Cyberwatch Finland

WHITEPAPER 2025

THE FUTURE CHALLENGES AND SOLUTIONS OF CRITICAL COMMUNICATION IN MODERN SOCIETIES

Cybersecurity is Built by Small Actions and Management of Large Concepts

CONTENT

Cyberwatch WHITEPAPER

PUBLISHER	Cyberwatch Oy Nuijamiestentie 5 C Helsinki, Finland
CONTENT	CEO Aapo Cederberg aapo@cyberwatchfinland.fi
LAYOUT	PuulaMedia / Mari Riepponen
ILLUSTRATIONS	AdobeStock
PRINT	Scanseri Oy, Helsinki
ISSN	2490-0753 (print)
ISSN	2490-0761 (web)

Introduction

Technology is developing at a faster pace than ever before, while the war in Ukraine and others elsewhere are morbidly highlighting the challenges that critical infrastructure faces in such difficult conditions. New regulation is trying to meet these challenges, especially in the EU, but often also imposes new ones in the process. A key part of critical infrastructure is critical communication, the future of which is very complex, but that does not mean it cannot be prepared for. In fact, that is precisely what this white paper is aiming to do. There are lessons to be learned from the conflicts around the world and emerging technologies should be put to use based on them.

Data is a key element in both companies and critical services of a society. According to the EU Data Strategy, the possibility of widespread access to and use of data is a key prerequisite for innovation and growth. The EU's goal is a secure and dynamic data economy, in which the collection and utilisation of data are a key part of organisations' operations. Most of the global added value is created through digital and technological innovations. The utilisation of data offers opportunities for value creation and productivity growth in all sectors of the economy.

The data economy and data centres are closely linked. Data centres are essential for enabling the functioning of the data economy, as they provide the infrastructure for storing and processing data. The importance of the data economy is emphasised by the fact that Prime Minister Orpo's Government will commission a roadmap report on the data economy during the period 18 June – 31 October 2025. The Government aims to implement a broad, strategic program on the data economy, with quantum computing, high-speed wireless networks, health data, cyber security, artificial intelligence, and the promotion of the data economy and the availability of data for the use of artificial intelligence at its core. In this context, a secure communication infrastructure plays a key role.

The utilisation of data offers opportunities for value creation and productivity growth in all sectors of the economy.

The third key driver of change is the use of artificial intelligence in networking. Artificial intelligence can be used to outsource the understanding of people. Artificial intelligence and data can be used to develop intelligent advisors, teachers, or assistants for users that can then help in complex decision-making situations. Generative AI has already become a widely used tool in industry, public administration and people's everyday lives. Artificial intelligence and machine learning have also become available to both cyber attackers and cyber defenders. In the ongoing transformation of data and telecommunications, the aim is to build a data- and network-centric operating concept that utilises artificial intelligence, which can be used to enhance decision-making at different levels of operations in both military and civilian environments.

1 Regulation Directs Development

When imagining the requirements for future products, it is best to start by looking at what they are right now. The logical first step is to check the legislation, in this case the NIS2 directive and Finland's recently passed cyber law that stems from it. The most relevant requirements for communication technologies include protection of communication networks and systems, separation of said systems from any outside environments, access control and regular updates. Last but not least, the systems have to be usable in times of serious disturbances and unusual conditions as well. This calls for resilience, both digital and physical.

There are several ways to approach the need for resilience. First and foremost, systems need to have backups in case of a failure. Secondly, repairing them has to happen quickly. Dual-use systems are one way to ease this burden, since interchangeable components and personnel between civilian and military system maintenance can greatly improve the speed at which systems can be repaired. It also allows the military systems to be scaled up during wartime quicker than what would otherwise be possible. Dual-use products are not without issues, namely the differing requirements of security when comparing traditional civilian and military use cases, but developing such products does still provide a competitive edge to any companies that wish to succeed in the current geopolitical environment.

What needs to be kept in mind, however, is the risk-based approach to such products. That is what the cyber law and the Critical Entities Resilience Directive call for, but it also is the key to understanding the security requirements of military use cases. All data should not be processed on the same device, since gaining access to it would then instantly provide an attacker with everything. The security of a system is only as strong as its weakest link, so segmenting and access control are essential for security. This is true for critical infrastructure as well, and separating systems from one another can be an effective way to prevent single threats from taking out entire capabilities.

The next step in the regulatory process is related to the Regulation of the European Parliament and Council on horizontal cybersecurity requirements for products with digital elements. On the basis of this Cyber Resilience Act, the national implementation will be devised during 2025. The Cyber Resilience Act is based on developments related to cyber security, in which devices and software are increasingly exposed to cyberattacks. The overall objective of the Cyber Resilience Act is to create the right conditions for the development of secure products with a digital element, ensuring that there are fewer vulnerabilities in devices and software and that manufacturers take security considerations seriously throughout the product lifecycle.

Another goal is to increase visibility into the cybersecurity features of products for device users. The Cyber Resilience Regulation is directly applicable and does not include any national room for manoeuvre. Requirements for the use of cyber security certification systems and the authorities' supervisory and notification responsibilities can be set and defined nationally. The Act and its implementation create significant requirements for action for operators in the sector.

The security of a system is only as strong as its weakest link, so segmenting and access control are essential for security.

2 Key Lessons from the War in Ukraine and Recent Cyber Operations

The war in Ukraine has first and foremost shown us how diverse the methods employed in modern warfare are, and how quickly they can develop. At the start of the war Russia was attacking anything and everything, but since then the attacks in cyberspace have become more precise and targeted. Much more emphasis is placed on gathering intelligence and tailoring the attacks for each target to achieve the best possible results. They are also more tightly connected to military and information operations than before.

Ukraine had already improved their cyber capabilites during the years leading up to the full-scale invasion of 2022. For example, automated process control systems and their corresponding cybersecurity mechanisms were deployed. These systems have successfully provided a high level of protection and functionality under conditions of armed aggression. In addition, the largest operators agreed on permitting national roaming to ensure the resilience of networks. According to Ukrainian sources, another key aspect of a successful cyber defense is, perhaps a little ironically, the effective use of offensive cyber capabilites. It seems that attack is the best defense in cyberspace as well.

The key ideas behind this thought are deterrence, pre-emptive strikes and effective retaliation. In an active state of war, deterrence takes a backseat, but especially pre-emptive strikes are emphasized, since disrupting the enemy capabilities before they can stage more attacks is arguably the most effective form of defense.

The most vulnerable targets for Russian cyber-attacks have been different parts of Ukrainian critical infrastructure. Attacks have been going on for over a decade now, and new ones are constantly being conducted. The most effective operations have resulted in widespread blackouts, complete shutdown of communications networks and growing public distrust on both governmental institutions and private companies alike. This highlights the immense importance of resilience in civilian infrastructure. Although not all attacks in the cyber domain are directed at civilians, they often provide easier targets due to more relaxed security measures. Russia has recently shifted their focus towards anything even indirectly connected to the theater of war, including attacks on service providers. These are aimed at maintaining a low profile while sustaining a presence in systems related to warfare and politics. Hackers are no longer merely exploiting random vulnerabilities but are now deliberately targeting areas critical to the success and support of military operations.

The success of hacker activity in the commercial sector is also explained by the fact that the Armed Forces of Ukraine increasingly assimilate and adapt commercial technologies for military use. This makes pre-emptive cyber operations targeting such technologies a strategically promising direction for the adversary in the near future. In 2024, Ukraine handled over 3 million information security incidents. 4315 of these were confirmed as cyber operations. The growth from 2023 was almost 70 %.

The adoption of standardized (unique) hardware and infrastructure within organizations significantly enhances resilience and facilitates rapid recovery following cyber incidents. The importance of co-operation and support from the private sector, volunteers and especially partner states has been proven throughout the war in Ukraine. Russia as an adversary only understands power and the only way to affect its actions is projecting force in various domains. Cyber is one of these, and projecting power in it is necessary for both Ukraine and any nation targeted by Russia's offensive operations. Because of the war, Russia and Ukraine are developing roughly 10 times faster than non-warring states when it comes to cyberwarfare, so keeping track of developments within their conflict is the key to staying up-to-date on current cyber capabilities and trends.

The adoption of standardized (unique) hardware and infrastructure within organizations significantly enhances resilience and facilitates rapid recovery following cyber incidents.

The cyber domain has been present in other conflicts as well. Pakistan and India used cyberattacks to compliment other operations during their short clash this spring, and Israel and Iran have done the same in June. During the first conflict, Pakistan was very active in conducting offensive cyber operations, with some sources claiming that over 1,5 million attacks were launched against Indian targets. Pakistan proclaimed that their attacks were a massive success, the results supposedly including a blackout in 70% of India. The wildest claims have later been proven to be false, but Pakistan successfully utilised them in their information operations before that. A clear parallel can be drawn to how Russia ties their information and cyber operations together. Most of the successful operations were just basic denial-of-service attacks targeting governmental and private sector websites in India. The retaliatory actions by India were very small, possibly indicating that the country does not have cyber capabilities that could directly compete with Pakistan.

As for Iran and Israel, it is a different story. Both countries have been investing in cyber capabilities for years or even decades, and both are also supported by various non-governmental hacker groups. The amount of cyberattacks in Israel increased by almost a factor of ten after the air strikes started in Iran. Most of the attacks were once again relatively harmless denial-of-service attacks or website defacements. An interesting aspect of the attacks is who is making them. Most of the attacks are coming from third parties, such as pro-Palestinian groups or Islamist hackers.

It is very difficult to get any sort of accurate information about attacks on Iran, since the country essentially shut itself off from the internet fairly early on. It is an interesting strategy for avoiding attacks, but so far it is difficult to assess its effectiveness. Before the shutdown, however, there was reportedly at least one major strike that was successful. An Israeli group managed to shut down most of Iran's bank transfers. It is difficult to find out the actual scope of the disruptions, but many Iranian media outlets reported widespread currency disruptions and difficulties for citizens to access their accounts or withdraw money.

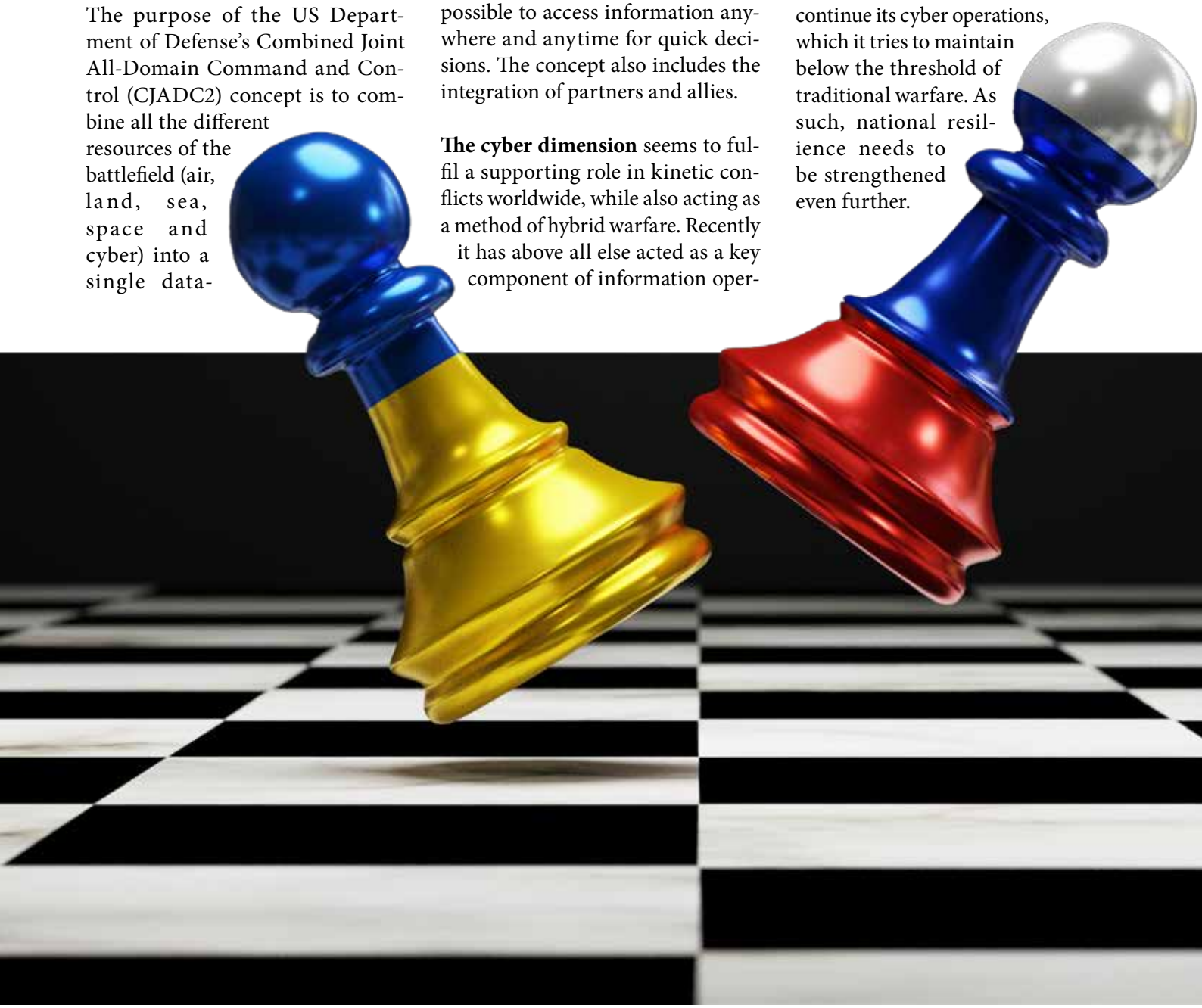
In war and conflicts, the role of intelligence is emphasised. For Ukraine, for example, intelligence is just as important as the material aid

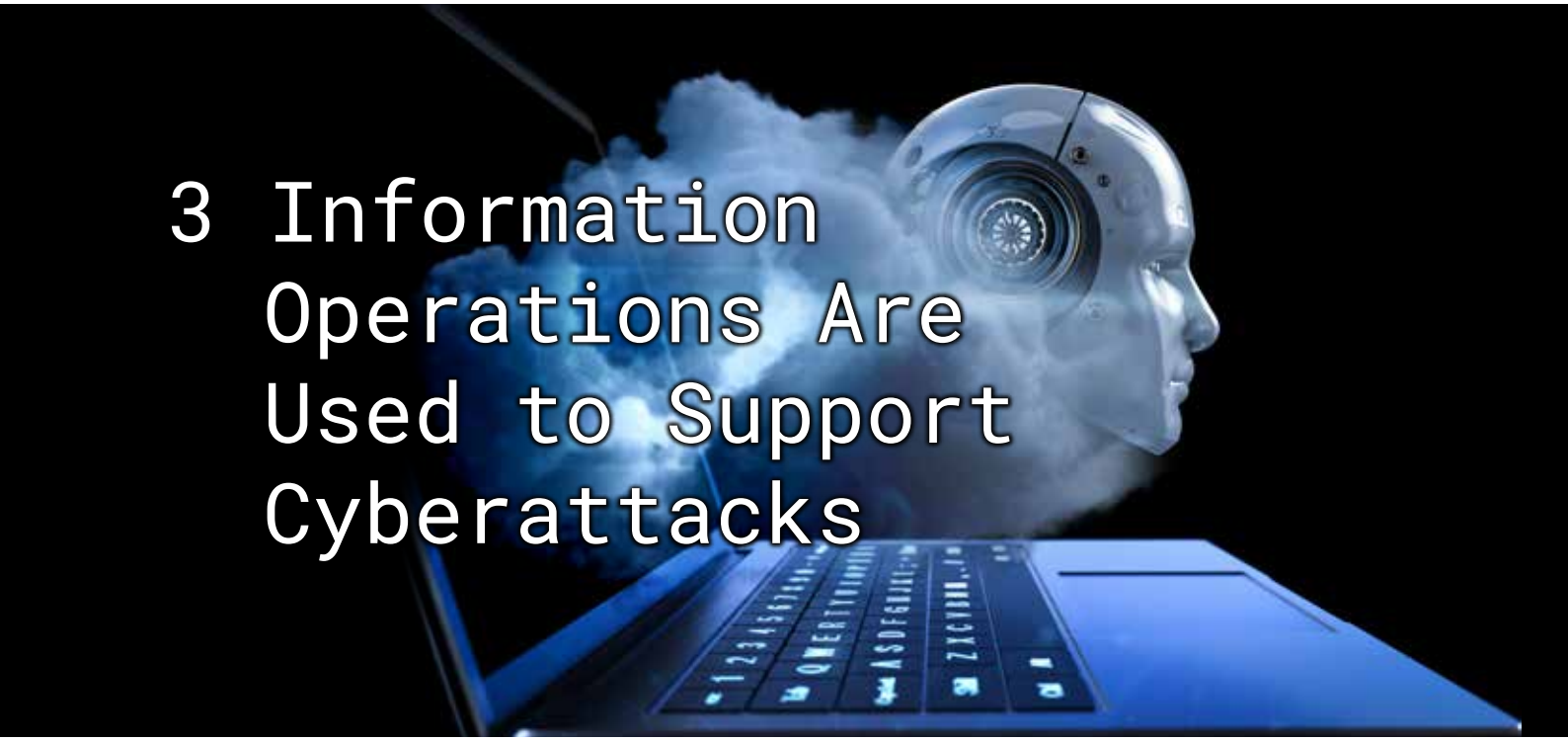
it receives. Strategic intelligence provides Ukraine with a picture of Russia's strategic-level objectives. At the operational and tactical level, intelligence can be used to direct the operations of different services, including cyber operations. Performance in the intelligence environment requires mastery of the communications sector. The battlefield is filled with numerous systems and actors. Fighters, weapon systems, manned and unmanned aircraft, land and sea vessels, and communication equipment form a dynamic and networked entity.

In the United States, the importance of communication and data collaboration has been noticed. The purpose of the US Department of Defense's Combined Joint All-Domain Command and Control (CJADC2) concept is to combine all the different resources of the battlefield (air, land, sea, space and cyber) into a single data-driven, integrated and AI-supported network entity. The aim of the concept is to improve situational awareness on the battlefield, speed up and refine decision-making and enhance military operations by enabling seamless information sharing and communication between different actors and systems. This makes it possible to access information anywhere and anytime for quick decisions. The concept also includes the integration of partners and allies.

Performance in the intelligence environment requires mastery of the communications sector.

The cyber dimension seems to fulfil a supporting role in kinetic conflicts worldwide, while also acting as a method of hybrid warfare. Recently it has above all else acted as a key component of information operations. When it comes to Russia, it seems that most cyber resources are directed against countries supporting Ukraine, rather than Ukraine itself. This can be explained by the ability to strike against Ukraine with kinetic means, which is not true of other targets in the West, although one could make a case for sabotage and the damaging of data cables in the Baltic Sea being kinetic operations. Just like within Ukraine itself, communication systems seem to be a priority target for Russian operations in nations supporting Ukraine as well. Cyberattacks will continue to have a significant role in hybrid warfare. Even if a ceasefire in Ukraine would come into effect, Russia would continue its cyber operations, which it tries to maintain below the threshold of traditional warfare. As such, national resilience needs to be strengthened even further.





3 Information Operations Are Used to Support Cyberattacks

Civilians are better targets for information operations as well, and Russia has increasingly linked those to cyber-attacks, as seen in the most effective results of operations mentioned earlier. Russia's information operations outside Ukraine have likewise been targeting civilian societies in an attempt to change public opinion towards narratives that Russia could better exploit. This includes interfering with democratic elections and political decisionmaking in the West, and some would even go as far as to say that Russia is practicing "election interference as a service." This means that certain politicians are contacting Russians to ask for support in the form of information operations that would help them get elected.

Russia makes extensive use of artificial intelligence in its information operations to produce endless content for social media and other similar platforms. Just two years after the publication of AI language models, there have been cases of malicious actors using generative AI to mass-produce harmful and false narratives. Now, Russia's obvious attempt is to contaminate AI chatbots with the propaganda it produces. Russian platforms spread lies by instructing AI models to mass-produce false narratives – for example, by using AI to create thousands of articles containing disinformation and to publish them online.

A Prompt infection attack targets Large language models (LLMs) by inserting malicious or misleading text into inputs, causing the LLM to produce unintended or harmful results. This method is used to manipulate and distort the operation of the LLM. Synthetic data content (e.g. deepfake videos) is increasing rapidly on various media platforms. It can consist of different types of content, such as images, videos, audio, and text. The technology used to create synthetic content is often trained on existing, real-world content found online. This means that it looks realistic and is very difficult to distinguish from genuine media content. In the hands of malicious actors synthetic content has a significant impact on our information security.

The Russian-based Pravda network is an important actor in the world of Russia's hybrid warfare. The network consists of 182 unique internet domains and subdomains targeting at least 74 countries and regions and 12 commonly spoken languages. It is estimated to produce more than 3.6 million pro-Russian disinformation articles annually. As a result, search engines and LLM-based artificial intelligences (e.g. ChatGPT) thus repeat Russian propaganda.

Russia is also using AI for reconnaissance and exploitation in cyber operations. Despite the use of AI and other developments in technology, human factor remains the most vulnerable link in the cybersecurity and managing vulnerabilities chain. Raising cyber awareness and maintaining a high level of cyber hygiene among personnel remains essential. Phishing attacks, malware deployment, and the creation of botnets are among Russia's leading tactics for information theft and disruption of information and communication systems at this stage of the conflict. Hackers are increasingly targeting messenger accounts to spread malware and launch phishing campaigns, aiming to compromise as many users as possible. Among a victim's contacts, there may be high value targets whose messaging histories are of particular interest to the aggressor nation's intelligence services.

4 Future Communication Solutions as a Strategic Capability in a Global Context

The war in Ukraine has definitely taught a lot about the meaning of resilience and how current communication systems work in a wartime environment. But what about the future? To be able to have a vision of what the requirements and possibilities for communication will be in the coming years, it is not enough to just study the events that have already passed, or even the ones that are currently unfolding. Instead, it is possible to draw some conclusions on what the requirements for communication in the future might be by taking a look at what is and what is not working right now, as well as what kinds of possibilities emerging technologies will provide.

4.1 The Need for Secondary Systems

First of all, the need for secondary systems is not going anywhere. In a conflict situation, whether it be kinetic or cyber in nature, eventually an attack will succeed in disabling at least some parts of a system. When that happens, resilience steps in. It means there must be a backup solution while the primary one is being repaired or replaced, which also needs to be as easy and fast as possible. One of the best ways to achieve this are dual-use technologies. If something can be used both by the military and the civilian society, that means there will be more of them around, making sure the logistics chains are not stretched too thin. It can also provide an opportunity to transfer a system from civilian to military use or the other way around and means parts from one can be used in the other. Regardless of whether the system is in civilian or military use, it is important to remember that effective resilience requires personnel in addition to components to be close by, otherwise repairs cannot be completed quickly.

The rapid militarization and integration of commercial technologies into military operations also introduce new security challenges. Many dual-use systems, originally developed for civilian use, lack the resilience and protection required for combat conditions. Especially resistance to electronic warfare is important. Ensuring proactive security assessments and adapting these technologies to military needs is essential. Going forward, it would be wise to prepare for this already during the development process. New products can be designed with dual-use in mind, especially if it is clear how they will be used in both contexts.

Ensuring proactive security assessments and adapting these technologies to military needs is essential.

The use of secondary systems is emphasised in active war zones. Today, a zone about 40 kilometres deep from the front line has formed on the Ukrainian front, where devices using the electromagnetic spectrum can hardly be used due to interference and spoofing. In addition, electronic intelligence immediately pinpoints the location of radios, links, and other transmitters. That is why fibre optic drones have been developed, since they do not need radio or satellite connections for control. In this area of the front line, the transmitter parts of equipment are usually placed in bunkers. In addition, easy-to-use fibre optic connections and inexpensive field radios are needed for tactical-level communication. This is because radios are short-lived in an environment of strong electronic warfare. At the same time, especially when looking at the war in Ukraine, it has become clear that civilian networks are widely used as backup systems in military operations. Another cost-efficient solution for a backup system for the new Virve 2.0 could be a network utilising a low-band spectrum.

4.2 The Need for Customisability

Systems need to be customisable for different use cases and targets. Since different users will obviously have different use cases for the product, it must be easy to adapt it to those needs. When developing a dual-use product from the ground up, this has to be kept in mind. Quite often it can mean that a system used primarily by the civilian society needs to have its security improved when it is transferred into military use. Network slicing can be a part of the solution for critical services – delivering priority service, lower latency and faster speeds. In network slicing, a section of the network is separated from the rest and made accessible for the client in question only, making sure other network traffic has no impact on the connection of the client, kind of as if they were driving on their own private road instead of the nearby highway full of traffic. The slicing could possibly be used to increase security as well, by cutting off the part of the network used by the military from its civilian counterpart, for example.

The Open Radio Access Network is an emerging technology that can be used to optimise the radio network with the help of open interfaces and an advanced division model for radio network functions. For example, some of the base station's functions can be transferred to the cloud so that it can distribute the available radio capacity more efficiently to other base stations. The benefit is better compatibility of the internal interfaces of radio networks between different operators. The Open-RAN concept also enables the rapid construction of light radio networks, utilising the processing of network functions in cloud services and COTS components. The concept would be useful in the dynam-

ically changing combat situations of military operations. The open radio network concept will also be an important capability in terms of the 6G environment.

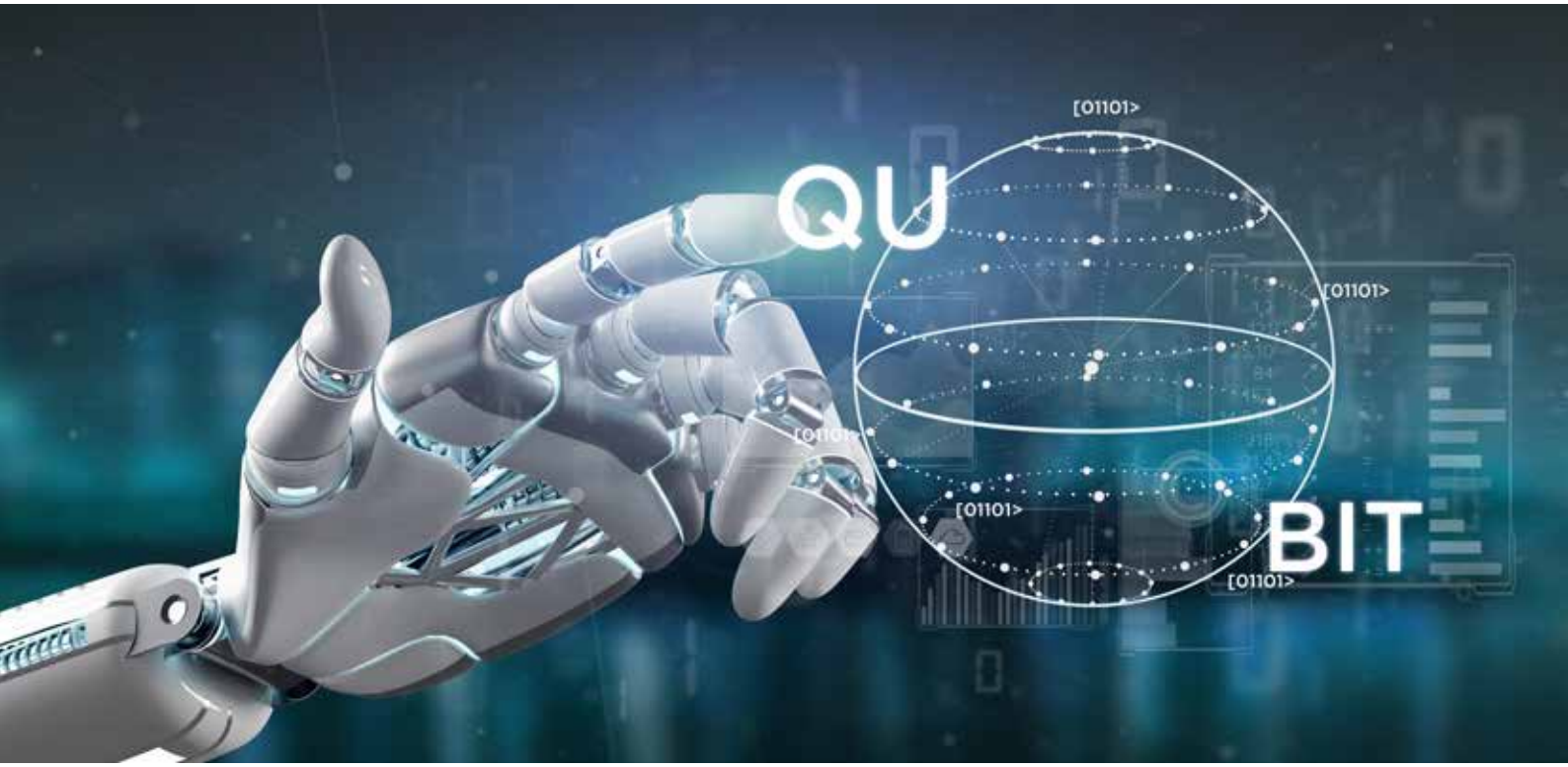
Traditional RAN architectures provide a good foundation and level of performance that largely meet the needs of telecommunications. By integrating AI into the RAN architecture, the efficiency and level of automation of the system can be increased. AI-RAN can be used to optimize the use of radio resources and frequency management, as well as to enhance adaptation to dynamically changing telecommunications and frequency conditions, thus improving the overall efficiency of the system.

The development of AI-RAN is tied to the development of edge computing, cloud services and artificial intelligence. The real-time operations of the AI-RAN system place additional demands on the implementation and performance of AI algorithms due to resource and latency limitations, which can somewhat be mitigated by edge computing. It means performing some of the computation "at the edge", in other words near the physical origin of the information, instead of in the cloud. It can help reduce the strain on networks and speed up processes, since less data is sent to a data center and back. Edge computing also provides various opportunities for cyber security due to the multi-location nature of data.

In radio systems, the use of a wide range of frequency bands increases resilience. The HF radio system, which was previously considered to be narrowband and limited in its transmission capacity, is now being developed towards cognition and broadband with the help of software-defined radio technology. The system uses an embedded waveform architecture, in which all communication components are integrated into the same waveform software. By developing waveforms, the performance of HF radios can be improved and new possibilities for operation can be discovered.

A mesh system is a group of wirelessly connected devices that form a unified wireless network. In a mesh radio network, several radios work together as repeaters, forming a network that can transmit large amounts of data over long distances. Each radio acts as both a transmitter and a receiver, and they use a routing protocol to transmit data over the best route. Mesh networks are flexible and scalable, and they provide redundancy, which means that if one radio is inoperable, data can still be transmitted through another radio. Mesh radio networks are useful in critical communication situations where traditional forms of communication do not work.

At the tactical level, mobile network solutions can be built to support the terminal devices of several hundred different operators and weapon systems in a selected area. Such on-premises network solutions provide their users with advanced edge computing capabilities, mesh network services, flexible frequency band management, and effective cybersecurity. If built right, local networks can be very flexible and quickly configurable.



4.3 The Need for Reliability

A key requirement when it comes to communication is reliability. When looking at the war in Ukraine, disruption of communications has been a recurring theme during the conflict. Methods that would be more resistant to jamming and other forms of disruption could be real gamechangers on the battlefields of Ukraine and any future conflict areas. It does not even necessarily require an active state of war for jamming to be a problem, as can be seen right now in South Karelia where Russia is disrupting mobile networks and GPS signals along the border.

There is also the question of possible AI-integration. AI-driven networks can enhance network efficiency, reduce latency, and enable seamless connectivity across satellite, aerial, and terrestrial networks. AI could enable many of the features that are needed to satisfy the aforementioned requirements, whether it be greater security for dual-use technologies or intelligent methods for avoiding signal interference. Network architectures that comply with the latest standards support the integration of artificial intelligence at the edges of the network close to the users who use them, whether they are devices or people. However, it is still unclear where exactly these solutions would be implemented and who would manage them, so there is plenty of work to be done before training and implementation can commence.

On of the most significant factors influencing the development of AI is quantum computing. That is because unlike normal computers, quantum computers can investigate all the possible solutions at the same time thanks to superposition and quantum entanglement. Quantum computers have a way to dramatically cut down the time it takes to solve the mathematical problems currently used to cypher communication from thousands of years to possibly all the way down to hours or even minutes. Suffice to say, the ability of quantum computers to fairly easily break nearly every type of encryption method currently in use has huge implications for cybersecurity.

According to the National Emergency Supply Agency, organisations should make a roadmap for the upgrade to quantum-proof systems, with all critical systems being updated by 2030. Perhaps the best possible way to prepare for this is to look for "crypto-agile" systems—ones where switching from one form of encryption to another is easy. This way it will be much easier to keep up with the undoubtedly rapid updates to quantum-resistant encryption methods. Quantum computing can be a major gamechanger in positive ways as well, with things like logistics optimisation becoming much easier than now. The impact on AI will likewise be revolutionary.

According to the National Emergency Supply Agency, organisations should make a roadmap for the upgrade to quantum-proof systems, with all critical systems being updated by 2030.

4.4 The Need for Security

Regarding the impact of quantum computing, but for other reasons as well, another requirement for future communications systems will be the ability to divide information into different categories of protection, for example into public, confidential and secret. Those could easily represent civilian, critical infrastructure and military actors and their requirements for communication security. It might not be necessary for civilian communication to be protected against quantum threats as early on as military or critical infrastructure, since these two are more likely to be targeted by hostile actors with early quantum capabilities. The requirements for security are different in other aspects as well, so it is something to keep in mind when designing dual-use systems.

That said, it is important to remember that functional communication systems are important for all three groups. While the military needs them for their command structure both during peace and wartime, as do people working on critical infrastructure, one should not forget about the civilian population either, since for them communication systems enable a variety of things ranging from payment services to staying in contact with loved ones. Disruptions in communications can have a profound impact on cognitive resilience.

Disruptions in communications can have a profound impact on cognitive resilience.

At the organizational (company) level, it is crucial to implement robust network segmentation and ensure the proper distribution and functioning of internal services, including cybersecurity systems. In segmentation, networks with different security levels can be distinguished from each other with the help of telecommunications technologies. Segmentation is done on both a physical and logical level. Physical segmentation can be implemented with optical fibres that are separated from each other. Logical separation can be done with network virtualisation. In cooperation between the authorities, attention must be paid to carefully defined security classifications and classification criteria defined for implementation, so that reliable gateway solutions that meet the security classifications can be built between the networks.

Today, companies' offices, data centers and cloud services are mainly connected by SD-WAN (Software Defined Wide Area Network) technology, which uses software-based network technology, such as data transfer over the Internet through overlapping encrypted tunnels. It enables secure inter-site communication by encrypting all traffic between network edge devices and points. SD-WAN enables centralised network management.

Blockchain technology can also act as a security-enhancing element in communication networks. In blockchain technology, actors who are strangers to each other can jointly produce and maintain databases in a decentralized manner. Technology allows chain members to trust each other, even if they don't know each other. Blockchain increases trust when a database is maintained without a separate actor to manage it. Every actor in the network has access to see the contents of the blockchain, and every transaction is verifiably and securely stored on the blockchain. In addition, the information is also traceable. Another advantage of using blockchains is that the database is distributed in several different places at the same time, which makes it difficult to forge. To achieve consensus, a consensus algorithm is formed for different uses. Blockchain technology can improve the management of society's critical information resources (e.g. Kela, Digital and Population Data Services Agency) and to prevent cyberattacks based on data manipulation.

4.5 The Effective Implementation of Regulation

Finally, it is important to mention regulation and legislation as well. The NIS2 directive enforces actors that are considered to be part of critical infrastructure to fulfil certain criteria relating to cybersecurity, which obviously means that those criteria need to be kept in mind when designing communication systems of the future. The directive calls for secure systems, access control, separation from other systems and regular updates. The actor also needs to be able to continue operating throughout serious disturbances and unusual conditions. One should also keep an eye on the application of the CER Directive, which needs to happen nationally by July 2026, and imposes further responsibilities on actors affected by it.

5 Resilience and Supply Security

Resilience is not limited to just physical infrastructure either. The importance of digital resilience is still often overlooked, but in a modern digitised society it is a crucial part of security. The aim of digital resilience is to have the ability to maintain operations in exceptional conditions with minimal effort. In an ideal situation, this capability is already included into the system during the design phase. If the system already exists, it is important to identify the most critical parts for continuity of service and how the system reacts to disturbances. If the system is critical, and it does not stay operational during a disruption, it needs to be improved. Especially so-called single point failures cannot be left unchecked. They are situations where one failing component takes down the entire system. The support of reliable vendors and a well-funtioning supply chain are critical.

One key aspect worth considering is the physical location of the system's critical components, such as servers and archives. If they are located in the same country as the service, the system can remain operational even during loss of connection to other countries. If, on the other hand, the critical services are, for example, in a foreign cloud service, an interruption in the connection has the potential to completely disable the entire system. This is also true in case just one critical service is unavailable. For this reason, it is also important not to rely on a single service provider for everything, since a disruption of their services would then result in the collapse of the entire system.

The importance of digital resilience is still often overlooked, but in a modern digitised society it is a crucial part of security.

6 The Growing Importance of Cloud Technologies in Resilience Building

There is an increasing global transformation away from local operators and towards cloud services. Because of that, almost anyone can soon build up their own mobile network. There are also certain risks in becoming more reliant on so-called hyperscalers, such as Google, Amazon Web Services and Microsoft. As recently seen with Microsoft blocking access to its products from certain ICC members due to sanctions from President Trump, American products are not completely failsafe in case of political escalation. Cloud services are not immune to it, so service providers need to be carefully evaluated. Legislation in Finland also specifically limits such reliances, so regular operators are definitely going to be playing a role in the future as well. That said, competition with hyperscalers is going to be very hard, so the operators are going to be facing many challenges going forward.

Cloud technologies could improve resilience and allow for more dual-use items to be easily integrated into defense solutions, with tactical edge computing further improving resilience and making sure connections are not overloaded. Thus cloud services could be one part in a solution for developing more flexible systems and structures. The scalability of cloud networks could enable unprecedented situational awareness, support for autonomous systems, realtime target tracking and more powerful simulation tools.

This, however, requires adjustments in both attitudes towards cloud integration and operating models when adopting it. Separating the system used by the military completely from any other systems might be a key requirement. It would still require a very thorough process of auditing for both the initial systems and also any further devices that would be connected to the cloud, including possible dual-use systems. That said, not everything can be solved by cloud services. Even with a completely separate cloud system, security will be a big concern, and secret data might be best kept out of the cloud completely. Therefore the need for more traditional communication solutions remains.

7 The Role of Satellite Technologies

Another key communications technology is the use of satellites, which has seen explosive growth in the past couple of years. Major and minor satellite communication actors are joining forces to offer full-services to their customers. Given the new geopolitic circumstances, where concepts such as redundancy (the existance of auxiliary systems to ensure functionality of systems during disturbances), resilience, multi-orbit, multi-band and communications security are becoming hot topics, plus the technological advances being made in AI, geospatial intelligence and more, it becomes a strategic advantage to be able to offer a wider range of services to one's customers, especially when it comes to dual-use systems.

Many satellite communications and telecommunications companies are focusing on the direct-to-cell connection in a vision to offer seamless connectivity to their customer base. Right now, there are two main tracks that are being developed: running the network on the mobile operator spectrum through "cell-towers in space" and partnerships with Telecom operators – this is what organizations like Starlink, Lynk Global or AST SpaceMobile are building at the moment. One key advantage to this solution is that today's smartphones are already tuned into these terrestrial radiowaves, which means there is no need to wait for a new generation of mobile phones for this technology to be usable.

The other option is the development of separate direct-to-phone constellations running on the mobile satellite spectrum (mainly L-band) with companies such as Iridium, GlobalStar or Ligado and Omnispace being the ones who have reached furthest for now. By using a spectrum that is already authorized to be beamed from space to the ground brings down the time to commercial launch as no extra authorizations or partnerships are technically needed. However, this relies on consumers using recent mobile phones with next-generation chips. When looking into the future, this seems like the likelier option in the long term, since the introduction of new devices will not be a problem. As far as dual-use is considered, this also seems to be the likelier option to better separate military communication from standard mobile phones.

At the forefront of this change is the emergence of non-terrestrial networks (NTNs)—networks that completely circumvent conventional ground infrastructure. These days, satellite organizations supply high-speed access to even the most remote and underserved regions of the world by providing connectivity from space. This has already been proven critical to Ukraine's military command structure, and it does not take a lot of imagination to picture

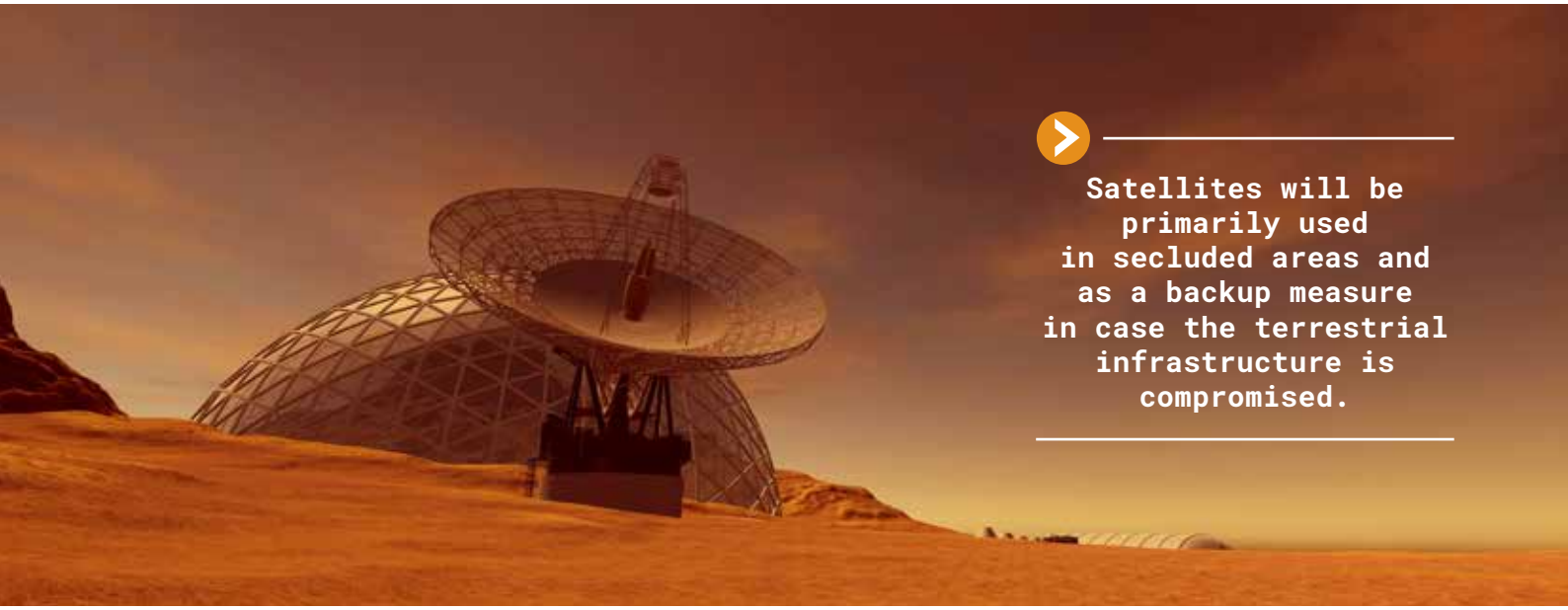
how important NTNs are in areas where critical infrastructure on the ground has been partially or completely destroyed.

Suffice to say, NTNs are going to become an almost mandatory backup system for both civilian and military communication during crises in the future. Satellite-based solutions could also be the best possible backup system for the communication of Finnish authorities, since a traditional radio network is much easier to destroy—especially if the network infrastructure is located close to other critical infrastructure. The Finnish Defence Forces is already investing into space technology during the coming years, so communication systems could be a part of this development.

Satellite systems provide the possibility of delivering high-speed, low-latency internet and data services in locations that are far beyond the reach of terrestrial infrastructure, including open waterways, rural villages, mountains, and disaster areas, including conflict zones. Satellite operators are creating reliable, scalable, and borderless systems that eliminate the need for ground infrastructure, enabling everything from national logistics to emergency response. NTNs provide connectivity from above, as opposed to conventional ground-based networks, which necessitate high-density ground infrastructure and are either costly or impractical to deploy in remote or hostile areas. It puts them in a prime position to help underserved communities across all political and geographic borders. In addition, NTN networks enable satellites and High Altitude Platform Stations (HAPS), such as stations deployed on aerial vehicles to operate in parallel with ground station networks. HAPS solutions could support a fixed broadband for end users and act as a transmission link between mobile networks and the fixed network.

Redundancy and mesh routing features are built into satellite constellations to improve network resilience and reduce single points of failure. Constellations are expanding coverage and propelling the transition to adaptive network designs when paired with AI-based traffic routing and autonomous aircraft operations. It is quite clear to see how current technology trends have the potential to form a positive feedback loop: quantum computing will boost AI capabilities, which in turn will speed up research on all aspects, facilitated by satellite communications, edge computing and cloud services expanding the reach of networks to everywhere on Earth. That said, traditional ground-based infrastructure will still have an important role as well, since it has some advantages over satellite-based solutions. Satellites will be primarily used in secluded areas and as a backup measure in case the terrestrial infrastructure is compromised.

Satellite positioning is a key part of the functioning of society and the warfare of today. GNSS (Global Navigation Satellite System) provides users with positioning, navigation, timing, and PNT (positioning, navigation and timing) services. The jamming and spoofing of GNSS systems in the Russia-Ukraine war show the vulnerability of the system and also how far-reaching its effects can be. GNSS anti-jamming systems work by detecting, mitigating, and in some cases completely neutralizing the effects of jamming signals, ensuring the reliability and accuracy of GNSS-based services. These services are critical, especially in environments where reliable navigation and positioning are crucial, such as military operations, aviation, maritime navigation, autonomous vehicles, and critical infrastructure. By using a variety of methods, such as antenna arrays, advanced signal processing algorithms, and adaptive filtering, GNSS anti-interference systems can help protect against potential threats from interference and maintain the continuous availability of GNSS services.



Satellites will be primarily used in secluded areas and as a backup measure in case the terrestrial infrastructure is compromised.

8 Strengthening National Resilience

When combining the lessons learned from Ukraine and elsewhere with the possibilities of emerging technology, it is possible to deduce solutions for the future challenges of critical communication in modern societies. Perhaps the most important requirement of any future critical infrastructure is resilience, both digital and physical. Especially based on the experiences from the war in Ukraine, that resilience should include resistance to electronic warfare operations.

Systems need to be well protected of course, but a fool-proof system does not exist. When something eventually does go wrong, there need to be backup systems available, and the repair or replacement of the original has to happen quickly. The way to facilitate this is through ensuring components and personnel are close enough to enable a quick response. Dual-use systems are one way to achieve this, since the expertise of personnel and interchangeable components can then be borrowed from civilian systems to military ones and the other way around. An example of the problems caused by the lack of backup systems is the impact of Russia's GPS jamming on air traffic. Some airports no longer have backup systems, and if the GPS does not work, a flight has to be interrupted, as has happened in Finland and Estonia. In Finland, replacement systems

Perhaps the most important requirement of any future critical infrastructure is resilience, both digital and physical.

and radar services have been introduced for approaching aircraft.

Dual-use systems do provide challenges too. Ensuring sufficient security for military use of civilian products is the most prominent one. Testing the systems and practicing with them can also prove to be more challenging than what it would be with strictly military systems, but fortunately Finland has a long history of close co-operation between the military and other parts of the society. Co-operation between the private and public sectors must be seamless, and concepts that have been proven to work, such as national roaming in Ukraine, should be prepared in advance to enable quick reactions. Unnecessary political obstacles for resilience should also be removed when establishing trusted partnerships with companies. Only through the common multi-actor-model of companies and the public sector can digital sovereignty be ensured at all times.

Of the technologies that are already available, satellite and cloud systems are perhaps the most prevalent when imagining solutions to the aforementioned requirements. Cloud systems can provide the ability to dynamically and cost-effectively connect different parts of an organisation to each other, with almost unlimited scalability while also retaining the ability to separate different sections from each other. When combined with AI developments, the possibilities are almost endless ranging from support for autonomous systems to real-time target tracking. Cloud systems are likewise an efficient way to boost physical resilience, since damaged infrastructure in one location will not necessarily mean loss of access to services, especially when combined with satellite-based connections. NTNs can be utilised to ensure network connections are always available everywhere, regardless of the state of terrestrial infrastructure. They can also become a fairly efficient solution for providing communications to desolate areas that are still lacking ground-based networks.

Besides just cloud solutions, AI will likely revolutionise many other fields as well. This is especially true once quantum computing develops to a stage where it can be used to power AI. Judging by public esti-

mates, that is likely to happen within the next five or so years. Therefore, comprehensive systems thinking is needed when building a resilient national communication system. In ”System of systems” thinking, entities consisting of several interconnected systems are perceived. The approach does not only look at individual subsystems, but also at their interactions and synergies in order to understand how the entire system works and to develop new, more efficient solutions.

The flexible and multi-layered use of several communication technologies is essential. Society's critical information infrastructure must be built on the shared network-like use of fixed, mobile and satellite technologies. Fibre-optic connections can provide high transmission speeds (100 Tbps for commercial systems, over 400 Tbps for research laboratories) and should be seamlessly connected to 5G networks. The latest optical fibre technology includes methods based on quantum mechanics that ensure safe data transfer. In addition, AI analytics and automation will be integrated into fibre networks to improve network performance, optimize bandwidth, and enhance fault detection. The role of fibre optic cable assemblies in automation will grow together with wireless systems. It is required in factories and warehouses where robotics and autonomous production methods are introduced. Wired and wireless systems increase redundancy and system resilience.

Future systems need to be highly customisable as well, because the operational environment is in a constant state of change. This is perhaps observed best in Ukraine, where the development cycle of drones is getting quicker and quicker. Prominent trends in technology, such as AI, 5G/6G, satellites, cloud services or quantum computing, are going to provide unique opportunities and challenges for communications systems. It is therefore imperative to pay attention to the development of these key capabilities in the near future. Being able to adapt systems already in use for new innovations and use cases is a massive benefit both financially and in terms of time when compared to the prospect of acquiring completely new hardware and software every time a new capability is developed. It will also make dual-use systems more appealing, if they can be tweaked to better suit military use cases when used by the military, and civilian ones when in civilian use.

Data is at the heart of operations of national critical infrastructure. In the data economy, different actors (citizens, companies and public organisations) work in a common environment to ensure the transfer and usability of data and utilise data to create new innovations and services. Data transfers between actors are a key part of communication and the operation of digital systems. Critical infrastructure operators must build a networked, cyber-secure entity that uses alternative forms of data transfer and advanced technologies to achieve the necessary resilience at different levels of operations. At the same time, the effective implementation of data-related regulation must be ensured.

Being able to adapt systems already in use for new innovations and use cases is a massive benefit both financially and in terms of time when compared to the prospect of acquiring completely new hardware and software every time a new capability is developed.

SOURCES:

https://www.comsoc.org/publications/ctn/predicting-future-communications-technologies

https://www.hs.fi/alueet/art-2000011306235.html

https://www.avenga.com/magazine/satellite-technology-bringing-satellite-in-the-palm-of-the-hand/

https://satcube.com/news/current-satcom-trends-shaping-the-future-of-connectivity?gad_source=1&gad_campaignid=21079435382&gclid=EAIaIQobChMIpNOMseiijgMVvluRBR1C2iy1EAAYASAAEgICY_D_BwE

https://www.techtarget.com/searchdatacenter/definition/edge-computing

https://www.telekom.com/en/company/management-unplugged/details/satellite-communication-a-powerful-addition-to-europe-s-digital-future-1093760

https://spacenews.com/shaking-up-satcom-the-time-is-now-for-radical-innovation-in-satellite-communications/

https://www.critical-entities-resilience-directive.com/

https://www.telia.fi/yrityksille/artikkelit/artikkeli/tutustu-digitaaliseen-huoltovarmuuteen

https://gofore.com/kuka-suojelee-meita-kriisissa-jossa-kysytaan-digitaalista-huoltovarmuutta/

https://www.dna.fi/yrityksille/blogi/-/blogs/5g-ssa-voit-viipaloida-yritysverkkosi-mita-se-kaytannossa-tarkoittaa

https://thebulletin.org/2025/03/russian-networks-flood-the-internet-with-propaganda-aiming-to-corrupt-ai-chatbots/

https://viestiupseeriyhdistys.fi/wp-content/uploads/2021/08/VM-2-2021.pdf

https://viestiupseeriyhdistys.fi/lehti/viestimies-4-2023/

https://issuu.com/viestimies/docs/vm_2024-1

https://issuu.com/viestimies/docs/viestimies_1_2025/30

https://issuu.com/viestimies/docs/viestimies_2_2025

https://ai-ran.org/

https://www.erillisverkot.fi/virve2-0/?gad_source=1&gad_campaignid=16178890739&gclid=EAIaIQobChMI8ontv6PQjwMVNQiiAx3n2Bf-EAAYASAAEgJvh_D_BwE

Cyberwatch analysis of the war in Ukraine

Cyberwatch Weekly Reviews

Presentations of the Cyber Breakfast 2025

WHERE TO FIND US?

On our website

https://cyberwatchfinland.fi/en/

On LinkedIn

www.linkedin.com/
company/cyberwatchfinland

On Instagram
(posts both in Finnish and in English)

https://www.instagram.com/
cyberwatchfinland/

By following us you will receive information about our new publications, cybersecurity events, and tips for developing cybersecurity.

Our aim is to add cyber capabilities in the World

Contact

Cyberwatch Oy | Nuijamiestentie 5 C | 00400 Helsinki, Finland
aapo@cyberwatchfinland.fi | info@cyberwatchfinland.fi | +358 40 500 8177