E-Health Systems for Remote and Disaster-Resilient Digital Environments

Aarne Hummelholm[1] and Pekka Neittaanmäki[1,2]
[1]University of Jyväskylä, Finland
[2]Lappeenranta, University of Technology, Finland

aarne.hummelholm@elisanet.fi
pekka.neittaanmaki@jyu.fi

Abstract: We talk a lot about our digital services, artificial intelligence, virtual reality, and the metaverse, along with the platforms they run on. We focus on how we can further improve services in the systems operating on these platforms to support smart societies in the future and deliver value to a wide range of stakeholders across all sectors. The situation with this new type of service is not necessarily good enough in some regions of the world. People live in remote areas far from population centres on different continents, northern regions, wilderness areas, deserts, mountains, islands, etc. How can we guarantee suitable societies and well-being services for all people even in these conditions, far from core centres and large villages, regardless of time and place? We must strive to take advantage of the opportunities provided by innovative ideas and technologies and use renewable energy in all areas, especially in areas where electricity systems do not always work, and telecommunication connections are not always available. Artificial intelligence is already integrated into many areas of smart society services. Virtual reality (VR) functionalities are also coming to be used in many service portfolios. Nowadays, we are talking a lot about the metaverse. To fully utilize new technologies and their services, we need robust solutions for the interfaces between smart devices and network systems, ensuring seamless and secure access anytime, anywhere. These solutions must be designed to prevent cyber attackers from exploiting vulnerabilities in the new systems and the smart devices connected to them. This article outlines principles for future smart society services, possibly using PeAN smart devices designed for areas that might be far from major cities and villages.

Keywords: Remote healthcare, Satellite communication, Metaverse, Smart society infrastructure, AI in healthcare, Quantum encryption

1. Introduction

Today, our society wants to take advantage of digitization's possibilities in all of society's everyday services: autonomous cars, factories, ships, healthcare services, remote schooling, remote work, remote management of financial affairs, remote diagnostics of patients and the senior citizens, remote analysis of diseases, prevention of diseases, and monitoring of progress. One example of the need for such services is the COVID-19 pandemic.

However, the rapid technological development underlying digitization poses challenges for all future technical systems, such as 5G-6G transition or metaverse environments, and their services. These challenges involve the creation of guidelines and regulations, along with the necessary processes for testing, analysis, verification, validation, and certification. The cost-effectiveness and useability of all smart society services have become increasingly essential in decision-making, affecting service processes, methods, solutions, and where people get their services. The goal is to organize all services to allow people to access them in the shortest time possible, regardless of time or location. One critical issue is that healthcare services are available 24/7 regardless of time and place, anywhere with quality and equity, not forgetting that patients or senior citizens may live in cities or rural areas or far from hospitals or treatment centres. Additionally, it is possible to track their movements by using the location information of patients and senior citizens. Their whereabouts can be reported if necessary, ensuring they receive help at the right location, even if they live in rural areas far from large cities or towns.

The EU has developed Galileo satellite systems (EU-Galileo) and Galileo Public Regulates Services (EU–Space program, PRS) to ensure accurate location information and secure communication between different authorities in different regions of Europe. EU has started a new project, ECHO 2, a European concept for higher altitude operations and systems integration (EU-ECHO 2). Figure 1 presents a new digital society environment of the future with new technical solutions and communication possibilities at a high level. Today, people can already use smart devices with satellite communication capabilities, but they must consider the challenges and limitations of these connections (IEEE, Oltjon Kodheli) (IEEE, Yunchou Xing) (IEEE, Gunes Karabulut Kurt). With the help of these satellite concepts, we can provide people with different services at a cheaper and faster rate. This new technical solution gives us new possibilities to develop different services which can be used anywhere in the world in different areas. The expansion of these new network functions gives us many new opportunities to provide services, for example, connections in crises situations (war, harassment, natural disasters, large floods, surveillance, and rescue operations, etc.) and to areas where legacy technology is limited or even without mobile technology, etc. In some areas, we can only use narrowband communications systems or amateur radio networks. In this new satellite- and HAPS-concepts (HAPS=High Altitude Platform System), presented in Figure 1, we can combine the various parts of our societies' communication systems to work together and offer people the services they need, regardless of time and place (Aarne Hummelholm, et al., pp. 110-114). These new HAPS and satellite concepts provide opportunities for rapid network expansions, integrations and service delivery between different networks for different areas (mobile and fixed network, satellite networks (LEO = Low Earth Orbit), (MEO = Medium Earth Orbit), (HEO = High Elliptical orbit), (GEO = Geostationary Earth Orbit)).

Today, we see significant new challenges in the world due to climate change and its effects on the climate of different regions, causing various disasters such as floods, storm damage, forest fires, destruction of structures and infrastructures in cities and villages, etc. In these areas, people need help, food, warmth, shelter, sleeping facilities, healthcare services, various transport services, etc. How can we organize, plan, and ensure communication in these areas as quickly as possible? Figures 1, 2 and 3 show examples of how we can organize communication systems in various places regardless of time and place, including rural areas, deserts, sparsely populated areas, mountains, and so on. The challenges of this development increase by the simultaneous transitions from 5G network technologies to 6G network technologies, the implementation of artificial intelligence, the introduction of virtual reality into services in different operational areas, and the introduction of metaverse platforms. Other significant challenges are that in different regions, technologies at different stages of the life cycles of different devices, systems and applications are used, and we must adapt our new technical solution to work together with these old systems, as well as make integrations and adaptations between different systems so that they work well together, and peoples get services well. The new satellite solutions give us energy-efficient networks and service possibilities. They help to save energy by reducing the need to build as many base stations and communication towers in rural areas as possible, unlike we do today.

To ensure the effective functioning of the services offered, we must also consider Shannon's theorem, *which defines the maximum rate at which information can be transmitted over a communication channel without error* (Shannon). Many mobile network base stations are idle for quite a large part of the time and consume energy. The energy consumption must be optimized according to the time used (Aarne Hummelholm et al., pp. 168 - 175).

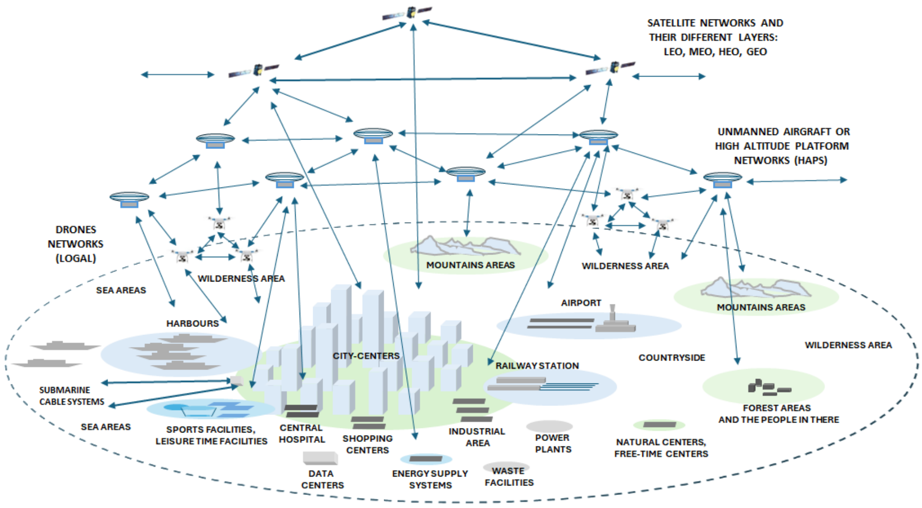

Figure 1: Smart society's new future digital living environment with new technical possibilities (IEEE, Oltjon Kodheli) (Ju Han) (IEEE, Yunchou Xing) (IEEE, Gunes Karabulut Kurt)

2. Objective and Grouping of Paper

The research question in this paper is: Can new digital devices and systems be used safely in future digital and metaverse environments, supporting various purposes and services, accessible independently, anytime and anywhere, across our societies?

In this study, we use actual use cases related to rescue services and emergencies, where information exchanges related to cooperation with different parties are needed. We have also used the NATO architecture framework, v 4.0 and JHS 179 (Aarne Hummelholm et al., p. 32) and their methodological models. We can use services offered by societies from various places and through different communication systems regardless of where people live or stay in diverse situations, as presented in Figures 1, 2 and 3. These figures show the infrastructures people can access the services they need in near real-time. This article profoundly analyzes healthcare use cases with wearables, sensors, and IoT devices, including environmental devices and healthcare services, because they are the most critical use cases in our future smart societies' healthcare environments and rescue operations in different situations, including wartime. Working in rescue operations in different situations is also a big challenge if the communication systems are not working correctly. We analyze these use cases together with healthcare use cases. Chapter 3 deals with healthcare services in the future digital living environments independent of time and place, even if people live far away from healthcare centres. Chapter 4 deals with making and modelling threat analyses. Chapter 5 concludes this paper, our solution models and suggests future work.

3. Health Care Services in the Future Digital Living Environments Independent of Time and Place

Currently, numerous applications and services require better communication functionalities than the characteristics of 5G. They include, for example, global coverage, ultra-high data transfer rate, ultra-low latency, ultra-dense number of devices, ultra-accurate positioning, ultra-reliable and secure connection, low power consumption, and high energy efficiency (EU- Energy Efficiency). New virtual reality applications and services will also need better and faster communication options in the future, and their use will be developed and expanded for use in numerous new areas of use. We can meet these requirements in 6G mobile networks in the future. New types of smart devices with cross-over communication functions and MIMO (Multiple-Input and Multiple-Output) technologies give people even more freedom of movement (Aarne Hummelholm et al., pp.142-147). One example of the most critical service of smart societies to its people is digital healthcare services independent of time and place, Figures 1 and 2.

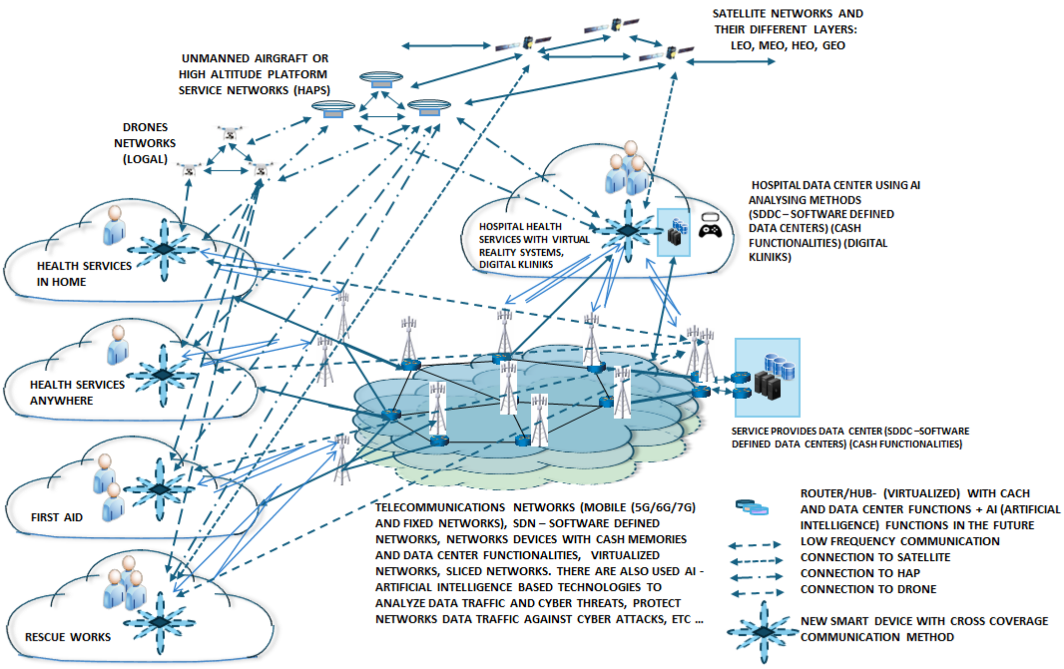

Figure 2: Architectures of digital healthcare services provided by society in different areas at the overall architecture level (IEEE, Mohammed Salih Mohammed Gismalla)

Today, we have situations where hospitals and healthcare centres are key treatment centres where patients and senior citizens are examined and treated. Accessing treatment takes time and frustrates patients or older people in several situations. This may result from a shortage of healthcare personnel, but long geographical distances may also hinder medical examinations or access to treatment. Long distances also increase costs, so achieving a cost-effective solution for each treatment situation is not always possible. People may have to travel to a treatment point just for a check-up that could have been done remotely with digital systems without visiting a hospital or treatment point. The principle of future healthcare communication environments can be seen in Figures 1, 2 and 4, which allows us to offer healthcare services to everyone, regardless of time and place, anywhere in the world. Because of numerous needs, the development of digital treatment environments and methods with sensors and IoT devices is strongly developed to improve the treatment of patients, to see their condition even from a distance from home or anywhere else in real-time and analyses are done with the help of artificial intelligence (AI) also in real-time. The use of AI accelerates the analysis of patient data, enables more accurate and faster analyses, and enables continuous monitoring and quick reactions when the treatment situation requires it. The principle of the remote healthcare model is presented in Figure 4. Figure 3 shows accident or rescue situations in which the police, healthcare personnel, rescue workers and operational managers must communicate with each other using different communication systems to communicate with each other even in critical situations in rural areas far from large cities and in areas where communication systems may not work correctly or not at all. Today, we have seen numerous situations where tsunamis, hurricanes, big floods, volcanic eruptions, or tropical storms hit some areas of the continents or places or countries in some storm-prone areas that we cannot easily go to, and the communication systems there may not work at all in these situations. Carrying out rescue operations in such situations is challenging.

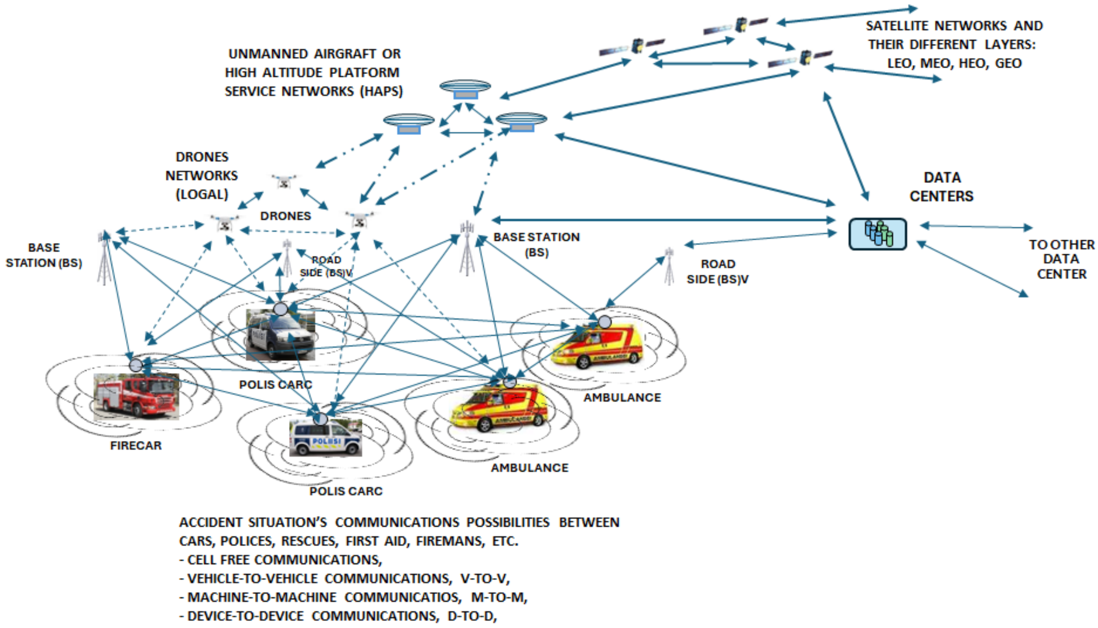

Figure 3: Accident situations in the field, roads, cities, buildings, homes, wilderness areas, etc. (Aarne Hummelholm et al., ECCWS 2024 Jyväskylä)

We must find new and better solutions and technical platforms for rescuers, police, healthcare personnel and operational managers who help people in such situations. A possible solution is presented in Figure 3. We need new technical communication platforms for disaster areas, such as storm areas or tsunami disaster areas, where communication networks may no longer work. We also need good and organized communication systems for temporary peacekeeping operation situations or when energy supply systems are down for one reason or another. When situations in the area of tsunamis, hurricanes, volcanic eruptions or tropical storms are sufficiently stable, we can bring ready-made communication stadion containers to the area, in which communication and electrical systems have already been installed, including, e.g. satellite, HAPS or DRONE connection systems. This way, the communication systems needed in these areas are ready to be used quickly and remain continuously in use until the situation stabilizes and new fixed systems are installed. In these situations, we could also use mobile masts to meet the needs of mobile communication networks.

We can equip a communication station container with renewable energy systems such as solar cells and small wind generators (0.5 kW, 1 kW or 5 kW). We can install renewable energy systems on the roofs of the containers or use masts or other buildings to raise them so that the sun and wind can better affect them. We also need batteries for energy storage and use when other systems cannot produce energy (Aarne Hummelholm et al., pp. 99–109). In this way, we can develop new energy supply systems for remote areas with the help of solar cells and wind generators, which form energy supply systems so that patients and senior citizens can go to certain places to charge their smart devices if necessary. From those places, they can also send messages from their smart devices to healthcare systems because it is possible to build interfaces to these new communication systems. (Figure 1)

One way to establish or build telecommunication connections far from large cities and villages is by using various satellite, HAPS, or DRONE systems. (Figures 1, 2 and 3). However, geostationary satellites are unsuitable for this purpose in northern regions, as their orbit is above the equator. In this case, the radiation angle of their antennas is too small, and the earth's shape is an obstacle to establishing effective communication connections. One possibility is using a highly elliptical earth orbit (HEO) satellite in northern regions.

Our design must also consider the challenges caused by the Van Allen radiation and space debris belts.

- The Van Allen radiation belts, where the earth's magnetic field confines energetic particles such as protons and electrons, can damage satellites' electronic components.
- Another obstacle is space debris belts, where spacecraft are abandoned at the end of their lifetime. Such spacecraft are becoming an increasing problem for the international community as they can damage satellite networks and future space missions.

Digital healthcare systems are one of the most critical service environments through which our future society offers its healthcare services to people because the requirements of those systems for the functionality of physical devices and communication networks and applications are more challenging than before, e.g. because artificial intelligence applications and virtual reality are involved in everyday operations in different areas. Figures 2, 3 and 4 show the general architecture of future smart societies' healthcare service, analysis, and monitoring systems. Figure 4 also shows the sensors on the patient's body, which form the body area network (WPAN) concept. In this solution, a new type of smart device, the Personal Access Node (PeAN), sends the information obtained from sensors (Aarne Hummelholm et al. pp. 142-147).

The PeAN device sends the patient's bio-signals to the hospital's healthcare system through different communication networks, depending on the situation, Figure 1, and the environment. Once the healthcare staff receives the patients' biosignals for analysis, they review the data and then provide feedback to the patient with recommended next steps. We can do this analysis in real time with artificial intelligence. The healthcare staff have real-time information about the patient's situation and can act quickly to give fast feedback to patients.

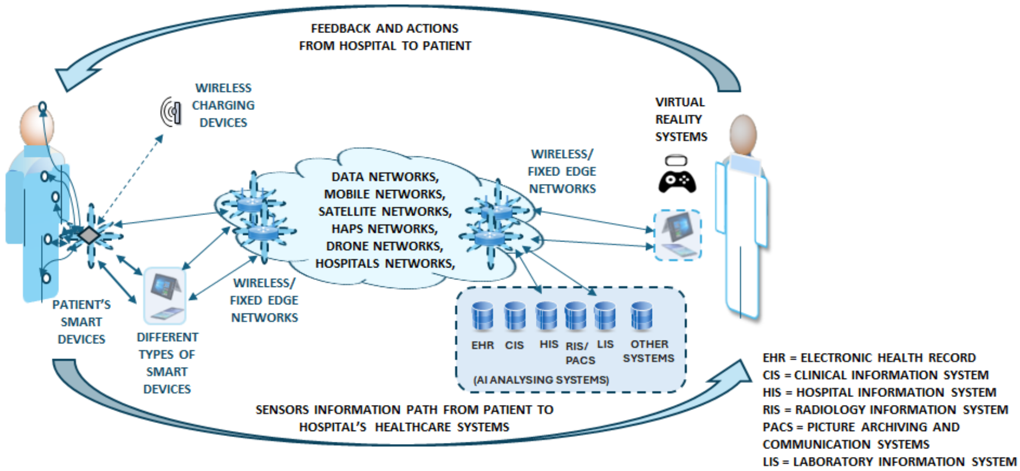

Figure 4: General architecture of the healthcare analysis and monitoring system of future smart societies with new healthcare devices, systems, and applications (Aarne Hummelholm et al., pp.123-138)

Table 1 shows key wireless biomedical monitoring systems' data transfer rates and bandwidth requirements in remote healthcare environments. Table 2 shows the requirements for virtual reality and its applications in future operating environments, including digital twin and Hologram systems requirements. These requirements must also be considered when developing and designing services for working in metaverse environments.

Table 1: Data Rates and Bandwidth of Key Biomedical Wireless Monitoring (Robert S. H. Istepanian)

Physiological/Biomedical Parameter	Bandwidth	Rate Latency/Data
ECG (12 leads) = Electrocardiogram	0.1 – 1 kHz	~144 Kbits/<200 ms
EEG (12 leads) = Electroencephalogram	0.1 – 0.2 kHz	~40 Kbits/<300 ms
EMG Electromyography	0 – 10 kHz	~350 Kbits/<200 ms
Body temperature	0 – 1 kHz	~0.1 kHz
Medical imaging and video streaming data	-	~ > 10 Mbps/<100 ms

Physiological/Biomedical Parameter	Bandwidth	Rate Latency/Data
Speech and voice	-	~50 – 100 Mbitps/<10 ms
Accelerometer and motion sensing	0 – 0.5 kHz	~30 Kbitps
Blood glucose monitoring	0 – 40 kHz	~1.5 Kbitps
Blood pressure	0 – 1 kHz	~15 Hz

Table 2: Communication requirements for metaverse applications (Mansoor Ali)

Applications	Latency (ms)	Reliability (%)	Data Rate (Mbit/s)
Hologram Education (light field)	20	$1–10^{-5}$	$1x10^5 – 1X10^6$
Augmentit Reality Smart Healthcare	5	$1–10^{-5}$	10000
Digital Twin (Smart city)	5–10	$1–10^{-5}$	10
Virtual Reality Entertainment	7–15	$1–10^{-5}$	250
Tactile internet	1	$1–10^{-6}$	1

The metaverse is a virtual world where humans interact as avatars with each other in a three-dimensional space that mimics reality (Cambridge Dictionary). We need new types of operations environments to improve the services of our smart societies. These operations should be more cost-effective than our previous traditional based on centralized operations environments in communications and data centre systems and their services. We can use more efficient 6G-based (later 7G) communications connections and services in these new digital environments. 6G technologies provide better opportunities to use services based on virtual reality in various services together with artificial intelligence. Table 2 shows the latency values of different technical solutions. Due to these latencies, in the future, we cannot use cloud services in the way we are using them today. For example, in public safety use cases, Figures 2 and 3, we can use mobile devices with limited backhaul connections via satellite, HAPS, or DRONE links and in direct communication between security personnel using a device-to-device communication concept. This concept makes creating a functioning network possible without needing other networks.

When using wireless networks in metaverse environments, which enable improved freedom of movement and availability for people, we must consider these new communications environments and their requirements. For example, related to healthcare and public safety use cases, Figures 2, 3 and 4, we need to design Access -, EDGE - and MEC networks with cyber security challenges in mind in these new operating environments and network models so people can use services securely. New technical encryption solutions and systems are also being introduced in future environments, such as Post Quantum Encryption systems (IDQ - ID Quantique) (ITU-T Y) (ENISA), virtual reality devices and concepts, and artificial intelligence. For example, those new encryption systems will be used in healthcare data analysis environments, data validation environments, treatment optimization, and metaverse environments. The taxonomy of electronic health, or m-healthcare system, can be described by describing information flows and processes, such as when health information is obtained from the patient with the help of sensors and the information is sent to the hospital's medical information system. In these medical analysis systems, the incoming data is analyzed and conclusions are drawn based on the results (Robert S. H. Istepanian). Metaverse environments are also coming into use in healthcare environments, which means even more challenges to developing cyber security systems for our healthcare environments now and in the future, considering future technical development and its effects.

4. Making and Modelling of Threat Analyses

As presented in Figures 1 - 4, healthcare systems are highly complex and have interfaces in many directions, such as different wireless networks, fixed networks, and, nowadays, different satellite networks. In addition, several service providers, administrators, and stakeholders work on the same networks and information systems. The operating limits of the responsible actors must be able to define and instruct the functions so that interoperability is ensured between operators and those using the services. To be able to conduct cyber threat assessments and analyses, we must first work with architectural descriptions of the operating environments of the hospital, home, and outside the home, with equipment and operating processes (NATO architecture framework, v 4.0 and JHS 179 (Aarne Hummelholm et al., p 32)). To prevent or mitigate the risks outlined in Chapter 3, all healthcare system components should be segmented into distinct functional units, each protected by robust security mechanisms and appropriate gateway solutions. These segments will then be examined also based on use cases. We must carefully look at attackers, their capabilities, and their motivations to disrupt healthcare systems and organizations. It is also important to consider that attackers may leverage artificial intelligence to aid in carrying out their attacks. Figure 5 shows one architecture model of various network control and management systems at the principle level for these telecommunications environments.

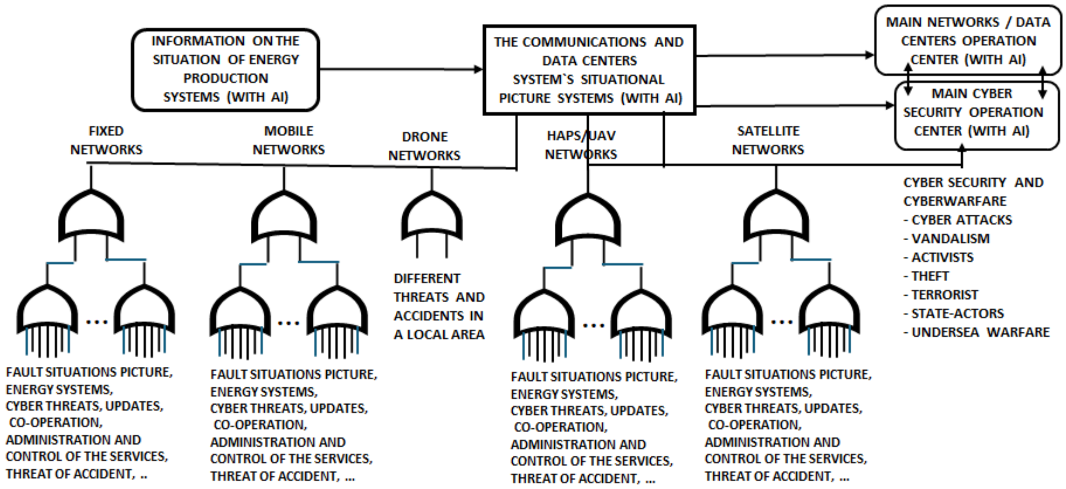

Figure 5: Architecture model of various network control and management systems at the principle level

We must look carefully at these all end-to-end communication paths and all the devices connected to this path. The integration described above is accelerating horizontally and vertically at all operational levels in each area. Analyzing the latest technologies and available services and applications in these smart environments becomes even more difficult as technologies rapidly evolve throughout communication chains and in their devices. These considerations should be taken into account when final dependency analyses, cyber threat assessments, vulnerability assessments, risk assessments, and analyses are carried out for the target area. We must use the EA (Enterprise Architecture) framework to simplify auditing, understand how our systems connect with other networks and services, and spot possible end-to-end attack risks. We must analyze different OSI (Open Systems Interconnection) layers of communications networks and the protocols and data models used. When we use artificial intelligence in these analyses, we need reference models to verify the basic data of our analyses and the algorithms used in the processes. When we use AI to analyze the cybersecurity of our systems and applications, we need to use taxonomies to get better and verified results from our analytics (NIST, Trustworthy and Responsible AI, Adversarial Machine Learning) (NIST, Trustworthy and Responsible AI, Artificial Intelligence Risk Management Framework). There must be secure, isolated reference models and stored data to verify the integrity of the information used in analyses. This is crucial, as cyber attackers—who increasingly leverage AI in their attacks—may attempt to alter or manipulate these resources. We must also consider the EU Tempest requirements (EU-Tempest). Table 3 shows different attackers, their capabilities, motivations, and targets. The probability values of attacks and threats can be calculated using the features of the EA system (NATO architecture framework, v 4.0) (JHS 179) (MITRE).

Table 3: Capabilities and Motivations for Disrupting Healthcare Systems and Organizations, with examples and updates (Aarne Hummelholm, et.al. p.132)

	Patient Health		**Patient / Hospital Records**		**National Health Care Systems**	
Adversaries / Attackers	Targeted (Specific Victims)	Untargeted (Not Specified)	Targeted (Specific Victims)	Untargeted (Not Specified)	Targeted (Specific Victims)	Untargeted (Not Specified)
Individuals / Small Group	Yes		Yes		Yes	
Political Group / Hacktivists	Yes	Yes	Yes	Yes	Yes	Yes
Organized	Yes		Yes		Yes	

	Patient Health		Patient / Hospital Records		National Health Care Systems	
Crime						
Terrorism / Terrorist org.	Yes	Yes	Yes	Yes	Yes	Yes
Cyber Attackers	Yes	Yes	Yes	Yes	Yes	Yes
Nations, States	Yes	Yes	Yes	Yes	Yes	Yes

5. Conclusion of the Current Situation, our Solution Model PeAN and Future Work

5.1 Conclusion of the Current Situation

We talk a lot about our digital services, artificial intelligence, virtual reality and metaverses and their operating platforms and how we can further develop offered services in the systems operating on these new platforms to work even better and produce services for smart societies in the future, for various stakeholders in all areas of our smart society and for everyone to people even if they are living far away from big city centres and villages. Figures 1, 2 and 3 show that the living environments of the smart societies of the future and the services they offer will operate in very complex operating environments in terms of telecommunications. They will be full of major challenges, such as our healthcare services and rescue operations and their functionalities in different situations.

5.2 Our Solution Model, PeAN

Figures 1, 2, and 3 present examples of solution models designed to provide essential services to people everywhere, regardless of time and place.

We can use satellites at different altitudes and the networks formed with them for telecommunications purposes (Leo, Meo, Heo, Geo), networks formed by uncrewed aerial vehicles or high-altitude platform networks (haps) or drone networks (local only). From these networks, we have interfaces to our new PeAN smart devices, which can form their own network between different devices where it is needed.

5.3 Future Work

Because healthcare devices may have many vulnerabilities and security challenges, we need to find suitable architectures for healthcare equipment and systems and give them requirements so that patients and treatment staff can use them safely in this medical care environment (EU-GDPR) (EU—MDR) (EU—NIS) and also in the metaverse environments.

Healthcare systems and devices, sensors, smart devices, IoT devices, and actuators must be developed so that the use of Postquantum Encryption technologies (IDQ—ID Quantique) (ITU-TY) (ENISA) is possible to achieve better information security features against cyber attackers, state actors, hackers, terrorists, and so on, ensuring the confidentiality and operation of healthcare systems in all situations.

Artificial intelligence (AI) needs to be studied and evaluated for its ability to protect e-Health's IoT devices, sensors, and other healthcare systems so that we can better protect these devices against malicious software and cyber-attacks (EU 2024/1689), considering that cyber-attackers also use AI in their attacks.

Verifying that people's healthcare devices work in every situation is one big challenge. So, we must develop wireless charging systems (or charging while we move) (WIRELESS POWER CONSORTIUM) for devices so that we can verify their working day and night in different situations.

One of the research topics is measuring and evaluating frequency disturbances in the hospital and in the patient's home environment and identifying cases that debilitate the patient's treatment.

Virtual reality systems and metaverse environments are now beginning to see broader implementation, and they are one research and development target. In certain situations, doctors and health care personnel can, for example, visit people's homes virtually to check their condition and health status and carry out analyses and examinations there.

We must study the functions of the future metaverse operating environment and cyber security and search for solutions where quantum computing and quantum encryption are used in the same operating environments. We must also plan the clocking of different data flows in metaverse environments and develop the applications to minimize the effects of delay dependencies and delay fluctuations in the services used (using an atomic clock source).

One area of research is to find different wireless communication systems that we can use even in rural areas and in the wilderness where other communication systems do not work well or are unreliable (For example, new Software radios).

Today, people travel to different countries worldwide for vacation or work reasons or want to spend their free time abroad in a holiday area. We should cooperate with healthcare organizations in other countries to develop communication standards for communication systems interfaces through which tourists visiting the country could secretly send their biosignals from abroad to home healthcare systems.

Energy efficiencies are a critical research area for investigating them in the healthcare environment and healthcare smart devices (EU—Energy).

One area of research is to find cooperation opportunities where communication operators, service providers, different actors, governments, and authorities can work together and exchange information in critical situations.

References

Aarne Hummelholm, et al. Cyber Security and Energy Efficient in the Infrastructures of Smart Societies, JYU Dissertation 173, http://urn.fi/URN:ISBN:978-951-39-8004-7.

Aarne Hummelholm, ECCWS 2024, Jyväskylä, Poster: Quantum- and cyber-secure smart devices for use in the smart Metaverse networks

Cambridge Dictionary, Metaverse, https://dictionary.cambridge.org/dictionary/english/metaverse.

ENISA, Post Quantum cryptography, Integration study, October 2022.

EU-ECHO 2, European Concept for Higher Altitude Operations (ECHO 2), https://www.eurocontrol.int/project/european-concept-higher-altitude-operations

EU- 2024/1689, AI regulation 13.6.2024.

EU- Energy Efficiency Directive, 2012/27.

EU- Galileo, Satellite Navigation, https://defence-industry-space.ec.europa.eu/eu-space/galileo-satellite-navigation_en

EU- GDPR, The General Data Protection Regulation, 2016/679.

EU- MDR, The Medical Devices Regulation, 5/2017.

EU- NIS, Concerning measures for a high common level of security of network and information systems across the Union, 6/2016.

EU-Space program, PRS, EUSPA 2021-2024, https://www.euspa.europa.eu/eu-space-programme/galileo/services

EU- 2022/640 of 7 April 2022.

EU-Tempest, 25 March 2019, based on NATO standards SDIP-27, -28 ja -29.

IDQ - ID Quantique, info@idquantique.com

IEEE, Gunes Karabulut Kurt, Senior Member, IEEE, Mohammad G. Khoshkholgh, Member, IEEE, Safwan Alfattani, Student Member, IEEE, Ahmed Ibrahim, Member, IEEE, Tasneem S. J. Darwish, Senior Member, IEEE, Md Sahabul Alam, Member, IEEE, Halim Yanikomeroglu, Fellow, IEEE, and Abbas Yongacoglu, Life Member, IEEE, A Vision and Framework for the High Altitude Platform Station (HAPS) Networks of the Future, Mar 2021.

IEEE, MOHAMMED SALIH MOHAMMED GISMALLA, (Senior Member, IEEE), ASRUL IZAM AZMI (Member, IEEE), MOHD RASHIDI BIN SALIM (Member, IEEE), MOHAMMAD FAIZ LIEW ABDULLAH (Senior Member, IEEE), FARABI IQBA, WAFI A. MABROUK (Graduate Student Member, IEEE), MAISARA BINTI OTHMAN4, (Member, IEEE), ADEL Y. I. ASHYAP, AND ABU SAHMAH MOHD SUPA'AT, Survey on Device to Device (D2D) Communication for 5GB/6G Networks: Concept, Applications, Challenges, and Future Directions.

IEEE, Oltjon Kodheli, Eva Lagunas, Nicola Maturo, Shree Krishna Sharma, Bhavani Shankar, Jesus Fabian Mendoza Montoya, Juan Carlos Merlano Duncan, Danilo Spano, Symeon Chatzinotas, Steven Kisseleff, Jorge Querol, Lei Lei, Thang X. Vu, George Goussetis, Satellite Communications in the New Space Era, Mar 2020.

IEEE, Yunchou Xing, Frank Hsieh, Amitava Ghosh, Theodore S. Rappaport, High Altitude Platform Stations (HAPS): Architecture and System Performance, April 2021.

ITU-T Y.3800 series – Quantum key distribution networks – Role in end-to-end cryptographic services with non-quantum cryptography

Ju Han, Recent Progress and Future Development in Satellite Communication, ESAC 2022, Highlights in Science, Engineering and Technology.

Mansoor Ali, Member, IEEE, Faisal Naeem, Member, IEEE, Georges Kaddoum, Senior Member, IEEE, Ekram

MITRE, ATT&CK, https://attack.mitre.org.

NATO, ARCHITECTURE FRAMEWORK Version 4. Document Version 2020.09, Chapter 2 –, p. 22-65.

NIST, Trustworthy and Responsible AI, NIST AI 100-2e2025, Adversarial Machine Learning, A Taxonomy and Terminology of Attacks and Mitigations.
NIST, Trustworthy and Responsible AI, NIST AI 600-1, july 2024, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile.
Hossain, Fellow, IEEE: Metaverse Communications, Networking, Security, and Applications: Research Issues, State-of-the-Art, and Future Directions, 9 Jan 2023.
Robert S. H. Istepanian, Bryan Woodward, m-Health, Fundamentals and Applications, Wiley, 2017.
Shannon, Shannon limit, Stanford University, June 4, 2024, https://web.stanford.edu/class/engr76/lectures/lecture19.pdf.
WIRELESS POWER CONSORTIUM, Qi Specification, 2021 (Wireless charging) Wireless Power Consortium, Wireless charging Qi v2.0 standard.