Ethical Resilience Management Framework for Critical Healthcare Information Infrastructure

JYRI RAJAMÄKI, AARNE HUMMELHOLM
Leppävaara Campus
Laurea University of Applied Sciences
Vanha maantie 9, 02650 Espoo
FINLAND

Abstract: - The growing complexity of the digital ecosystem in combination with increasing global risks involves various ethical issues associated with cybersecurity and resilience. This paper offers a conceptual resilience governance framework and design aspects for ethical and resilient cyber-physical e-health and e-wellbeing systems. Our safety and security thinking has been based on a supposition that inside defensive walls we are safe. The focus of our actions has been controlling our own systems, improvement of protection, and staying inside the protection. However, nobody can control complex large integrated cyber-physical systems, but on the other hand, coordination and cooperation is a salient point. In e-health and e-wellbeing, this means that the focus is shifting from the control and securing of health and welfare data in a silo to using that data to promote health and wellbeing worldwide in our connected world. On the other hand, we have an ethical need to complement the existing security and risk management knowledge base by developing frameworks and models where we are using, for example, artificial intelligence systems that enable network-wide flexibility and resilience management that strive to maintain and improve critical operations.

Key-Words: - cloud services, cross-border healthcare, eHealth, healthy aging, SHAPES project, well-being

Received: April 18, 2021. Revised: January 27, 2022. Accepted: February 28, 2022. Published: April 4, 2022.

1 Introduction

Digitalization changes societies; especially the use of information and communication technology (ICT) in the health and wellbeing (H&W) sector effects on aging persons. Digital transformation and ecosystem thinking steer the Smart and Healthy Ageing through People Engaging in Supportive Systems (SHAPES) project that supports the wellbeing of the elderly at home. Ethical questions have always been crucial in H&W. The rapid dissemination of ICT makes some of those questions even more pressing making cybersecurity an important ethical dimension of the features of future H&W solutions ethical principles [1], [2].

This design science research (DSR) continues the work presented at the DIGILIENCE 2020 conference [3] going deeper into the ethical problem of how to design the level of trust that promotes to exchange of health data for promoting H&W of citizens. The Relevance Cycle of DSR bridges the contextual environment of the research project with the design science activities [4]. This DSR's environment is the e-health and e-wellbeing domain and ambient assisted living of elderly persons. The main problem concerning this DSR: The mental picture of cybersecurity should turn from "threat, crime, attack" to "trust" and willingness to share H&W information. The Rigor Cycle connects the design science activities with the knowledge base of scientific foundations, experience, and expertise that informs the research project [4]. The knowledge base of this study consists of (i) ethics of cybersecurity science [5], (ii) science and practice of resilience [6], [7] (iii) cybersecurity science [8], (iv) trust-building in the digital world [9], and (v) situational awareness in cyber systems [10]. The central Design Cycle iterates between the core activities of building and evaluating the design artifacts and processes of the research [4].

2 Ambient Assisted Living of Elderly Persons

Applications of intelligent sensor systems, analytical devices, telecommunication systems, and various information systems are very rapidly evolving and adaptable to people's daily activities and needs, including more efficient and intelligent home-related services. This development means that in the digital world, also elderly persons can be provided with more effective treatment methods that allow

them to live longer in their homes and live there better. Elderly persons can be provided with better home care and preventive healthcare. Elderly persons can easily carry portable sensors and intelligent devices on their bodies and wrists that relay their vital information to hospital systems in real-time, from which healthcare staff can track human vitality even in real-time.

At the same time, we must develop artificial intelligence (AI) which is gathering information through several types of communications systems (e.g. wireless sensor networks, wireless ad hoc networks, wireless mesh networks, and so on) over using different types of communication technologies (e.g. device-to-device, machine-to-machine, sensor-to actuators communications systems). All this kind of development together with artificial intelligence gives elderly persons better life and healthcare possibilities, now and in the future when they are living in their homes.

2.1 People in the Environment

The latest sustainable development systems and healthcare systems, which can also be used at home, improve the quality of life of special groups, including elderly persons. Such systems allow older people to stay alone at home for longer, to be more independent, and reduce hospital stays and time spent with doctors and healthcare. Internet of things (IoT) devices, actuators, and sensors can be used to improve the safety of the elderly lifestyle and home environment. Such developments are very important for the elderly and society as a whole, as the number of elderly persons is growing rapidly, as lifestyle changes in developed countries and improvements in the medical field increase the amount of the aging population. These innovations are used together with information and communication technologies to develop applications and services for elderly persons to help them in their needs of daily affairs.

As people, as well as the elderly, live in homes for much longer and healthier lives and their well-being is much better than before because of these new healthcare services, the development also requires health professionals to adapt and train in a new environment, so that they can use and manage they get from new technologies - and healthcare information and wellbeing information obtained from them so that they would make their treatment decisions as quickly and efficiently as possible. As applications for intelligent sensor systems, analytical equipment, telecommunications systems, and various information systems evolve rapidly and adapt to people's daily activities and needs, including more efficient and intelligent home services, we also need new types of service companies and companies to maintain home systems, who assist, maintain equipment and systems in this type of home environment. In all these activities, they must take into account the privacy and cyber and information security requirements of the newer EU directives (GPDR, MDR, and NIS). In these new sustainable development systems and healthcare systems, we must also take care of ethical and moral issues concerning developing and using these new services.

These new sustainable development systems and healthcare systems will also give relatives a better way to monitor the health status and wellbeing of their elderly. This opportunity also poses challenges for healthcare systems in the sharing of healthcare patient data, as these must take into account privacy, information, and cybersecurity issues, even if the patient's healthcare information is provided to the patient's relatives. In this situation, we must also take care of ethical and moral issues concerning the patient's healthcare information and which way we give this information to the patient's relatives.

2.2 Organizational Systems

The social and health authorities' organizations in Finland are 1) national healthcare systems, 2) The Social Insurance Institution, and 3) National Health Care Research Institute. Patient healthcare information is also shared with social and healthcare authorities' information systems and information banks. Nowadays we must take care of the difference between healthcare information and wellbeing information because they are classified at different security levels. Patients' healthcare information is classified, and they must be separated in data centers and communications systems from wellbeing information so that hackers and cyber attackers cannot use possible vulnerabilities in these systems and attack our healthcare systems.

Social and healthcare information systems are coming more and more complex systems and they are forming a lot of connections and federations between different ICT systems and applications in our societies. These service providers use many subcontractors, supply and service chains are complex, many different application developers work together developing different software components, and therefore maintenance chains are also branched out to many parties, and so on. In

such information and communication environments, it is difficult to ensure that security and cybersecurity are implemented by the requirements for all aspects of the entire production, service, and maintenance chains in healthcare services. In that kind of situation, we must also take care of ethical and moral issues concerning the patient's healthcare systems and which way they are developed with EU recommendations, and which way and where these service providers use and store these patients' information.

Integrating healthcare requirements in line with the new EU directives into the health and wellbeing environments and their systems also require action by the government and parliament, as well as line ministries, to bring legislation and standards into line with the directives. At the same time, these new laws can guide the actions of service providers to meet the measures related to the healthcare environment and day-to-day operations recommended by the new EU requirements. Legislation and regulations also impose requirements on organizations that develop healthcare systems and devices when developing new products and applications in this field.

2.3 Technical Systems

Today, patients and elderly persons can be in the hospital, in their homes, and anywhere they need to go to do issues needed, as Fig. 1 shows. When we are using new types of healthcare devices and services, we need also to verify that telecommunications operator networks and service providers in data centers are done according to needed requirements so, that we can trust e-health and m-health systems working the right way and trusted way, and our privacy and security issues are safely done.

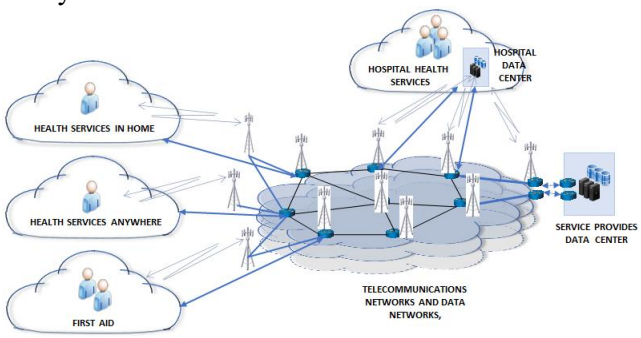

Fig. 1: E-health and mobile-health top-level architecture [11], [12].

Fig.2 shows an access network environment where elderly persons' and patients' devices are used every day. We don't know exactly the security and cybersecurity solution in that access network, and it is meaning challenge to use classified information in this kind of environment.

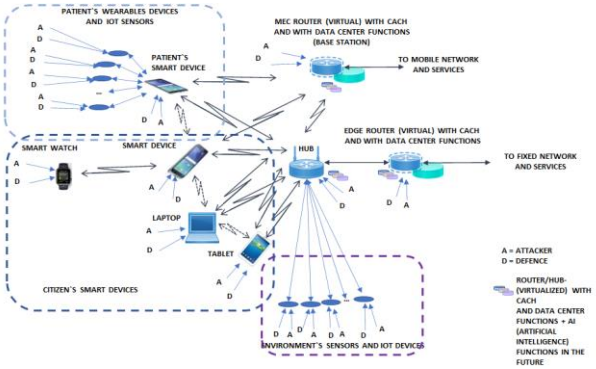

Fig. 2: Access network architecture [11].

The access network systems will utilize artificial intelligence (AI) in the future to help us to find vulnerabilities, malware, or if attackers try to attack our systems. AI can be used also to optimize network functionalities and energy consumption and also optimized used capacity.

Fig.2 shows the building and home environment's sensors and devices, which are using the same frequencies as e-health and m-health patients' and elderly persons' devices. This means possible interferences between different devices so that those healthcare systems maybe do not work at all. These devices use information that has different levels of security, such as public, restricted, or confidential information. Today, there are many vulnerabilities in these IoTs, sensors, and actuators, so cyber attackers and hackers can attack our system in such environments. Such attacks are carried out already in the world today. Building LANs is one important part of service chains from elderly persons' and patients' smart devices to the service provider's server center as we design and develop security and cybersecurity solutions. There must be separate data of the different security levels so that the data can be transmitted securely from end to end of the service chains.

When elderly persons move around daily, shopping, or even walking, tracking systems would make it possible to know where elderly persons are going or where they are. Location information is very important because if an elderly person has health-related incident problems, we know exactly his or her situation, and healthcare organizations can send the right help to the right place. It has happened that people do not get help at the right time and in the right place and a person has died when he has not received help in time. This situation also includes issues of privacy and ethics that need

to be taken into account and addressed when using this monitoring system, even if we use this monitoring system to save lives in critical situations. Location data has also been used against a person when someone knows the person's smart device and its movements and knows exactly where the person is. An example is that when a person goes into his/her car, the car can be hacked and its systems are modified so that the car can be steered to drive a crash where a person can lose his/her life.

Fig.3 shows a network architecture where elderly persons' and patients' smart devices are sending bio-signals and welfare signals end-to-end. In the communications environment, we must separate bio-signals data from other information so that the data can be safely transmitted from end to end of the service chains and there are not any other information going to the same address. Fig.4 shows one service chain from IoT devices and sensors to elderly persons' smart devices and from that to a data center and storage systems there. Table 1 shows the vulnerabilities of the IoT devices and sensors shown in Fig.4, as well as the user interface vulnerabilities and also the probabilities of attack.

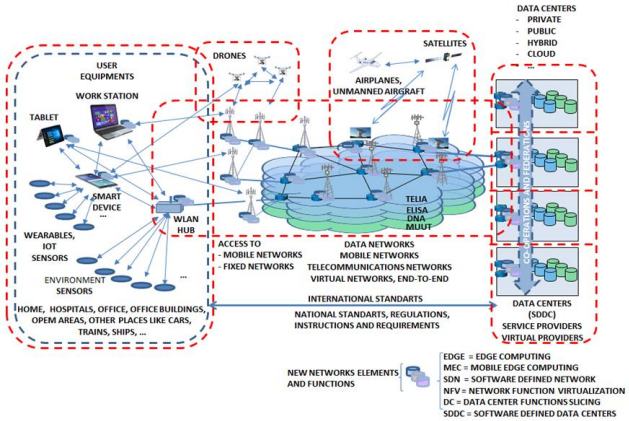

Fig. 3: Network architecture [11].

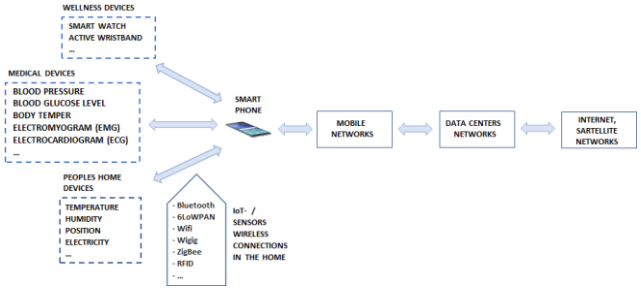

Fig. 4: Access Network architecture and sensors used by the elderly.

Today, almost all medical devices and wellness devices use wireless interfaces when connected to smart devices for the elderly. Those wireless access network connections are vulnerable because maybe there is not any kind of security mechanism there and that gives hackers and cyber attackers an easy way to attack our healthcare systems. The same kind of situation is also inside IoT devices and sensors. We may not notice if someone is connected to our system because IoT devices and sensors use wireless networks. After all, those devices' radio technical coverage areas extend up to 100 meters from the device with certain solutions. Even though we use encryption systems on our smart devices, it doesn't help us because hackers and cyber attackers are already inside because they can take advantage of the wireless connections of these IoT devices and sensors and install malware on our smart devices. The smart device may then be part of the BOT network or a device containing malware may contaminate our information systems and applications which are in the data center.

Table 1. Vulnerabilities of access network sensors.

Type / Devices	Devices (from Fig. 4)	Types of Communication system	Existing control in access side	Existing control in data center	Vulnerabilities In IoT-/sensor-devices	Vulnerabilities in access connection	Attack probabilities
Medical devices	Wireless connected devices (sensors and IoT Devices)	BAN, PAN, WAN	ID CODE or none	Firewall	Often non-security solution	Vulnerable wireless connection	Very high
Wellness devices	Wireless connected devices (sensors and IoT Devices)	BAN, PAN, WAN LTE, 3G, 4G, 5G	ID CODE or none	Firewall	Often non-security solution	Vulnerable wireless connection	Very high
Elderly peoples home devices	Wireless connected devices (sensors and IoT Devices)	PAN, WAN	ID CODE or none	Local or remote, (Firewall)	Often non-security solution	Vulnerable wireless connection	Very high

Figures 1-4 show how complex and fragmented the critical healthcare information infrastructure is, with many different types of sensors, IoT devices, and smart devices, before older people's bio-signals are sent to the network and data centers servers. Then healthcare professionals receive and analyze this bio-signal data and provide feedback and recommendations to elderly care. It is very difficult to make real security solutions and protections in this kind of environment. IoT devices and sensors are maybe using different types of data models, they use different protocols and there are not many possibilities to install any kind of security concepts inside the systems, and so on. On our IoT devices and sensors are many different suppliers which mean also challenges these devices' management and do real security solutions and protections to these devices. Because these systems are so complex and fragmented and have many different types of IoT devices and sensors in use, it is also very difficult to take care of ethical resilience things in such operating environments. Same time we must

also take care of security things so that hackers and cyber attackers could not attack our systems and use malware there. Because our IoT devices and sensors are many different suppliers that mean also challenges these devices' resilience management.

3 Designing Path of Resilience Management Framework

3.1 Ethics of Cybersecurity in Healthcare

The growing complexity of the digital ecosystem in combination with increasing global risks involves various ethical issues associated with cybersecurity. Christen, Gordijn and Loi express the dilemma [2, p. 1]: "Overemphasising cybersecurity may violate fundamental values such as equality, fairness, freedom or privacy. However, neglecting cybersecurity could undermine citizens' trust and confidence in the digital infrastructure, in policy makers and in state authorities." They continue "cybersecurity is still an under-developed topic in technology ethics. Although there are numerous papers discussing issues such as 'big data' and privacy, cybersecurity is—if at all—only discussed as a tool to protect (or undermine) privacy." For example, if a medical implant producer protects the data transfer between the implant and receiver server utilizing suitable cryptology, this significantly increases the energy consumption of the implant and frequently requires more surgeries for battery exchange [2, pp. 1-2].

Weber and Kleine [1] have investigated the ethical issues of cybersecurity in H&W applying the approach of principlism based on Beauchamp and Childress's [13] four principles of biomedical ethics (respect for autonomy, nonmaleficence, beneficence, and justice). The important aims of the employment of ICT in H&W are efficiency and quality of services, the privacy of information, and confidentiality of communication, usability of services, and safety [1]. Fig.5 maps the ethical principles to technical aims.

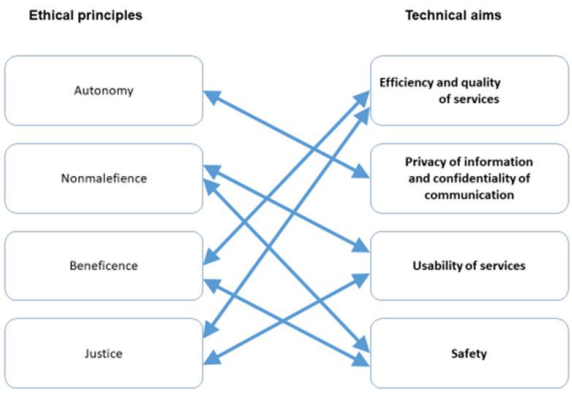

Fig. 5: Technical aims mapping to ethical principles (Adopted from [1])

3.2 Fundamental Concepts of Cyber Resilience

The human body is inherently resilient in its ability to persevere through infections or trauma, but our society's critical infrastructure lacks the same degree of resilience, typically losing essential functionality following adverse events [14]. Without proper protection and development with cybersecurity in mind, modern society relying on critical infrastructures would be extremely vulnerable to accidental and malicious cyber threats [6], [7]. Resilient systems can minimize the negative impacts of adverse events on societies and sustain or even improve their functionality by adapting to and learning from fundamental changes caused by those events [14].

The Network-Centric Warfare (NCW) doctrine [15] identifies four domains that create shared situational awareness and inform decentralized decision-making:

Physical: Physical resources and the capabilities and the design of those resources;

Information: Information and information development about the physical domain;

Cognitive: Use of the information and physical domains to make decisions; and

Social nexus: Organization structure and communication for making cognitive decisions.

The National Academy of Sciences identifies four event management cycles that a system needs to maintain to be resilient [16]:

1. Plan/Prepare: Lay the foundation to keep services available and assets functioning during a disruptive event (malfunction or attack).
2. Absorb: Maintain the most critical asset function and service availability while repelling or isolating the disruption.
3. Recover: Restore all asset functions and service availability to their pre-event functionality.

4. Adapt: Using knowledge from the event, alter protocol, a configuration of the system, personnel training, or other aspects to become more resilient.

Linkov et al. [17] combined the event management cycles and NCW domains to create resilience metrics for cyber systems. The process of building resilience is a collective action of public and private stakeholders responding to infrastructure disruptions [18].

3.3 Situational Awareness and the Concept of Cyber-Trust

The purpose concerning security is to know what is going on and what will happen in the network(s), and to be aware of the current level of security in the network(s), how to design or build-in security and resilience to a networked environment, and to define trade-offs for security and privacy levels versus system's usability [9]. The overall aim is to mitigate cybersecurity risks, which in turn supports the business continuity and operations of the whole society [9].

Investing in systems that improve confidence and trust can significantly reduce costs and improve the speed of interaction. From this perspective, cybersecurity should be seen as a key enabler for the development and maintenance of trust in the digital world. Cybersecurity has the following four themes [9]: (1) security technology, (2) situational awareness, (3) security management, and (4) resilience of operational systems, as shown in Fig.6 Situational awareness is needed for having a correct understanding of security incidents, network traffic, and other important aspects that affect security; and 6 technologies are needed for protection [9]. Human aspects have to rule in via security management. Consequently, resilient systems and infrastructures can prepare and plan for, absorb, recover from, and more successfully adapt to adverse events.

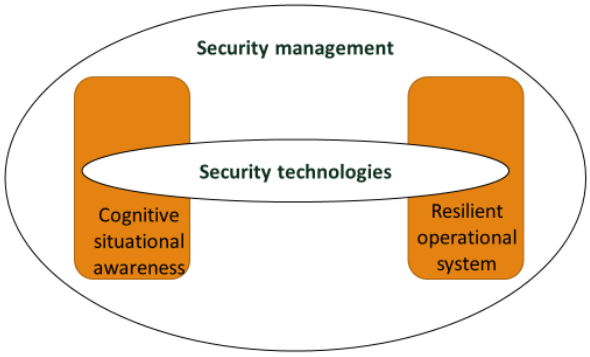

Fig. 6: Themes of Trust-building (adopted from [9])

Situational awareness (SA) is the main prerequisite of cybersecurity and resilience. Without SA, it is impossible to systematically prevent, identify, and protect the system from cyber incidents and if a cyber-attack happens, to recover from the attack [9]. SA involves being aware of what is happening around your system to understand how information, events, and how actions affect the goals and objectives, both now and soon. It also enables the selection of effective and efficient countermeasures, and thus, protects the system from varying threats and attacks.

Situational awareness is needed for creating a sound basis for the development and utilization of countermeasures (controls), where resilience focuses. The most important enablers of SA are observations, analysis, visualization, governmental cyber-policy, and national and international cooperation. For the related decision-making, relevant information collected from different sources of the cyber environment or cyberspace, e.g., networks, risk trends, and operational parameters, is needed. This requires information exchange between different stakeholders. And always, when dealing with information exchange, the main question is "trust".

Cyber situational awareness high-level architecture includes the data fusion engine, information interfaces, and the HMI providing an effective visualization layer [10]. These functionalities should be as automatic as possible without human interaction. However, there should be an operator for controlling the sensors and data fusion algorithms and inputting information into the system.

The cognitive SA system for supporting decision-making needs several input and output interfaces [10]:

- Sensor information interfaces. The system implements interfaces for the input of cybersecurity sensor information.
- Interfaces for status information. The system implements interfaces for inputting the status information of all the known cyber entities. Information on systems, devices, and sensors with their status and configuration information, but also the spare parts of physical devices are relevant information for a cybersecurity SA system. Also, information about the status of saved data and the status of information flows should be reported. Some of that information can be automatically generated using data interfaces and some should be user-generated by using HMI.

- Interfaces for analysis information. The system implements interfaces for information based on the analysis. That kind of information includes analyzed impact assessment information, Indicator of Compromise (IOC) information, and early-warning information from open-source intelligence using, e.g., social media or CERT bulletins. Further, required policies and objectives should be input into the system.
- Interfaces for information exchange. The system implements interfaces for cybersecurity information exchange with trusted companions.
- HMI. The system implements HMI for effective visualization of the current status of the cyber domain under control and for the input of information that cannot be entered automatically. HMI is also used for controlling the data fusion process. HMI should implement different visualizations for different levels of users: e.g. technical user who requires detailed technical information, whereas a decision-maker needs different visualization. HMI also implements filters for data allowed for different users.

3.4 Cyber Security Science

Cybersecurity aims to make cyberspace safe from damage or threat. Fig.7 shows three perspectives of cyberspace: (1) a data or information perspective that comes from the information theory space; (2) a technology perspective that includes the hardware, silicon, and wires, as well as software, operating systems, and network protocols; and (3) a human perspective that acknowledges that the human is as responsible for the dynamics of the system as the data and the technology are [8].

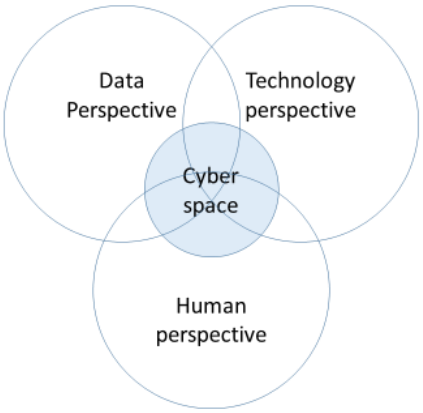

Fig. 7: Cyberspace at the overlap of data, technology, and human [8]

The overall goal of cybersecurity is that all systems and infrastructures are resilient. An e-health platform is a cyber-system that has human, technology, and data domains. One can think of a cyber-system as consisting of two sub-systems: the proper resilient operating system and the (*cognitive*) situational awareness system that both have human (*social*), technological (*physical*), and data-based (*information*) domains. Fig.8 shows this concept. *Security management, security technologies,* and *security information* connect these sub-systems. However, security information is mostly created or transferred from the operational system to the SA system via security technologies.

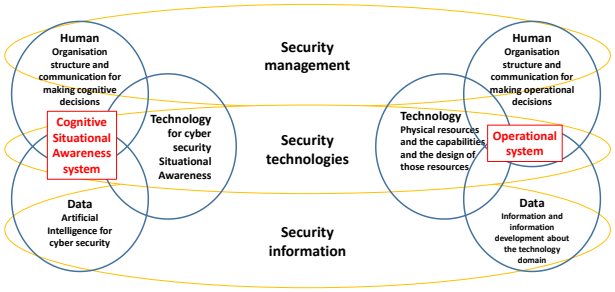

Fig. 8: Resilient Cyber-system as a combination of Operational system and Cognitive SA system

3.5 Security Management and Governance

Security policy is currently the main element used to communicate secure work practices to employees and ICT stakeholders. It is a declaration of the significance of security in the business of the organization in question. Additionally, the security policy defines the organization's policies and practices for personnel collaboration. However, people still often fail to comply with security policies, exposing the organization to various risks. One challenge is to promote methods and techniques that can support the development of comprehensible security policies in the emerging ICT paradigms, e.g., cloud computing and multiple devices [9]. Developing policies that can defeat the main reasons driving non-compliance, such as a habit, is challenging.

An information security management system (ISMS) focuses on the continuous management and operation of a system by the documented and systematic establishment of the procedures and processes to achieve confidentiality, integrity, and availability of the organization's information assets that do the preservation. ISMS provides controls to protect organizations' most fundamental asset, information. Many organizations apply audits and certification for their ISMS to convince their stakeholders that the security of the organization is

properly managed and meets regulatory security requirements. An information security audit is an audit of the level of information security in an organization. Security aware customers may require ISMS certification before a business relationship is established. Unfortunately, ISMS standards are not perfect and they possess potential problems. Usually, guidelines are developed using generic or universal models that may not apply to all organizations. Guidelines based on common, traditional practices take into consideration differences between the organizations and organization-specific security requirements.

In Fig.8, *security management* covers the human and organizational aspects of cybersecurity. Its focus areas include security policy development and implementation, risk management and information security investment, incentives, and trade-offs. Security management also integrates the social layer's operational and cognitive aspects; all technical and organizational components should learn from prior events and incidents.

3.6 Security Technologies and Security Information

Security technologies include all technical means towards cybersecurity, such as secure system architectures, protocols, and implementation, as well as tools and platforms for secure system development and deployment. Security technologies are needed for fulfilling the recognized security requirements, and for building resilient infrastructures and systems with dependable hardware and software that can also meet future security challenges [9].

Security technologies enable the technical protection of infrastructures, platforms, devices, services, and data. Technical protection starts with secure user identification and authorization which are necessary features in the most secure infrastructures, platforms, devices, and services. Fortunately, well-known technologies exist for their implementation. Typically, processes and data objects are associated with an owner, represented in the computer system by a user account, who sets the access rights for others. A global trend is to increase the use of cloud service technology when providing critical services. Data go into a cloud and will not come back to end-user's devices. Also, government data has already gone to a cloud, and in the future more and more government data will migrate to cloud servers and services. Partnerships between cloud service providers and security solution providers are becoming more common. We will see the emergence of cloud service-specific solution providers as well. Identity management and encryption will be the most important cloud security services to be offered. These services will be eventually offered for small to medium-sized businesses as well. We will also see the emergence of cloud security standards. Challenges are that quite often cloud service providers believe that security is just an end-user issue and firewall means security. Therefore, currently, we do not have proper cloud security standards and we lack awareness of a true understanding of comprehensive cloud security [9].

Security technologies are needed also then if something has happened. For example, forensics can lead to the sources of the attack/mistake and provide information for legal and other ramifications of the issue. Forensics also facilitates the analysis of the causes of the incident, which in turn, makes it possible to learn and avoid similar attacks in the future.

In Fig.8, *security technologies* include all technical means towards cybersecurity, such as secure system architectures, protocols, and implementation, as well as tools and platforms for secure system development and deployment. Technologies that create or transfer *security information* from the operational system to the SA system include sensors that collect the first level of data. Commonly, host- and network-based tools generate logs that are used for SA. Firewalls, system event logs, antivirus software, packet captures, net flow collectors, and intrusion detection systems are examples of common cyberspace sensors [8]. Level-two technologies generate information from the data to determine a current situation. Generally, level-two technologies require the bringing together of data and performing some level of analytics. The simplest form is signature-based tools such as antivirus and intrusion detection systems. These systems have encapsulated previous knowledge of detected attacks into signatures that detect and alert when attacks are detected in operational systems. More advanced systems such as security information and event managers (SIEMs) provide infrastructure to bring together datasets from multiple sensors for performing correlations. Vulnerability analysis to determine how many unpatched vulnerabilities exist in a system is also a form of level-two technology [8]. The third and final level is hard to achieve and only a few examples of effective tools exist. Cyber-threat intelligence provides information on active threat actor methods, techniques, and targets providing some level of predictive information to enable taking pre-emptive security measures [8]. Artificial

intelligence for cybersecurity develops with high speed and offers new possibilities for better SA.

3.7 Cognitive Situational Awareness and Resilience Management

Increasingly interconnected social, technical, and economic networks create large complex systems, and risk assessment of many individual components becomes cost and time prohibitive, or even impossible [14]. No one can control the whole system of infrastructures, and our outlook should move to coordination and cooperation. The uncertainties associated with the vulnerabilities of these systems challenge our ability to understand and manage them. Risk assessment and risk management are no longer sufficient in the modern cyber-physical world, which has unforeseeable and non-calculable stress situations. To address these challenges, a risk assessment should be used whenever possible to help prepare for and prevent the consequences of foreseeable events, but resilience must be built into systems to help them quickly recover and adapt when adverse events do occur [14].

The cognitive situational awareness system in Fig.8 utilizes the information from the operating system to make decisions that aim toward better resilience.

3.8 Governance Framework and Requirements

Fig.9 presents the conceptual resilience governance framework for a resilient e-health cyber-system.

4 Discussion

This paper offers a conceptual resilience governance framework and design aspects for ethical and resilient cyber-physical e-health and e-wellbeing systems. Our safety and security thinking has been based on these days a supposition that inside defensive walls we are safe.

Nowadays our societies provide a wide range of services available to citizens in real-time, regardless of location or time together with e-health and e-wellbeing services. This also means that almost all systems are interconnected through different integration platforms. There are also many federations between information systems. Before we can design ethical and flexible cyber-physical e-health and e-wellbeing systems, we need to look at different scenarios, use cases, and requirements. Also, large cross-system integrations and federations in ICT systems mean that there is a lot of interdependence between different ICT systems and between organizations and stakeholders. We need to identify dependencies on all internal and external systems and data flows, and only then can we design and implement flexible cyber-physical e-health and wellbeing systems.

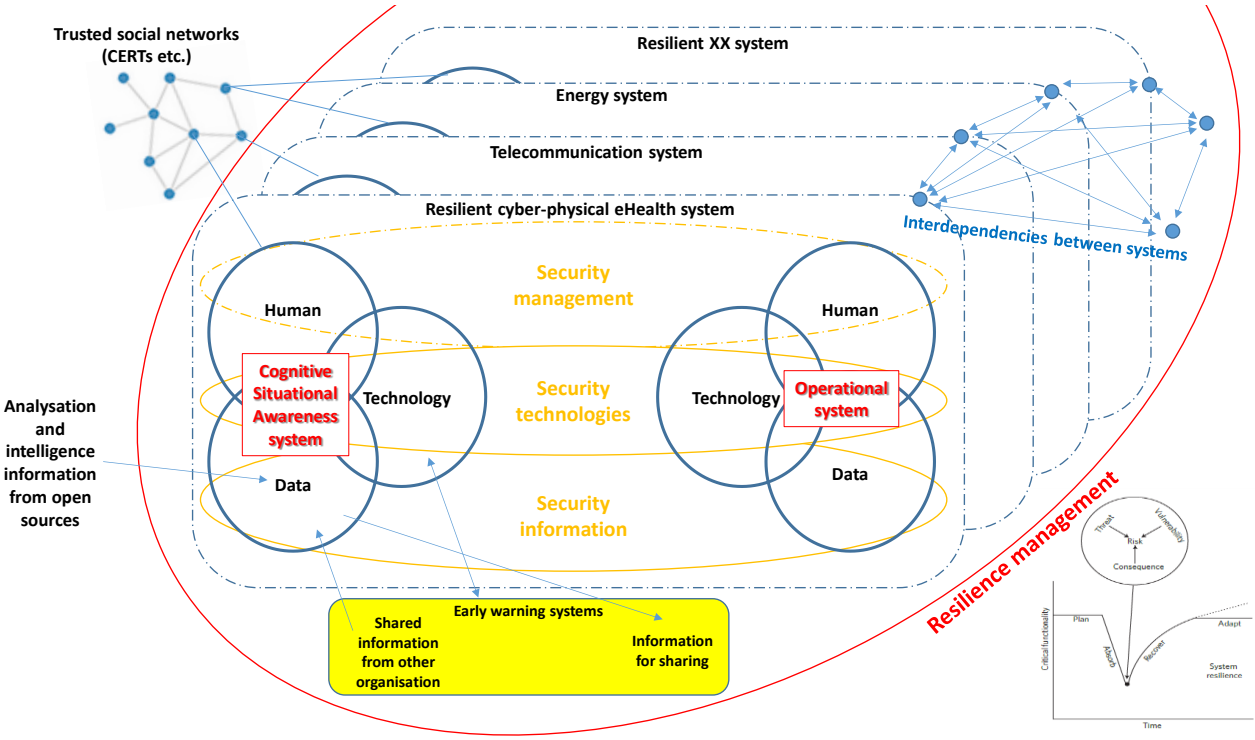

Fig. 9: Conceptual resilience governance framework for e-health CPSs

Ethical and resilient cyber-physical e-health and e-wellbeing systems includes also analyses of attack vectors, threats, vulnerabilities, and risks to specify a comprehensive cybersecurity architecture for electronic health and wellbeing systems. For this ethical and resilient development and design of cyber-physical e-health and e-wellbeing systems, we need to use, for example, the Enterprise Architecture Framework (EA) to describe all systems and environments [11] and then get the systems to work together in a controlled way with cybersecurity and information security in mind.

When we are taking ethical and resilient cyber-physical e-health and e-wellbeing systems in use we must be also test systems in real environments to verify their functionalities and security aspects.

Acknowledgments:
This work was supported by the SHAPES project, which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 857159.

References:

[1] K. Weber and N. Kleine, "Cybersecurity in Health Care," in The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology 21, Cham, Springer, 2020, pp. 139-156.
[2] M. Christen, B. Gordijn and M. Loi, "Introduction," in The Ethics of Cybersecurity, Cham, Springer, 2020, pp. 1-8.
[3] J. Rajamäki, "Resilience Management Framework for Critical Information Infrastructure: Designing the Level of Trust that Encourages the Exchange of Health Data," Information & Security, vol. 47, no. 1, pp. 91-108, 2020.
[4] A. Hevner and S. Chatterjee, Design research in information systems: Theory and practice, New York: Springer Science and Business Media, 2010.
[5] M. Christen, B. Gordijn and M. Loi, The Ethics of Cybersecurity, Cham: Springer Nature, 2020.
[6] I. Linkov and B. Trump, The Science and Practice of Resilience, Cham: Springer Nature, 2019.
[7] A. Kott and I. Linkov, Cyber Resilience of Systems and Networks. Risk, System and Decisions, Cham: Springer, 2019.
[8] T. Edgar and D. Manz, Research methods for cyber security, Cambridge: Syngress, 2017.
[9] DIMECC, The Finnish Cyber Trust Program 2015–2017, Helsinki: DIMECC, 2017.
[10] T. Kokkonen, "Anomaly-Based Online Intrusion Detection System as a Sensor for Cyber Security Situational Awareness System.," Jyväskylä studies in computing 251. University of Jyväskylä, 2016.
[11] A. Hummelholm, Cyber Security and Energy Efficiency in the Infrastructures of Smart Societies, Jyväskylä: University of Jyväskylä, 2019.
[12] A. Hummelholm, "E-health systems in digital environments," 18th European Conference on Cyber Warfare and Security, pp. 641-649, 2019.
[13] T. Beauchamp and J. Childress, Principles of biomedical ethics, New York: Oxford University, 2009.
[14] I. Linkov, T. Bridges, F. Creutzig, J. Decker, C. Fox-Lent, W. Kröger, J. Lambert, A. Levermann, B. Montreuil, J. Nathwani, R. Nyer, O. Renn, B. Scharte, A. Scheffler, M. Schreurs and T. Thiel-Clemen, "Changing the resilience paradigm," Nature Climat Change, vol. 4, pp. 407-409, 2014.
[15] D. Alberts, "Information age transformation, getting to a 21st century military. DOD Command and Control Research Program," 2002.
[16] National Academy of Sciences, Disaster resilience: a national imperative, 2012.
[17] I. Linkov, D. Eisenberg, K. Plourde, T. Seager, J. Allen and J. Kott, "Resilience metrics for cyber systems," Environ Syst Decis, 2013.
[18] H. Heinimann and K. Hatfield, "Infrastructure Resilience Assessment, Management and Governance – State and Perspectives," in I. Linkov, J.M. Palma-Oliveira (eds.), Resilience and Risk, NATO Science for Peace and Security Series C: Environmental Security, Cham, Springer, 2017, pp. 147-187.