Valvira is a national agency operating under the Ministry of Social Affairs and Health. Vastaamo is a service provider approved and supervised by Valvira. Its information system is part of the Category B systems regulated by law, for which the law does not require an external assessment of data security. Vastaamo's patient information system was developed by Vastaamo itself. It is one of 260 social and health care information systems that are monitored by the authorities only if there are particular information security-related reasons to suspect problems, or if the service provider requests it [48].

Class B patient information systems are registered with Valvira under the Customer Information Act. They may be purchased as commercial products or manufactured by the company itself. According to Valvira, their monitoring is very limited due to resource problems. It is possible that patient information from Kanta could also be stored in a private register, allowing just one healthcare professional at a time—and one who is in a care-giving role with the patient—to process patient data.

2.4 Central Concepts

This section introduces the central concepts related to the research framework and defines the meaning of the concepts, and used terminology.

2.4.1 Artificial Intelligence

Artificial intelligence (AI) is part of a system that engages in intelligent behavior by analyzing the environment and taking multiple actions—with a dimension of autonomy—to achieve specific goals [9]. AI-based systems can be software-based and act in the virtual world (e.g., image analysis software, search engines, shape and face recognition systems). AI can also be embedded in hardware devices (e.g., advanced robots, autonomous cars, unmanned vehicles, drones or Internet of Things applications) [9].

An *Intelligent Agent* (IA) is an entity that produces decisions. This allows, for example, for the performance of specific tasks for users or applications. An IA has the ability to learn during the process of performing tasks. Its two main functions are perception and action. Intelligent Agents form a hierarchical structure that comprises different levels of agents. A multi-agent system is one that consists of a number of agents interacting with one another [58] in combinations that can help solve challenging societal problems. An IA can behave in three ways: reactively, proactively, and socially [58].

2.4.2 Legislation and Regulation

Per the Emergency Powers Act, if Finland's government—in liaison with the President of the Republic—finds that exceptional circumstances exist in the country, a government decree can be issued to apply the provisions of this act (commissioning regulation). Said decree may be issued for a fixed period [13].

The ISO/IEC 27001 formally specifies an Information Security Management System (ISMS). This comprises a suite of activities concerning the management of information risks called "information security risks" in the standard ISO [27]. Information security management is an essential part of management, which should be supported by the management system. Information security ensures the confidentiality of information, as well as its availability and integrity.

ISO 27799:2016 defines guidelines for organizational information security standards and information security management practices—including the selection, implementation, and management of controls—taking into consideration the organization's information security risk environment(s). It defines guidelines to support the interpretation and implementation of the health informatics of the ISO/IEC 27002 and is a companion to the international standard ISO [26].

ISO/IEC 27032:2012 guides enhancing the state of cybersecurity, along with drawing out the unique aspects of that activity and its dependencies on other security domains—in particular: information, network, internet security, and critical information infrastructure protection (CIIP) ISO [24].

ISO/IEC 9001:2015 provides practical guidance on managing the total service produced for the customer. It also enables the healthcare organization to demonstrate that it meets customer satisfaction requirements and develops customer satisfaction by managing the risks of the operating environment International Organization for Standardization [25].

2.4.3 Situational Awareness

The Ministry of Defence of Finland [45] describes situational awareness as decision-makers' and their advisors' understanding of what has happened, the circumstances under which it has happened, the goals of the different parties, and the possible development of events. All of these are needed to make decisions on a specific issue or range of issues. A general definition of situational awareness is the perception of the elements in the environment within time and space, the comprehension of their meaning, and the projection of their status into the near future [12].

According to [14], cyber situational awareness is a subset of situational awareness—it comprises the part of situational awareness that 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 that can be interpreted directly by the decision-maker.

2.4.3.1 Command and Control

A command center is any place that is used to provide a centralized command for some purpose. An incident *command center* is located at or near an incident, to provide localized on-scene command and support from the incident commander. Mobile *command centers* may be used to enhance emergency preparedness and back up fixed command centers. Command centers may also include Emergency Operations Centers (EOC) or Transportation Management Centers (TMC).

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—whether 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 [16].

According to [16], SCADA systems' components may involve operating equipment such as valves, pumps, and conveyors that are controlled by energizing actuators or relays. Local processors communicate with the site's instruments and operating equipment—including a Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Device (IED), and Process Automation Controller (PAC). A single local processor may be responsible for dozens of inputs from instruments and outputs to operating equipment. SCADA also consists of instruments in the field or a facility that sense conditions such as power level, flow rate, or pressure. Short-range communications involve wireless or short cable connections between local processors, instruments, and operating equipment. Long-range communications between local processors and host computers cover a wide area—using such methods as satellites, microwaves, frame relays, and cellular packet data. The host computer acts as the central point of monitoring and control. This is where a human operator can supervise the process, as well as receive alarms, review data, and exercise control. The system may consist of automated or semi-automated processes. A Networked Control System (NCS) is a control system where in the control loops are closed through a communication network. The defining feature of an NCS is that control and feedback signals are exchanged among the system's components, in the form of information packages, through a network CSPC [4, 49].

RIDM is a risk-based decision-making process that provides a defensible basis for making decisions. It also helps to identify the greatest risks and to prioritize efforts to minimize or eliminate them. Risk-informed decision-making (RIDM) is a deliberative process that uses a set of performance measures, together with other considerations, to "inform" decision-makers' choices [66, 36].

2.4.3.2 Management of Situational Awareness at the National Level

The Ministry of Finance of Finland is responsible for the steering and development of the state's information security [45, 50]. Government situation centers ensure that Finland's state leaders and central government authorities are kept continuously informed. Finland's government situation centre was set up in 2007. It is responsible for alerting the government, permanent secretaries, and heads of preparedness—and for calling them to councils, meetings, and negotiations at exceptional times—as required by a disruption or a crisis.

The ministries must submit the situational picture for their entire administrative branch to the government situation center and notify the center of any security incidents in their field of activity. In urgent situations, the government situation center also receives incident reports for security incidents directly from the authorities. The government situation center also follows public sources and receives situational awareness information, in its role as the national focal point for certain institutions of the European Union and other international organizations.

2.4.4 Elements of Critical Infrastructure

Very often, Critical Infrastructure is defined from the view of the public sector despite it also consists private personnel and their activities as well as public operators of assets, systems, and networks. A very common public-private partnership approach ensures cooperation and information exchange intended to protect vital functions of the society. The human, physical and cyber assets provide many critical services that are necessary for a secure society.

2.4.4.1 Classification of the Critical Infrastructure in the United States

In the United States, critical infrastructure refers to those systems and assets, whether physical or virtual, that are deemed so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health, or safety, or any combination of those matters [46].

The U.S. Department of Homeland Security identifies 16 different sectors for the classification of critical infrastructure [7]:

1. Chemical,
2. Commercial facilities,
3. Communications,
4. Critical manufacturing,
5. Dams,
6. Defense industrial base,
7. Emergency services,
8. Energy,
9. Financial services,
10. Food and agriculture,
11. Government facilities,
12. Healthcare and public health,
13. Information technology,
14. Nuclear reactors, materials, and waste,
15. Transportation systems, and
16. Water wastewater system

Cyber threats—such as, for example, phishing attempts, blackmailing attempts, and hacking incidents—are an ever-changing threat to cyber systems across the sectors.

According to the National Institute of Standards and Technology NIST [38], the framework applied in the U.S. is also well suited to Finland. The risk management framework consists of three elements of critical infrastructure (physical, cyber, and human), which are explicitly identified and should be integrated throughout the steps of the framework. The critical infrastructure risk management framework supports a decision-making process, which critical infrastructure actors or partners collaboratively undertake to inform their 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 [7].

The risk management concept enables the critical infrastructure actors to focus on those threats and hazards that are likely to cause harm and to 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 the continuity of essential functions and services and support enhanced response and restoration [7].

According to the Department of Homeland Security [7], the first point recommends setting *infrastructure goals and objectives*, which 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 the provision of essential services.

The third point recommends *assessing and analyzing risks*. These risks may comprise threats, vulnerabilities, and consequences. A threat can be a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. Vulnerability-based risk may occur due to a 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, implies 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 [7].

2.4.4.2 Smart Grid System and the Internet of Things

The Internet of Things (IoT) connects systems, sensors, and actuator instruments to the broader internet. The IoT allows things to communicate and exchange control data and other necessary information, while executing applications towards a machine goal [11].

The idea of the Internet of Things was developed in parallel to Wireless Sensor Networks (WSN). Sensors are everywhere: in our vehicles, in our smartphones, in factories controlling CO_2 emissions, and even in the ground monitoring soil conditions in vineyards. A WSN can generally be described as a network of nodes that cooperatively sense and may control the environment, enabling interaction between persons or computers and the surrounding environment. The development of WSNs was inspired by military applications—notably, for surveillance in conflict zones [2].

The Internet of Things is an emerging paradigm of internet-connected things that allows physical objects or things to connect, interact, and communicate with one another—similarly to the way humans talk via the web in today's environment. It connects systems, sensors, and actuator instruments to the broader internet [11].

The IoT allows things to communicate and exchange control data and other necessary information, while executing applications towards machine goal. The Internet of Things (IoT) is also impacted by the industrial sector, especially for industrial automation systems in which internet infrastructure makes it possible to gain extensive access to sensors, controls and actuators, with the intention of increasing efficiency [11].

Cybersecurity risks should be addressed as organizations implement and maintain their smart grid systems. According to the National Institute of Standards and Technology NIST [37], the smart grid system provides the most efficient electric network operations based on information received from consumers.

A smart grid system may involve a discrete IT 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), including SCADA systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLCs) [5, 37].

The Industrial Internet of Things (IIOT) collects data from connected devices(i.e., smart connected devices and machines) in the field or plant. It then processes this data, using sophisticated software and networking tools. The entire IIOT requires a collection of hardware, software, communications and networking technologies [11].

2.4.4.3 Intelligence Solutions for Public Safety Organizations

Open-Source Intelligence (OSINT) 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. 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 ATP [1, 17, 43].

Social Media Intelligence (SOCMINT) identifies social media content in particular as both a challenge and opportunity for open-source investigations [55]. BigData is associated with OSINT and includes processes for the analysis, capture, research, sharing, storage, visualization, and safety of information. Big Data offers the ability to map standards of behavior and tendencies [47]. The availability of worldwide satellite photography, often of high resolution, on the web (e.g., Google Earth Pro) has expanded open-source capabilities into areas formerly available only to major intelligence services [14]. In the proposed hybrid emergency response model [52, 53] OSINT and SOCMINT features are integrated into the automated HERM as a part of an AI-driven decision support tool.

Threat information is any information related to a threat, which might help an organization protect itself against a threat or detect the activities of an actor [29]. Indicators are used to detect and defend against threats. These include the(IP)address of a suspected command and control server, a suspicious Domain Name System (DNS) domain name, or a Uniform Resource Locator that references malicious content. Tactics, techniques, and procedures (TTPs) describe the behavior of an actor. TTPs could describe an actor’s tendency to use a specific malware variant, order of operations, attack tool, delivery mechanism, or exploitative strategy. Security alerts are vulnerability notes. Threat Intelligence reports are documents describing threat-related information that is transformed, analyzed, or enriched to provide important context for the decision-making process. Tool configurations are recommendations for using mechanisms that support the automated collection, exchange, processing, analysis, and use of threat-related information. They may comprise information on how to install and use a rootkit detection utility or on how to create, for example, router access control lists (ACLs) [29].

2.5 Previous Works

The multi-methodological approach that has been used in previous studies [52, 53] consists of four case study research strategies [42]:

1. theory building,
2. experimentation,
3. observation, and
4. systems development.

[59] 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.

According to [22] (Chap. 2), information systems and organizations are complex, artificial, and purposefully designed. Such a problem-solving paradigm must lead to an artifact that solves the identified problem. This review concentrates on comparing how the proposed emergency model [52, 53] suits a pandemic situation in which information warfare is an ongoing process. Scientific publications, articles, and literary material have been comparatively reviewed with this aim. The review subject comprises the public safety organizations, procedures, and vital functions of Finland society.

The first purpose of this qualitative review was to analyze pandemic-related management and information-sharing risks, along with the formation of situational awareness, from the view of continuity management. We apply the modified risk assessment framework in this review. The second purpose was to find any hidden administrative and managerial-related state-level risks that are outside the official risk classification. A simple process model helps identify those fundamental hidden management-related factors that affect to the implementation process of the next-generation emergency response model proposed by [52].

2.6 Findings

In Finland, as we have seen, more than one factor influences the decision-making process at the state level. We have local and regional level administrations that form situational awareness from the view of their territorial region; decision-makers then share regional instructions and guidelines with the people. There are local corona teams that are responsible for regional security. Currently, tasks are separate from the government at the regional level and the members of the government do not give absolute commandments, such as mandatory instructions for using masks. Yet the continued lack of clarity around the workflow is a crucial barrier, when the purpose is to share relevant information with the right audience at the right time. It has been seen previously that labor movement or trade unionism can produce an agitating counterforce, by means that are not ethically valid. If the challenges to fighting the COVID-19 pandemic emerge from the nation's citizens, then the fundamental problems lie more deeply within the constructs of society.

Finland does not have an operative command and control institution for unexpected crises. The president of Finland leads foreign policy with the government, but there is no operative commander role for the president in the country's internal affairs. The ongoing COVID-19 crisis has shown that there is a lack of information exchange—both between the authorities and between the authorities and politicians. Yet citizens have likewise been kept unaware of the guidelines that should be followed. For small- or medium-sized social and healthcare companies, information security is based on self-monitoring. Public healthcare organizations also base their oversight of these operations on self-monitoring. The National Supervisory Authority for Welfare and Health (Valvira) supervises, for example, private sector licensing, healthcare, social welfare, legal protection, legal rights, and technologies [57]. A single staff member is responsible for supervising all issues like information security and privacy protection, around the Kanta-register [19].

This is not enough—especially since criminals may use private information in a variety of extremely dangerous ways. For example, criminals may try to affect the decision-making process by blackmail. A major information-sharing problem seen in the Vastaamo case was the fact that a data breach had occurred nearly two years before it was detected. There are no crucial privacy issue-related barriers to using the proposed hybrid emergency response model within a smart city infrastructure. When an alarm-based early warning procedure for data leakage is automatized, it offers possibilities to enhance privacy protection and other protective functions [51]. The proposed hybrid emergency response solution may also use sensors called flu-sensors, which can transfer data in real time from a public area—for example, from a shopping center—to the Hybrid Emergency Response Center. Data about virus particles might then indicate a need for mall closure, the early warning would allow this to be carried out immediately.

2.7 Discussion and Conclusions

By comparing different countries, crucial factors influencing the formation of information sharing can be found. For example, Finland is almost the only country in Europe that does not use scientist experts as advisors in the decision-making process at the state level. If decision-makers keep their eyes open, they can find massive amounts of research from foreign sources on how the coronavirus spreads and how its spread can be prevented.

First, there is a fundamental need to regulate new guidelines for the higher level crisis management and command relationships for exceptional circumstances.

Temporary provisions should be made for emergency situations, which may require imposing restrictions on citizens. There must be one incident team whose leader is from the central government. This leader should take control when adjutants and instructors have too much information to share, since it is difficult to gather the correct information from a large amount of the data in a time of crisis. To date, there have been too many assistants involved in the decision-support mechanism at the state level.

In the future, it is necessary to begin using artificial intelligence solutions to support decision-making. The proposed next-generation hybrid emergency model uses artificial tools to generate information for decision-makers. Algorithm-based decision-support and decision-making mechanisms make the system effective. As Fig. 2.3 illustrates, the crucial factors in the hybrid risk management framework are risk-informed decision-making (define risks and information), continuity risk management (handle risks continuously), and hybrid emergency response solutions (emergency operations). Because human beings are still decision-makers, people are responsible for the decisions they have made. Yet it is possible to combine human-based guidelines for risks and AI-driven decision-making [6].

This solution offers two possibilities to use automation. At the first level, automated protection functions are connected to semi-public spaces (e.g., shopping centers) and public open places (e.g., gardens). For example, a health sensor called “flu” may start an evacuation process if it observes several deviations from the guideline values. At the second level, an AI-aided decision support mechanism outputs analytical reports for the state level decision-makers. This level will greatly enhance the decision-making process, since the need for assisting staff will be reduced in high-level decision-making.

As mentioned above and illustrated in Fig. 2.4, the authorities’ information sharing process must move towards automated functions. Still, it is an important western tradition that a parliament is democratically elected by the country’scitizens.

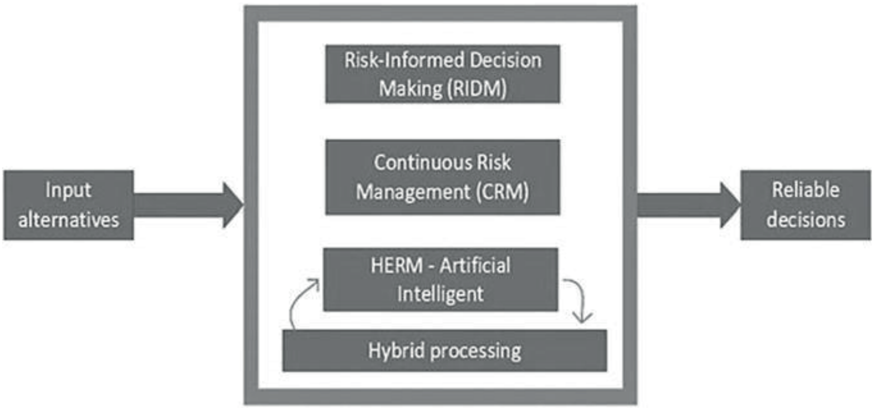
Input alternatives
Risk-Informed Decision Making (RIDM)
Continuous Risk Management (CRM)
HERM - Artificial Intelligent
Hybrid processing
Reliable decisions

Fig. 2.3 Reliable decision-making process

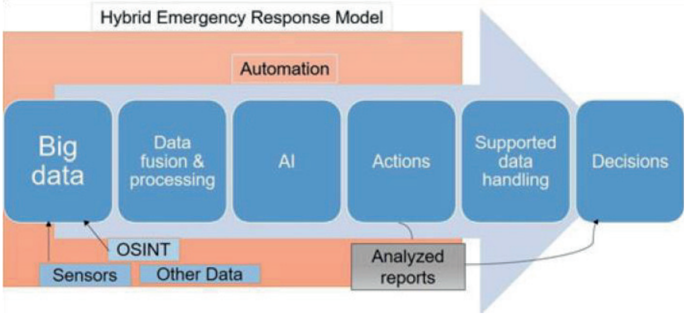

Fig. 2.4 HERM with artificial intelligence

At present, politicians' desire to maintain high levels of control over their decision-making ability may prevent the utilization and usefulness of the proposed smart hybrid emergency model. Many decision-makers want political aspects and opinions to be more represented than rational decisions. Yet Finland's politicians and other high-level decision-makers should take into consideration that cyber preparedness, operational preparedness, and reliability of decision-making are not separate parts of continuity management.

It is possible to combine operational, management, and strategic level decision support functions into a single entity. This does not mean combining all elements in one physical location. If fundamental risk factors—such as a pandemic that presents domino effects from many angles—are not recognized, then technical early warning solutions become useless. It is thus a fundamental societal requirement that a decision support mechanism be developed in jointly with the crisis management system.

It is not enough for the government of Finland to use just one international source (WHO), when they try to maintain the international level of situational awareness. Legislation around privacy issues does not cause permanent obstacles to using sensing elements (e.g., sensors) in the hybrid emergency response model. It is necessary to rationalize organizational responsibilities, for the development of overall security. A human is an individual with limited observation capability and overlapping data transmission limits the effective cooperation between politicians and authorities.

HERM’s nearly tireless data handling and transmission capacity can help prevent communication problems among the authorities. Embedding preventive functions against unexpected threats in the emergency response model is an essential part of overall security, in situation awareness management and critical infrastructure protection. In particular, the analysis of global research data regarding COVID-19 can be automated. We need more detailed, standardized information systems and rules for all information systems that handle sensitive information. All that is needed is the political will to exploit intelligence solutions.

The ongoing and tremendously challenging COVID-19 crisis requires us to powerfully leverage our common will—to change the dream of digitalization into concrete actions. The proposed model for smart cities offers solutions to many problems and

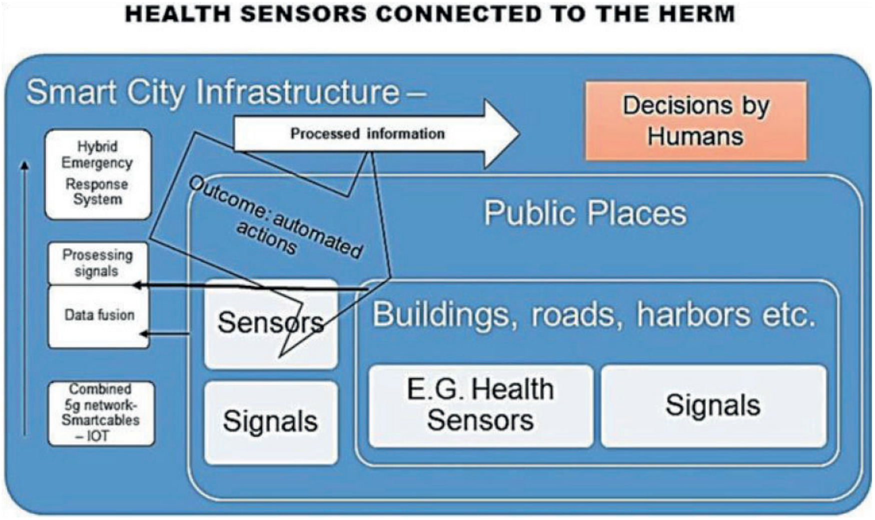
HEALTH SENSORS CONNECTED TO THE HERM
Smart City Infrastructure –
Processed information
Decisions by Humans
Hybrid Emergency Response System
Outcome: automated actions
Public Places
Prosessing signals
Data fusion
Sensors
Buildings, roads, harbors etc.
Combined 5g network-Smartcables – IOT
Signals
E.G. Health Sensors
Signals

Fig. 2.5 Predictive health sensors in a smart city

questions, as Fig. 2.5 shows. The model may use health sensors, as well as traffic sensors, in a predictive way.

References

1. ATP (2012) Open-source intelligence. Army Techniques Publication No. 2–22.9, Department of the Army, Washington, DC
2. Bröring A, Echterhoff J, Jirka S, Simonis I, Everding T, Stasch C, Liang S, Lemmens R (2011) New generation sensor web enablement. Sensors 11(3):2652–2699
3. Buranyi S (2020) The WHO v coronavirus: Why it can´t handle the pandemic. The Guardian, https://www.theguardian.com/news/2020/apr/10/world-health-organization-who-vcoronavirus-why-it-cant-handle-pandemic. Accessed 10 Dec 2020
4. CSPC (2014) Securing the U.S. electrical grid. Center for the Study of the Presidency &Congress
5. Chong C, Kumar S (2003) Sensor networks: Evolution, opportunities, and challenges. ProcIEEE 91(8):1247–1256
6. Colson E (2019) What AI-driven decision making looks like. Harvard Business Review, https:// hbr.org/2019/07/what-ai-driven-decision-making-looks-like. Accessed 10 Dec 2020
7. DHS (2013) NIPP 2013: Partnering for critical infrastructure security and resilience. U.S.DepartmentofHomelandSecurity,https://www.cisa.gov/publication/nipp-2013-partnering-criticalinfrastructure-security-and-resilience
8. DigiFinland (2020) Welcome to take care of your health and well-being in Omaolo. DigiFinland Oy, https://www.omaolo.fi/. Accessed 10 Dec 2020
9. EC (2018) Artificial intelligence for Europe. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2018) 237, European Commission
10. EC (2020) Coronavirus: commission delivers first batch of 1.5 million masks from 10 million purchased to support EU healthcare workers. Press release, European Commission
11. ElecTech (2016) Internet of Things (IOT) and its applications. Electrical Technology, http://www.electricaltechnology.org/2016/07/internet-of-things-iot-and-its-applications-inelectrical-power-industry.html. Accessed 8 Nov 2016
12. Endsley MR (1988) Design and evaluation for situation awareness enhancement. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 32(2):97–101
13. Finlex (2011) Emergency powers act 1552/2011. Finnish Ministry of Justice
14. Franke U, Brynielsson J (2014) Cyber situational awareness: A systematic review of the literature. Comput Secur 46:18–31
15. GPMB (2019) A world at risk: Annual report on global preparedness for health emergencies.Global Preparedness Monitoring Board
16. Gervasi O (2010) Encryption scheme for secured communication of web-based control systems.Journal of Security Engineering 7(6):609–618
17. Glassman M, Kang MJ (2012) Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Comput Hum Behav 28(2):673–682
18. Harjumaa M (2020) HUSin Järvinen purkaisi koronarajoituksia: ”Pitäisi yrittää saada sitäväestönosaa sairastamaan, jolle tauti ei todennäköisimmin ole vaarallinen”. Yle, https://yle.fi/ uutiset/3-11318716. Accessed 10 Dec 2020

19. Hautanen S (2020) IS: Yksi mies vastaa 260 sote-yrityksen tietoturvan valvonnasta. Verkkouutiset,https://www.verkkouutiset.fi/is-yksi-mies-vastaa-260-sote-yrityksen-tietoturvan-valvonnasta/#2fb860b4. Accessed 10 Dec 2020
20. Hemmilä I, Salminen V (2020) Oikeuskansleri moittii ministeriöiden yhteistyötä kevväänsuojavarustehankinnoissa—STM:ssä epäselvyyttä myös ministerien työnjaosta. Suomenmaa,https://www.suomenmaa.fi/uutiset/oikeuskansleri-moittii-ministerioiden-yhteistyota-kevaansuojavarustehankinnoissa-stmssa-epaselvyytta-myos-ministerien-tyonjaosta-2/. Accessed 4 Dec 2020
21. Henley J (2020) Sweden's Covid-19 strategist under fire over herd immunity emails.TheGuardian,https://www.theguardian.com/world/2020/aug/17/swedens-covid-19-strategist-under-fireover-herd-immunity-emails. Accessed 10 Dec 2020
22. Hevner A, Chatterjee S (2010) Design research in information systems: theory and practice.Springer
23. HkiTimes (2020) Finland to close borders to non-essential travel at 12 am on Thursday.HelsinkiTimes, https://www.helsinkitimes.fi/finland/finland-news/domestic/17450-finlandto-closeborders-to-non-essential-travel-at-12am-on-thursday.html. Accessed 10 Dec 2020
24. ISO (2012) ISO/IEC 27032:2012: Information technology, security techniques, guidelines for cybersecurity. International Organization for Standardization (ISO), https://www.iso.org/standard/44375.html
25. ISO (2015) ISO 9001:2015: Quality management systems, requirements. International Organization for Standardization (ISO), https://www.iso.org/standard/62085.html
26. ISO (2016) ISO 27799:2016 Health informatics, information security management in health using ISO/IEC 27002. International Organization for Standardization (ISO), https://www.iso.org/standard/62777.html
27. ISO (2017) ISO/IEC 27001: Information security management systems. International Organization for Standardization (ISO), https://www.iso.org/isoiec-27001-information-security. html
28. Jaskari K (2020) Ministeriö ei aio jatkossakaan suositella kangasmaskien käyttöä julkisillapaikoilla. Yle, https://yle.fi/uutiset/3-11305744. Accessed 10 Dec 2020
29. Johnson C, Badger L, Waltermire D, Snyder J, Skorupka C (2016) Guide to cyber threat information sharing. NIST Special Publication 800–150, National Institute of Standards and Technology (NIST)
30. Kela (2020) Tekniset liittymismallit Kanta-palveluihin. Ohje, Kanta-palvelut, Kela, https://www.kanta.fi/documents/20143/106828/Tekniset+liittymismallit+Kanta-palveluihin.pdf/a057c34a-f822-71fd-b2df-097245d582ee
31. Lakka P (2020) IS selvitti Pekosen ja Kiurun ministeriön kaaosta—ainakin nämä 5 syytävaikuttivat taustalla: ”Suksi lipsunut koko matkan”. Ilta-Sanomat, https://www.is.fi/politiikka/ art2000006482234.html. Accessed 10 Dec 2020
32. Lehto M, Limnéll J, Innola E, Pöyhönen J, Rusi T, Salminen M (2017) Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017, Valtioneuvoston kanslia
33. Lyngaas S (2020) Why the extortion of Vastaamo matters far beyond Finland—and how cyber pros are responding. CyberScoop, https://www.cyberscoop.com/finland-vastaamo-hackresponse/. Accessed 10 Dec 2020
34. Mediuutiset (2020) Lääkäri: Aletaan tartuttaa koronaa hallitusti hoitohenkilökuntaan immuniteetin saamiseksi. Mediuutiset, https://www.mediuutiset.fi/debatti/laakari-aletaan-tartuttaakoronaa-hallitusti-hoitohenkilokuntaan-immuniteetin-saamiseksi/dfbc96a4-c757-44e9-988 d38cf093a7e8b. Accessed 5 May 2020

35. Mäntymaa E, Mäntymaa J (2020) Sairaalat saivat varmuusvarastoista vuosia sitten vanhentuneita hengityssuojaimia—"Ihan kuranttia ei kaikki tavara ole ollut", sanoo HUS-johtaja. Yle, https://yle.fi/uutiset/3-11286164. Accessed 10 Dec 2020
36. NASA (2010) Risk-informed decision making handbook (NASA/SP-2010-576). Technical report,NASA. https://ntrs.nasa.gov/api/citations/20100021361/downloads/20100021361.pdf. Accessed 10 Dec 2021
37. NIST (2010) Guidelines for smart grid cybersecurity. In: Privacy and the smart grid, vol 2. NISTIR 7628, National Institute of Standards and Technology (NIST)
38. NIST (2018) Framework for improving critical infrastructure cybersecurity. Version 1.1,National Institute of Standards and Technology (NIST)
39. Natri S (2020) THL:n pääjohtaja kehottaa suomalaisia pukemaan kangasmaskin julkisillapaikoilla—"Näin oireeton tartuttaja suojelee muita". Yle, https://yle.fi/uutiset/3-11305102. Accessed 10 Dec 2020
40. NewsNowFin (2020) Maria Ohisalo: Vastaamo cyber attack and blackmail demands "serious, outrageous and cowardly". News Now Finland, https://newsnowfinland.fi/crime/mariaohisalo-vastaamo-cyber-attack-and-blackmaildemands-serious-outrageous-and-cowardly. Accessed 10 Dec 2020
41. NewsNowFin (2020) Vastaamo hacking and blackmail: 25,000 police reports filed. News NowFinland, https://newsnowfinland.fi/crime/vastaamo-hacking-and-blackmail-25000-police-reports-filed. Accessed 10 Nov 2020
42. Nunamaker J Jr, Chen M, Purdin T (1990) Systems development in information systems research. J Manag Inf Syst 7(3):89–106
43. Nurmi P (2015) OSINT: Avointen lähteiden internet-tiedustelu. Kehitysprojektin raportti,Aaltoyliopisto
44. Ollila A (2020) Lääkintöneuvos Pälve tyrmää Kirsi Varhilan näkemykset maskien käytönesteistä. Uusi Suomi, https://puheenvuoro.uusisuomi.fi/aveollila1-2/laakintoneuvos-palve-tyr maakirsi-varhilan-nakemykset-maskien-kayton-esteista/. Accessed 10 Dec 2020
45. PM (2010) Yhteiskunnan turvallisuusstrategia: Valtioneuvoston periaatepäätös 16.12.2010. Puolustusministeriö, Helsinki
46. PPD (2013) Critical infrastructure security and resilience. Presidential Policy Directive PPD21, U.S. White House Office
47. dos Passos DS (2016) Big Data, data science and their contributions to the development of the use of open source intelligence. Electronic Journal of Management & System 11(4):392–396
48. Ranta E (2020) Tällainen yritys on tietomurron kohteeksi joutunut Vastaamo. Ilta-Sanomat, https://www.is.fi/taloussanomat/art-2000006699437.html. Accessed 30 Nov 2020
49. Robles RJ, Kim T (2010) Communication security for SCADA in smart grid environment.In: DNCOCO'10: proceedings of the 9th WSEAS international conference on data networks, communications, computers,pp36–40.WorldScientificandEngineeringAcademyandSociety (WSEAS), Stevens Point, WI
50. SecComm (2017) Security Strategy for Society. Government resolution, Security Committee, Helsinki
51. Simola J (2020) Privacy issues and critical infrastructure protection. In: Benson V, Mcalaney J (eds) Emerging Cyber Threats and Cognitive Vulnerabilities. Academic Press, pp 197–226
52. Simola J, Rajamäki J (2017) Hybrid emergency response model: improving cyber situational awareness. In: Scanlon M, Le-Khac N (eds) ECCWS 2017—proceedings of the 16th European conference on cyber warfare and security. Academic Conferences and Publishing International, pp 442–451
53. Simola J, Rajamäki J (2018) Improving cyber situational awareness in maritime surveillance.In: Josang A (ed) ECCWS 2018—proceedings of the 17th European conference

on cyber warfare and security, pp 480–488. Academic Conferences and Publishing International

54. Solita (2020) The Finnish Covid-19 app Koronavilkku has been downloaded a million times already! Solita, https://www.solita.fi/en/the-finnish-covid-19app-koronavilkku-has-been-downloaded-million-times/. Accessed 10 Dec 2020
55. Trottier D (2015) Open source intelligence, social media and law enforcement: Visions, constraints and critiques. Eur J Cult Stud 18(4–5):530–547
56. Uosukainen R, de Fresnes T (2020) Poliitikot tulevat ja menevät, virkamiehet pysyvät—käynnissä on kamppailu siitä kenellä valta on. Yle, https://yle.fi/uutiset/3-11186910. Accessed 10 Dec 2020
57. Valvira (2020) Organizational structure. Valvira, https://www.valvira.fi/web/en/valvira/organisational_structure. Accessed 20 Oct 2020
58. Wooldridge M (2009) An introduction to multiagent systems, 2nd ed. Wiley
59. Yin RK (2017) Case study research and applications: design and methods, 6th ed. SAGE, Thousand Oaks, CA
60. Yle (2020) Daily: Gov't not planning to extend Uusimaa border closure. Yle, https://yle.fi/uutiset/osasto/news/daily_govt_not_planning_to_extend_uusimaa_border_closure/11303010. Accessed 10 Dec 2020
61. Yle (2020) Finland: Chinese face masks fail tests. Yle, https://yle.fi/uutiset/osasto/news/finland_chinese_face_masks_fail_tests/11298914. Accessed 10 Dec 2020
62. Yle (2020) Finland's first coronavirus case confirmed in Lapland. Yle, https://yle.fi/uutiset/osasto/news/finlands_first_coronavirus_case_confirmed_in_lapland/11182855. Accessed 10 Dec 2020
63. Yle (2020) Friday's paper: problem with corona alert app, more countries on restricted list, .drugs in the countryside, Yle. https://yle.fi/uutiset/osasto/news/fridays_papers_problem_with_corona_alert_app_more_countries_on_restricted_list_drugs_in_the_countryside/11586606. Accessed 10 Dec 2020
64. Yle (2020) President Niinistö defends role in coronavirus crisis. Yle, https://yle.fi/uutiset/osasto/news/president_niinisto_defends_role_in_coronavirus_crisis/11303872. Accessed 12 Dec 2020
65. Yle (2020) Two possible coronavirus cases in northern Finland. Yle, https://yle.fi/uutiset/osasto/news/two_possible_coronavirus_cases_in_northern_finland/11173752. Accessed 10 Dec 2020
66. Zio E, Pedroni N (2012) Risk-informed decision-making processes: an overview. Foundation for an Industrial Safety Culture, Touloise, https://www.foncsi.org/fr/publications/cahierssecurite-industrielle/overview-of-risk informed-decision-making-processes/CSI-RIDM.pdf. Accessed 15 Dec 2020