

Future Smart Devices in Future Digital Environments

Aarne Hummelholm¹, Pekka Neittaanmäki^{1,2} and Ruth Kaila^{1,3}

¹University of Jyväskylä, Finland

²Lappeenranta, University of Technology, Finland

³Aalto University, Espoo, Finland

aarne.hummelholm@elisanet.fi

pekka.neittaanmaki@jyu.fi

ruth.kaila@aalto.fi

Abstract: Our modern smart cities and societies are rapidly changing in all aspects. These entities can be described as digital, multidimensional hybrid entities, where everything is interconnected and where different technologies are used to acquire, transmit, exchange, process, use, and store information. We need to look at these multidimensional information and communication system entities in a new way. The information and data models we use, and their functionalities, require communication systems that consist of air-space-land-sea communication networks (ASGM), in which the different components work seamlessly together. These digital, multidimensional hybrid systems include several parts and functions, such as various digital platforms and their services; a range of technologies, including artificial intelligence (AI), machine learning (ML), and virtual reality (VR) solutions; blockchains; digital twins; quantum technologies (communication, cryptography, and computing); metaverse environments; and various data center functions. These environments also use the Large Language Model (LLM). Our new smart devices must be developed to adapt and operate in these environments, using the services they provide, and they must function regardless of time and place across all usage contexts, including extraterrestrial networks. Data center capabilities, MECs, and edge systems are also rapidly evolving due to emerging communication requirements. Quantum computing, cryptography, and communication, alongside ML, are becoming available, and their integration must be explored, as they introduce additional challenges for device design and functionality. We must ensure sufficiently low transmission and synchronization latencies so that physical and virtual environments can interact seamlessly without failures. In this article, we examine smart devices designed for future communication environments. These devices will utilize artificial intelligence, machine learning, and virtual reality to support the services of future smart societies across operational domains, including those beyond Earth. We also analyze cybersecurity threats to end-to-end services in different use cases and explore device-level functional enhancements.

Keywords: Smart devices, Artificial intelligence, Virtual reality, Quantum computing, Quantum cryptography

1. Introduction

The living environments of future smart societies form many multidimensional hybrid communication environments, where users may not be able to know or see what kind of communication systems they are using in their everyday services. It cannot be seen or known whether air-, satellite-, ground-, or maritime-based communication networks and services are being used, because everything is connected to everything, and the services in use may be located on other continents (Figure 1). Multiple service providers use the same telecommunications network resources, including telecom operators, as well as subcontractors and stakeholders. This means that the entire future telecommunications environment will be multidimensional from the sky to the bottom of the sea, with connections everywhere and interfaces to many information systems and networks simultaneously. This will all work automatically in the future (Ericsson, agentic AI) (Akash Takyar). Communication systems pass through multiple countries, and service providers also use different data center resources to provide their services from these countries. This also means that telecom operators and service providers may use different recommendations and standards to develop their networks and services in these different countries. People use services with different security levels from these telecom networks regardless of time and place, which poses many additional challenges for developers and designers of information security systems. People may use their one smart device in a variety of ways to access multiple services, even if these services have different security levels. This means that managing and monitoring these telecom networks and the services provided through them, as well as their users, is particularly challenging. These new operating environments also offer a lot of new opportunities for cyber attackers to attack our systems and services through multiple routes and different devices.

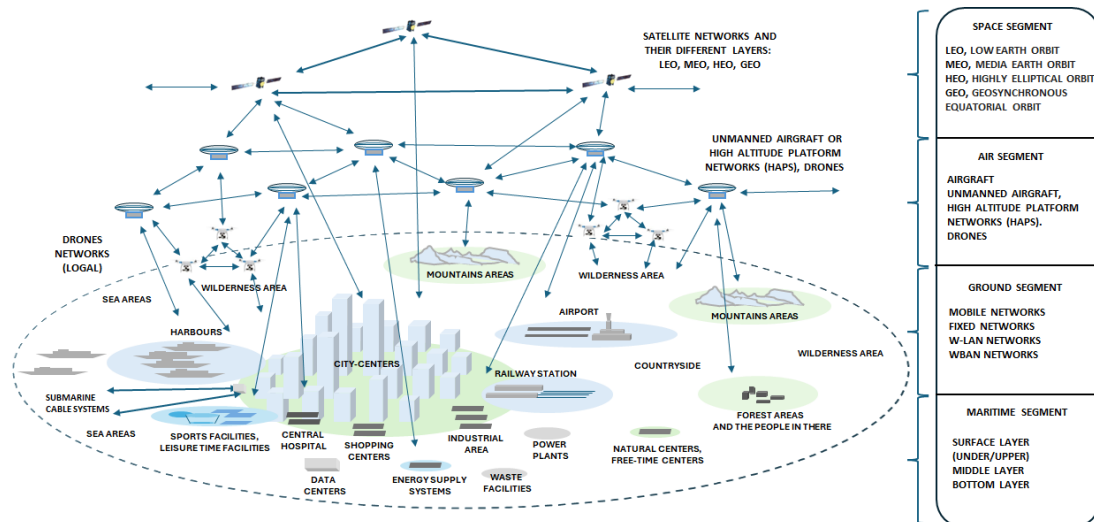


Figure 1: Our future societies' digital living environments and communications layers (EU-ECHO 2) (EU Space Programme) (IEEE, Oltjon Kodheli) (IEEE, Xufei Ding)

Artificial intelligence (AI) can be used in communication networks for many different purposes. It can be used to analyze information from data sources that we want to send to recipients through communication networks by performing multimodal data extraction on the sender side, encoding it, and decoding and reconstructing the data on the recipient side (Figure 2). Also, cyber attackers use AI in many ways to attempt to find vulnerabilities and attack opportunities from various parts of communication networks, their services and systems, and work environments, including all users' devices (EU-2024/1689) (EU-2022/640). As we evolve our digital communication and information environments through virtualization, slicing, and new virtual reality capabilities where everything is connected to everything, we are at the forefront of multidimensional communication and service environments. These different functionalities mean that the environment gives cyber attackers many more opportunities to attack these multifunctional environments than was previously possible for the networks of that time. These new functionalities in communication environments also mean that we need to take a deeper look at the devices and systems we use and to develop their architecture to meet these new requirements, functionalities, and cybersecurity challenges. Quantum computing, quantum cryptography, and quantum machine learning need to be researched and tested alongside these devices, as they are becoming integrated into this new generation of smart devices. We must strive to optimize the functionalities of new types of smart devices. Quantum computing, quantum cryptography, and machine learning must also be taken into account in new types of intelligent device architectures (IDQ) (ITU-T).

We need to optimize the functions of new types of smart devices, such as computing power, the use of artificial intelligence, the use of virtual reality, and energy efficiency. Since our smart devices provide a variety of services and are loaded with a lot of data, they are really loaded. We need to optimize and significantly reduce their load. One way to reduce the load is to form a semantic representation of the transmitted data and send it to an encoder, which encodes the data by optimizing its size; on the receiver side, the transmitted data is decoded and reconstructed accordingly. The goal of these processes is to optimize the load and improve the functions of these new types of smart devices in these new operating environments, Figures 2 and 3. Edge and MEC architectures and operations also need to be rethought due to the connectivity and cybersecurity requirements of these new types of smart devices and the new types of services they provide. These new types of end-to-end communication systems form the communication layers in these multidimensional (3D) environments where everything is interconnected to everything. This requires new types of analyses, control, and monitoring models and systems that can seamlessly analyze and manage data, prevent unauthorized access to data, prevent cyberattacks, and protect and keep our information systems operational under all conditions, end-to-end, across all communication environments. For these purposes, we use agent-based RAG concepts (Akash Takyar, Agentive RAG), which means that devices and systems can communicate with other systems and devices and react to their functionalities, adapting their behavior to be compatible with the various use cases of future digital environments and the various use cases of the systems there.

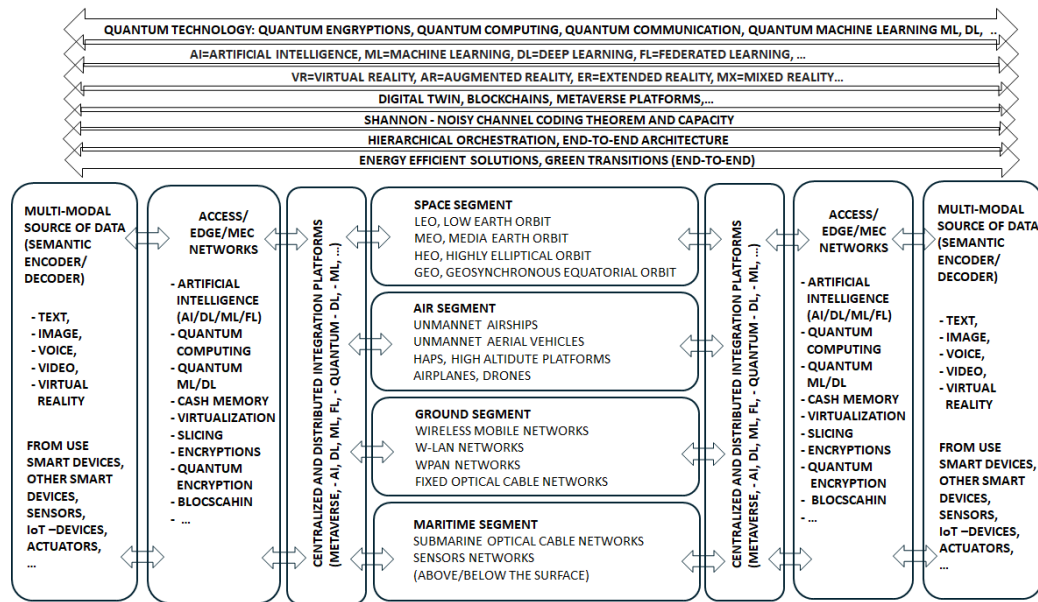


Figure 2: End-to-end communication segment layers and their functionalities

1.1 The Research Question

The research question of this study is: Can our new smart digital devices and systems be safely used in the multi-layered virtual environments of the future, where numerous services are available to us anytime and anywhere and artificial intelligence is used throughout our service and communication systems to enhance and improve our services?

2. Objective and Grouping of Paper

In this study, we use scenarios and use cases related to multimodal data in virtual reality and virtualized environments in different situations where collaborative information exchange with different people and parties is needed, and it needs to be done securely.

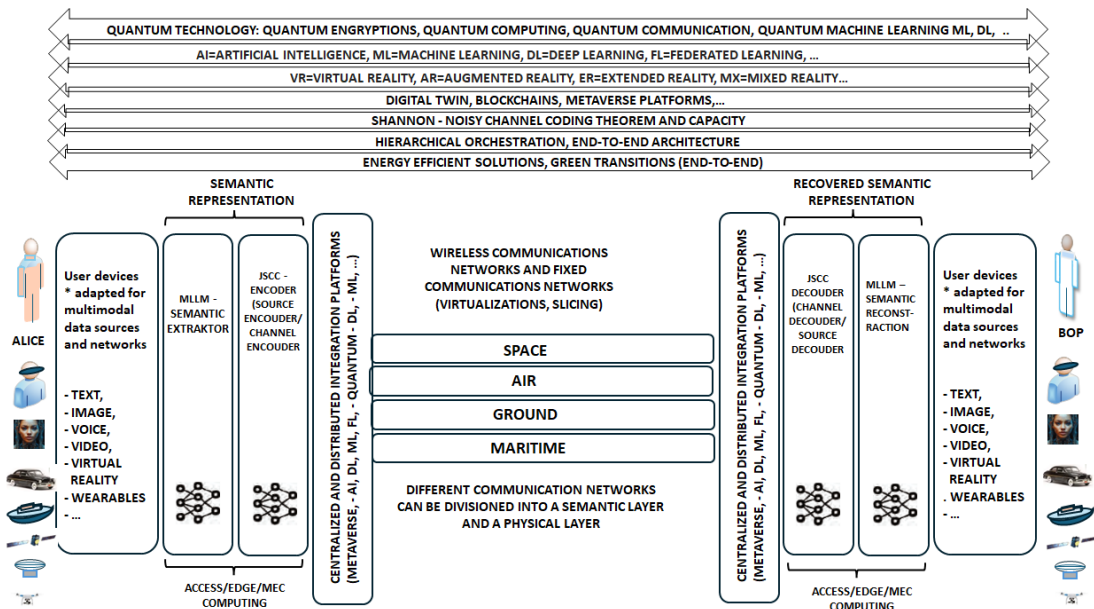


Figure 3: Secure MLLM semantic communications enabled Air-Space-Ground-Maritime networks, end-to-end, using AI agentic RAC and quantum technologies. MLLM (Multimodal Large Language Models) (IEEE, Huaifeng Shi) (IEEE, Mingkai Chen)

Methodology: We have used the Enterprise Architecture (EA) framework and its methodological models. We have also used Proof of Concept testing environments (Aarne Hummelholm et al. pp. 142–148) to identify the

improvement needs of the mobile devices people use. We also looked at the EU Tempest Directive guidelines to see what we need to also consider when designing our new device.

The structure of the study is as follows: Chapter 3 discusses numerous services that utilize virtual reality and different platforms in future societies in their multi-layered virtual and cloud-based digital environments, and the use of services is independent of time and place, even when service users are far from their workstations and offices. Chapter 4 discusses conducting threat analyses and modelling for these multi-layered platforms in virtual and cloud-based digital environments. Chapter 5 concludes this article, presents our solution model, and suggests future work.

3. Multimodal use Cases for Future Communication Environments at Different Levels

We use different technologies in communication environments across different segments. Multimodal data includes text, images, audio, video, virtual reality data, wearable data, IoT and sensor data, and so on. This multimodal data can include sensitive information from various fields, such as economic, industrial, medical, and welfare data; banking data; or technical development data. This data will be sent to various parts of the world using various communication systems (Figures 3, 4a, and 4b). The use of services in our future society's multi-layered virtual and cloud-based digital environments will be independent of time and location. Service users can be far from their offices and homes. Therefore, new types of smart devices are needed that include secure MLLM semantic communication functions, artificial intelligence-based agent-based RAC techniques, and quantum technologies.

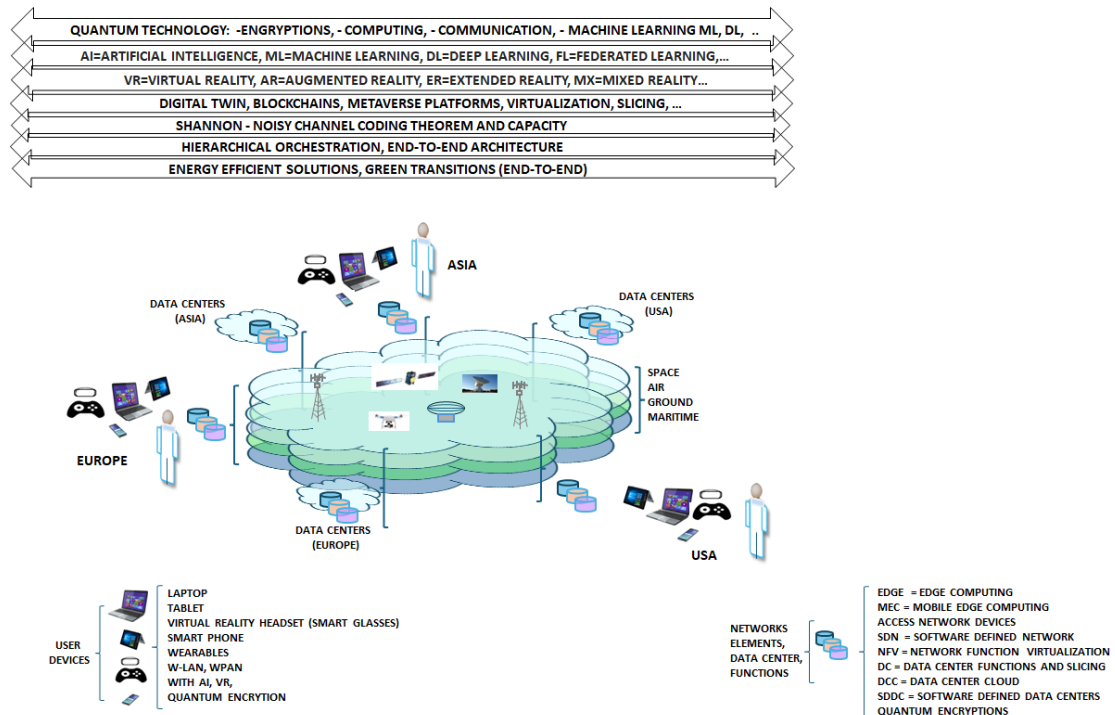


Figure 4a: A real-time business meeting with employees from around the world

We are also currently transitioning from 4G to 5G and 6G into mobile networks. This transformation brings with it technical challenges, as well as challenges related to privacy, accessibility, sustainability, and cybersecurity, but at the same time it opens revolutionary opportunities to develop services in our societies to be even more efficient, diverse, flexible, and energy efficient. For example, for various needs of rescue operations, we can easily introduce new types of mesh networks implemented with smart devices on an ad-hoc principle, without other networks. These solutions and new functions of the devices give us new opportunities and help us work much faster and easier in many situations. These new types of smart devices allow all of us to use services in a completely different way than before, and faster than today, regardless of time and place. Critical situations we do not need other networks and their services at all.

In Figure 4a, we see one example of the use of this new type of smart device, with its new functions, in meetings where people from companies are in various parts of the world (Nokia) (Ericsson). They can use a normal video conference connection with audio, video, and images. They also have virtual reality glasses that they can use,

but which are challenging to use due to delays in data transfer. The use of virtual reality glasses in meetings comes into play when the companies involved in the meeting are doing development work and the people from the companies want to see the results of their work up close. The connections used are complex and pass through different networks and countries (Figure 4a). The big challenge is that the inside information of the companies must not be available to parties outside the meetings and that hackers cannot access information. The connections must be encrypted, for example, with quantum encryption. This also increases data transfer delays. There may be many teleoperators and service providers who are responsible for making this type of connection through different countries using different communications networks. This gives more cybersecurity challenges to these types of connections.

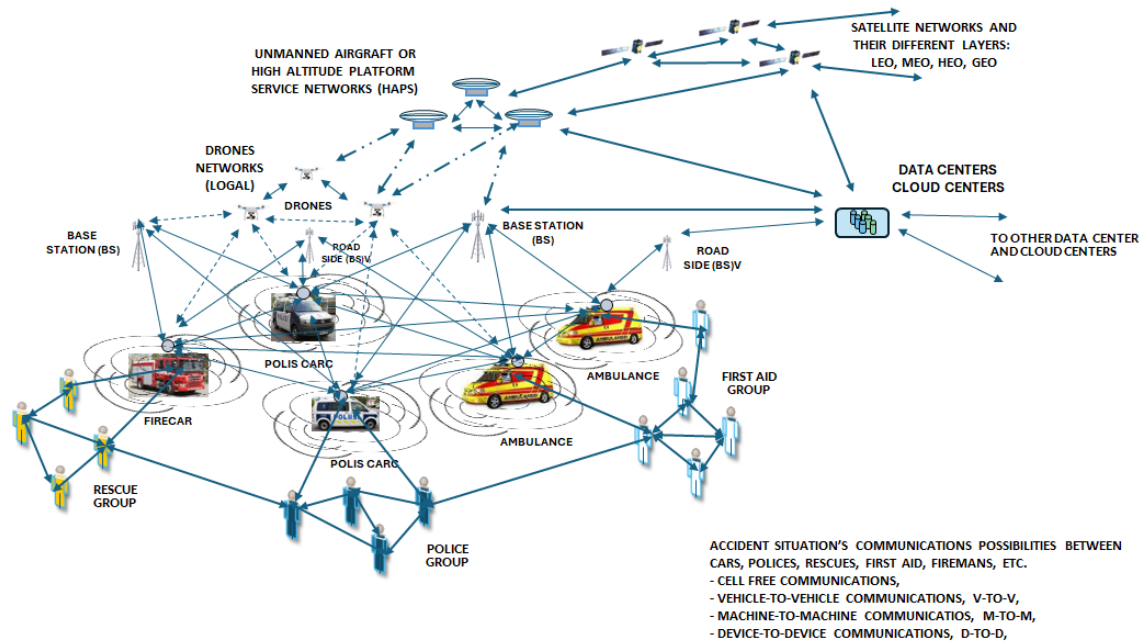


Figure 4b: A rescue operation in the field (Aarne Hummelholm et al., ECCWS 2025) (EU-NIS) (EU-GDPR) (EU-MDR) (EU-Galileo)

Figure 4b shows an example of the use of new types of smart devices that can form networks for rescue operations, for example, on an ad-hoc basis. The formed mesh networks operate without other networks, data centers, and their functions. The formed network is based on various functions of new types of smart devices (Aarne Hummelholm et al. p. 142-148). The mesh network is formed between user devices to user devices automatically without other networks when the necessary settings have been made in advance. If necessary, the network is connected to vehicles, which in turn are connected to each rescue operation command center and leader using various communication systems to get connections to the field (Figure 4b). Today, it is also possible to use direct connections from user devices to networks formed by satellite, HAPS and DRONE systems. Table 1 shows the technical requirements of different communication services in future service environments, which we need to consider when developing these systems and smart devices.

Table 1: 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
Augmented 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

There are direct connections between the field managers from the beginning. Figures 4a and 4b show this in critical situations, where every second counts for initiating and conducting rescue operations. The faster and more seamless launch of the field operations shown in Figure 4b is enabled by configuring the communication

settings on user devices. We can certify all users in advance and profile them based on their job responsibilities. This way, they have certain operations ready when they go into the field, and their profiles are visible to all users on the screens of their smart devices. This means we do not have to make any changes in the field, and we are ready to start the necessary operations quickly.

4. Making and Modelling of Threat Analyses

Figure 5 shows connections between users in multimodal communication environments. User devices, communication systems, data systems, and platforms are virtualized. In this model, artificial intelligence is used in all areas of communication and in all devices and systems to analyze and optimize all communication connections and prevent cybersecurity attacks.

Our new smart devices are connected to a wide range of sensors, actuators, IoT devices, virtual reality devices, home systems and sensors, other user devices, wearable devices, etc. The connections are wireless or fixed. For example, at home many devices are connected to home WLAN (Wireless Local Area Network) devices and, through them, to EDGE (Network Edge Device) or MEC (Multi-access Edge Computing) devices, as well as to operator networks via fixed or wireless connections. In this way, the user's smart devices are connected to these digital, multidimensional hybrid networks and entities, which can be divided into several parts and functions as needed (Figure 5).

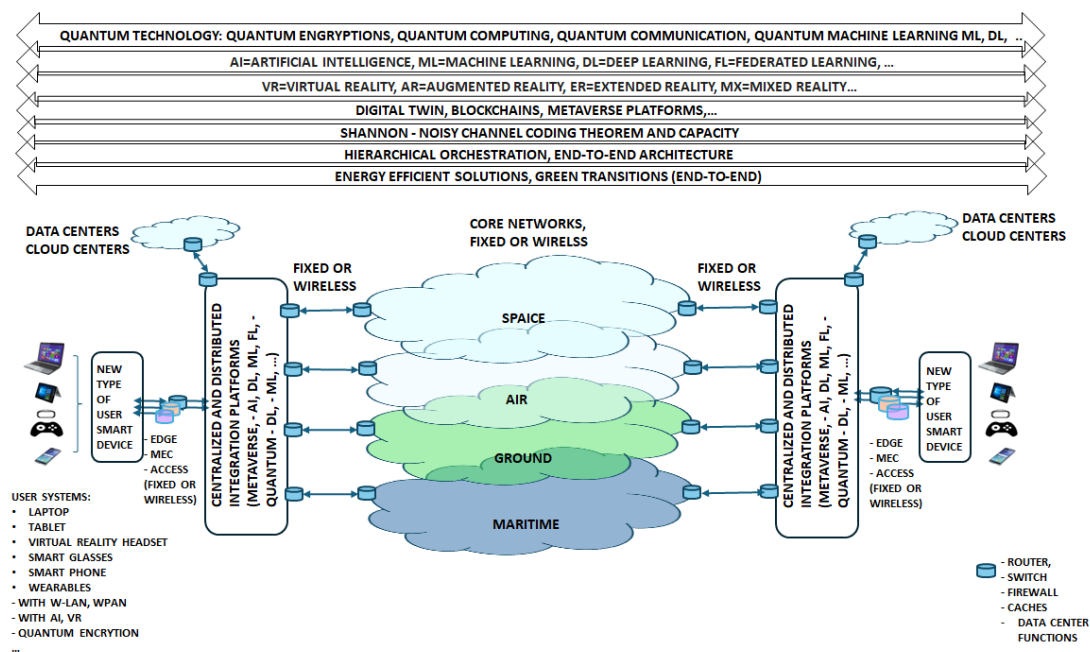


Figure 5: User-to-user communication connections in future multimodal environments

Some of these home systems are connected to the data centers of device suppliers via wireless or wired communication so that device suppliers can obtain information about the status and activities of home devices. Through all these connections and terminals, cyber attackers can attack our systems, even if our smart devices have encryption systems. This new environment offers cybercriminals, hackers, and state actors many new attack possibilities. The situation is only getting worse as they use different artificial intelligence (AI) concepts for their various attacks, as well as for vulnerability detection, dependency detection, detection of classified information, and so on in various parts of this multidimensional hybrid network. When we use wireless communication connections, cyber attackers use signal eavesdropping and interception methods. These methods have been used by state actors for a long time. Today, jamming is quite common among state actors around the world, including in Europe. Signal interception is used for many purposes, and users include state actors, cyber attackers, or criminals, etc. Through high-altitude communication systems, CPS spoofing and navigational deception are used quite frequently around the world through these communication routes. We have seen this from news reports on the international situation (IEEE, Miao Du) (Radware). State actors do it, and the purpose is to disrupt the normal operations of various states and companies. Wireless technologies offer the possibility of performing man-in-the-middle attacks on all wireless connections. Attacks against these wireless systems are easy to implement because they are difficult to detect if someone is doing something

alongside the connections. Side-channel attacks are also easy to perform in these environments. When state actors and cyber attackers use artificial intelligence and DRL (Deep Reinforcement Learning) (IEEE, Huaifeng Shi) to attack our systems, services, and system models, they can go faster inside our systems (Figures 1–5). Based on the information obtained, attackers perform more targeted attacks on our system models and try to find more backdoors for their attack possibilities.

Because we work in these multimodal communication environments and our communication connections go through multiple layers to data centers and cloud centers, cyber attackers and state actors can easily carry out eavesdropping and data leakage attacks to find the interesting information they want. When using artificial intelligence methods, they can easily conduct data manipulation attacks and privacy attacks. When cyber attackers and state actors use artificial intelligence methods, they easily find opportunities to conduct disruption attacks on their desired target. With the help of artificial intelligence, they find opportunities to get inside systems and devices and can easily conduct protocol attacks inside systems and devices. Finding such attacks is particularly challenging when we work in these multimodal communication environments and our communication connections go through multiple layers and paths to data centers and cloud centers, where services are potentially hosted by multiple service providers and where the information needed by users is stored.

The Access, MEC, and EDGE systems and devices of this future ASGM network must incorporate AI-based capabilities to detect, analyze, protect against, mitigate, and eliminate a wide range of cyberattacks. This is critical because all information flows through these systems and devices, as well as through users' smart devices, to networks and data centers around the world. If there is even one small vulnerability in these systems, cyber attackers will quickly find it using AI and quantum computing and exploit it for their own purposes. Figure 6 shows the attack vectors in our air-space-land-sea (ASGM) networks across its various segments and layers.

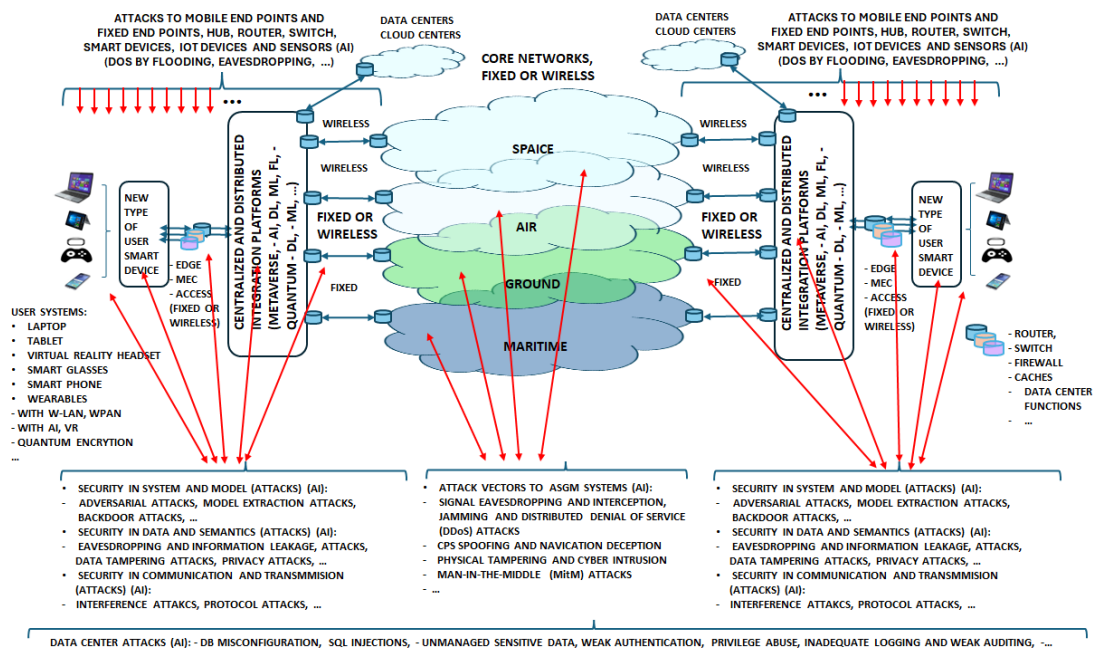


Figure 6: Our Air-Space-Land-Sea (ASGM) network and attack vectors against it (based on 5G threat vectors by Aarne Hummelholm et al.)

The management, control, and supervision of such multimodal and multilayered communication environments, user devices, communication systems, information systems and platforms, and cybersecurity-related protection systems in these virtualized and multilayered environments require good, functional analysis, control, and management systems for the network and its devices, as shown in Figure 7 as an example model (Aarne Hummelholm et al.). We need to get real-time information about our network situations and services and use artificial intelligence to create situational pictures faster and more broadly, to launch measures faster, and to collaborate to share information with different organizations working in these communication and service environments in their maintenance, servicing, analysis, and repair tasks.

Figure 7 shows two different operational centers: NOC and SOC. NOC is the network operational center, and SOC is the information security operational center. From the NOC, we see the real-time situation of the communication systems of networks and services, as well as the smart devices used. From the NOC, real-time information is sent to operators and service providers according to their needs. From the SOC, we see the real-time cybersecurity situation of networks and services, communication systems, and smart devices used. From there, real-time cybersecurity information is transmitted to various security organizations that are responsible for the activities of these areas in cybersecurity issues and respond to cyber-attacks as effectively as possible. For this reason, a real-time situational picture is important for initiating countermeasures, preventing cyber-attacks, and improving protection based on the analysis performed with AI.

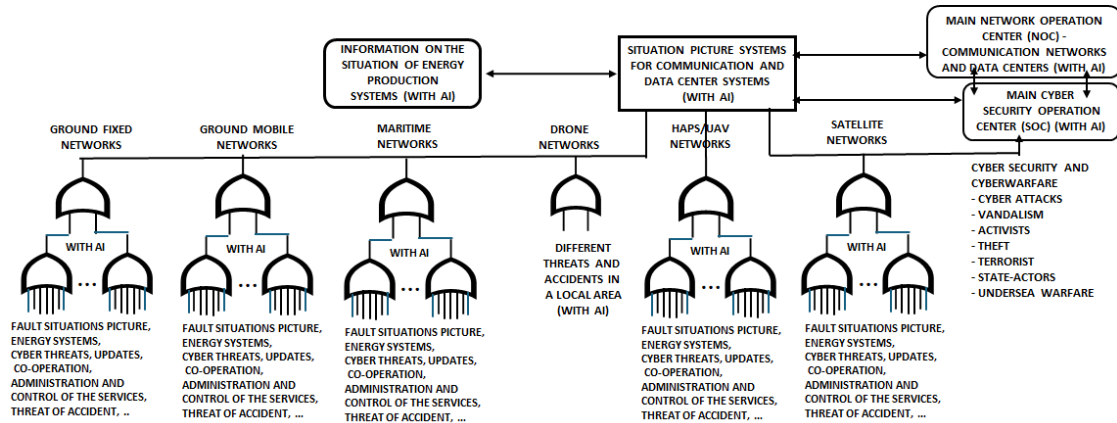


Figure 7: Architecture model of various network control and management systems at the principal level (NOC, SOC with AI and quantum computing) (Aarne Hummelholm et al., updated from the ECCWS 2025 article)

5. Our new Intelligent Smart Device Model

Figures 1–7 show how important and central the new smart terminals used by people are in these future digital multidimensional hybrid operating environments. A large part of the data flows passes through them, and various sensors, actuators, wearable devices, IoT devices, and other data sources are connected to them. Thanks to these functions, the device has become an increasingly central and important device that utilizes various services of future digital multidimensional hybrid operating environments and ICT operating environments.

Our new type of smart device includes functions that allow us to process data from incoming data streams (MLLM) and send the processed data to the recipient. The receiving device has corresponding functions for processing the incoming data. This method provides us with optimized data streams and energy-efficient data processing solutions on our smart device, as well as reducing the energy consumption of our smart device. We are also able to use these solutions to shorten the overall transfer times of data streams and improve the functionality of highly time-critical services.

Inside our smart device, we use artificial intelligence to analyze the device's functions and cyberattack potential, as well as to detect cyberattacks on our systems. We are developing these new smart devices with the use of quantum computing, quantum machine learning, quantum encryption systems, and EU-Tempest requirements in mind.

We plan to use Agentic AI to transform RAN optimization by enabling fully autonomous networks that manage themselves without human input (Ericsson, Agentic AI), so we need much deeper and faster AI-based analysis solutions to find out if something is going on inside the devices without our knowledge, even if it is not cyber attackers.

We also plan to use MCP (Model Context Protocol) in conjunction with LLM (Large Language Models) to provide a universal interface for reading files, executing functions, and managing contextual prompts on our new smart device.

One application of our new smart device is also the use of Agentic RAG functions, which improve the search and additional text creation process and enhance the use of MLLM models.

6. Conclusion and Future Work

6.1 Conclusion

The digital, multidimensional, and multimodal hybrid information systems of the future, where everything is interconnected and where different technologies are used to acquire, exchange, process, use, and store information, are particularly challenging in terms of functionality, usability, and cybersecurity (Figures 1–7). The same communication and service environments simultaneously give resources to multiple telecom operators, service providers, and stakeholders.

Our communication environments are changing rapidly, moving from 4G to 5G and eventually 6G in wireless technology. Extraterrestrial networks and services are already directly accessible from our smart devices. Our services are provided by multiple data centers and cloud service centers around the world. Such data environments offer attackers using artificial intelligence technologies a vast number of exploitable opportunities to attack our information systems and services from anywhere and at any time. Such future scenarios show us cybersecurity challenges that we must address with increasingly powerful analysis and protection tools to keep our systems and data safe from cyber attackers.

6.2 Future Work

We need to develop a testbed with robust integration platforms where we can evaluate, analyze, and validate our devices, systems, services, new protocols, and new quantum encryption systems much deeper used in these environments than before. We also need to test the use of artificial intelligence in conjunction with them because cyber attackers are using AI in their attacks in quite new ways. We need to evaluate and verify the use of quantum encryption systems in end-to-end mobile networks in such multidimensional hybrid computing environments (ENISA).

One of our research projects is to develop a secure new communication platform for our future smart devices, which will allow us to reduce the bandwidth requirements of data flows by modifying the information coming to smart devices through our new platform. After processing, the data is sent to communication networks (Table 1). At the same time, we will get energy efficiency solutions for our smart devices.

If we move to agent-based AI, it will revolutionize RAN optimization by enabling fully autonomous networks that manage themselves without human intervention. This means that we need to consider this possibility in the development of our future smart devices as well.

Ethical clearance: Ethical clearance was not required for the research.

AI declaration: I have not used AI in my work.

References

- 5trnhIDQ - ID Quantique, info@idquantique.com.
Ali M., et al (2023), Metaverse Communications, Networking, Security, and Applications: Research Issues, State-of-the-Art, and Future Directions, IEEE Communications Magazine September.
Chen M, et al, (2020) Secure MLLM Semantic Communication Enabled Air-Space-Ground-Maritime Networks, IEEE Communications Magazine July.
Ding X, et al (2025) QFMLNet: An AI-Driven Quantum Communication Architecture for 6G Space-Ground Networks, IEEE Communications Magazine July.
Du M., et al, (2025) HYShield: A Multi-Layered Security Framework for Air-Space-Ground-Maritime Networks in 6G Scenarios, IEEE Communications Magazine July.
ENISA, Post Quantum cryptography, Integration study, October 2022.
Ericsson, Agentic AI for RAN optimization: Pathway to autonomous networks level 5, <https://www.ericsson.com/en/blog/2025/8/one-6g-network-for-all-services--from-massive-iot-to-enhanced-mobile-broadband>
Ericsson, Explore the impact of 6G: Top use cases you need to know, Dec 19, 2024.
EU- 2022/640 of 7 April 2022, on implementing rules for the roles and responsibilities of the principal security actors, <https://eur-lex.europa.eu/eli/dec/2022/640/oj/eng>
EU- 2024/1689, AI regulation 13.6.2024.
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-ECHO 2, European Concept for Higher Altitude Operations (ECHO 2),

- EU-Galileo-Satellite Navigation, https://defence-industry-space.ec.europa.eu/eu-space/galileo-satellite-navigation_en
- EU-Space program, PRS, EUSPA 2021-2024, <https://www.euspa.europa.eu/eu-space-programme/galileo/services>.
- EU-Tempest, 25 March 2019, based on NATO standards SDIP-27, -28 and -29.
<https://www.eurocontrol.int/project/european-concept-higher-altitude-operations>
- Hummelholm A., et al. (2025) Aarne, E-health systems for remote and disaster-resilient digital environments, Proceedings of the European Conference of Information Warfare and Security, ACIL, Reading, UK
- Hummelholm A., et al., (2019) Cyber Security and Energy Efficiency in the Infrastructures of Smart Societies, JYU Dissertation 173, p.142-148.
- Hummelholm A., et al., (2021) Based on 5G Threat Vectors, By Ashutosh Dutta, IEEE, Future Network, Artificial Intelligence, and Machine Learning,.
- ITU-T Y.3800 series – Quantum key distribution networks – Role in end-to-end cryptographic services with non-quantum cryptography.
- Kodheli O. et al (2020), Satellite Communications in the New Space Era, March.
- Nokia, 6G system architecture: where innovation meets evolution for a more sustainable and connected world, 5 March 2025.
- Radware, 2025 Cyber Survey, Applications Security at the Breaking Point,
https://www.radware.com/documents/?utm_term=radwarereport&utm_campaign=Search_Brand_EMEA&utm_source=google&utm_medium=cpc&gad_source=1&gad_campaignid=1427682478&gclid=EAlaIqobChMI4sqvp4H0kQMVRE6RBR2SwBztEAAyAIAAEgKlu_D_BwE
- Shi H., et al, (2025) Diffusion Model Enhanced Deep Reinforcement Learning for Traffic Control in 6G Networks, IEEE Communications Magazine, July.
- Takyar A.,, Agentic RAG: What it is, its types, applications and implementation, LEEWAYHERTZ,
<https://www.leewayhertz.com/agentic-rag/#Looking-ahead-Challenges-and-opportunities-in-agentic-RAC>