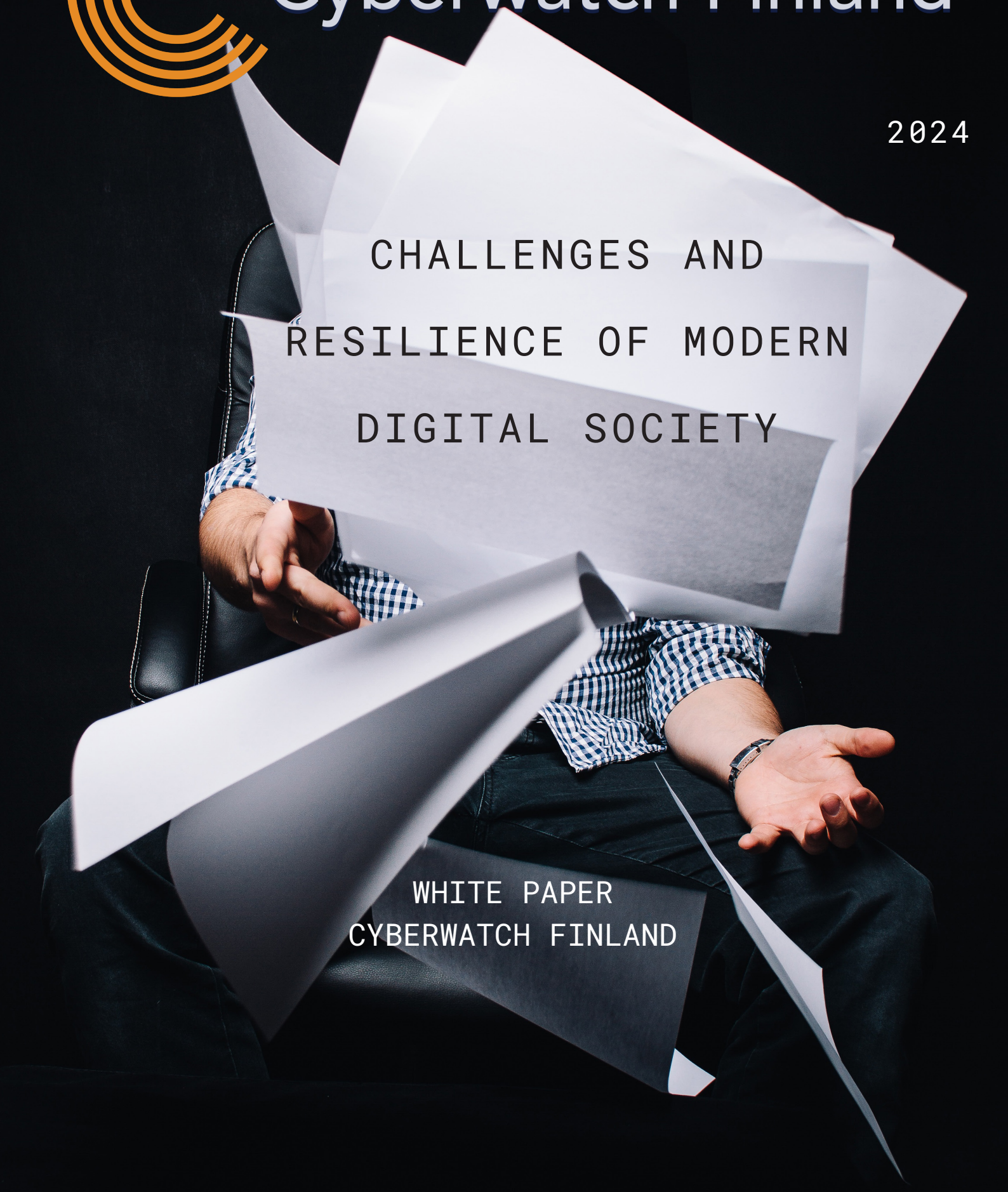
Cyberwatch Finland

2024

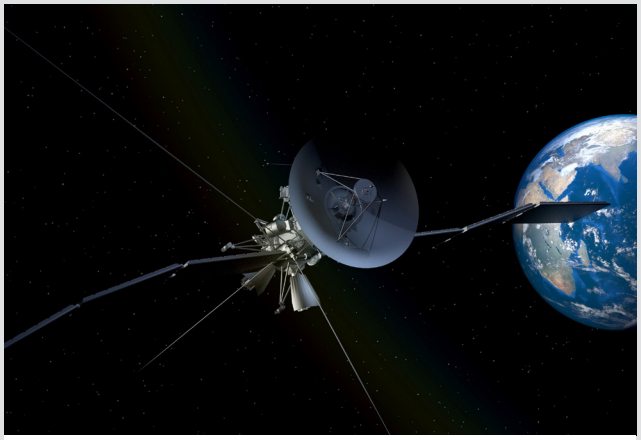
CHALLENGES AND RESILIENCE OF MODERN DIGITAL SOCIETY



WHITE PAPER
CYBERWATCH FINLAND

Cybersecurity is Built by Small Actions and Management of Large Concepts

CONTENT



5 NON-KINETIC INFLUENCING AND OPERATIONS

5.1 Hybrid influencing and operations
5.2 Cyber influencing and operations
5.3 Information influencing and operations
5.4 Electronic influencing and operations
5.5 Cognitive influence and warfare

6 CYBER-SECURE SOCIETY

6.1 National security
6.2 Resilience of society
6.3 The current state of comprehensive security management
6.4 Developing comprehensive security model and security of supply
6.5 Security of cyber supply
6.6 Developing security of supply

7 COOPERATION BETWEEN PUBLIC AUTHORITIES AND BUSINESS

8 CONCLUSIONS

9 MAIN SOURCES

1 INTRODUCTION

According to the EU, the electricity grid, transport network as well as information and communication systems are critical infrastructures necessary to sustain vital societal functions. Currently, the geopolitical environment surrounding this critical infrastructure is highly unstable, which is explained in particular by Russia's war of aggression against Ukraine. Russia sees itself as waging a kinetic (traditional) war in Ukraine and a hybrid war against Western civilization. This manifests itself in various cyber sabotage attacks, hybrid and information influencing, and the pursuit of dominance in the cognitive environment in Finland and throughout Europe.

The European Commission has launched the European Programme for Critical Infrastructure Protection (EPCIP), which, as the name implies, aims to improve the protection of critical infrastructure in Europe. Emerging threats and unconventional attacks on critical infrastructure have exposed shortcomings in traditional risk assessment and risk management measures. Not all threats can be pre-empted using traditional methods, which is why more effective risk analysis and system resilience are required. The Finnish comprehensive security model which divides responsibility for critical infrastructure between different ministries acts as good example for more thorough protection. However, it does pose some challenges regarding its implementation, especially in crisis situations requiring rapid reactions.

The war in Ukraine has changed our security environment forever. Critical infrastructure has been the main target of kinetic and non-kinetic attacks. This highlights the necessity of coordinating national leadership, creating new cybersecurity enhancing programs and effective crisis management. Cyber warfare in Ukraine has had less impact than expected. Russia seems to prefer to use conventional military force in Ukraine, which has greater destruction and deterrence. The lack of cyber operations could be due to the inability to reuse them once they have been revealed. It seems that the smartest cyber operations will be saved as hybrid influencing tools against Western countries. This allows Russia to operate below the threshold of conventional war and creates an information-psychological deterrent effects. Cognitive warfare has become a strong part of asymmetric warfare. The aim is to undermine citizens' mental crisis resilience through long-term hybrid operations.

Cyberwatch's analysis team has been monitoring the events and impact of the war in Ukraine since it began as part of our cyber situational picture reviews. In this report, we review the new challenges and development needs raised by the war and in the change in the international operating environment and make concrete proposals for practical measures to improve the resilience of the modern digital society.

2 WAR IN UKRAINE HAS BROUGH CRITICAL INFRASTRUCTURE TO FOREFRONT

2.1 CYBERATTACKS ON UKRAINE'S CRITICAL INFRASTRUCTURE

Russia has continued its military operations in Ukraine since 2014 following the illegal annexation of Crimea. On 24.2.2022, Russia launched a military invasion of Ukraine in violation of the UN Charter and international law. Yuriy Schygol, head of Ukraine's National Cyber Security Agency, announced in January 2023 that there were 2,194 cyberattacks against Ukraine in 2022, including 1,655 after a major Russian military offensive (February 24). According to the Geneva-based independent CyberPeace Institute, as of December 2023, there have been 666 attacks on civilian targets in Ukraine, 331 attacks on Russian targets and 2258 attacks on other countries. According to the CyberPeace Institute, these cyberattacks are linked to Russia's war of aggression. Russia's targets during the war have included:

- Ukrainian government
- Energy
- Telecommunications sector
  - Triolan Internet Service Provider
  - Vinasterisk Internet Service Provider
  - Ukrtelecom
- Media
- Transportation and logistics
- Voluntary organisations and NGOs

The vast majority of attacks have been distributed denial-of-service (DDoS) attacks, of which there were 493 between January 2022 and December 2023 (CyberPeace Institute). During the same period, there were 26 reconnaissance attacks, 23 phishing attacks, 22 website manipulation attacks and 18 file destruction attacks (Wiper malware). In addition to cyberattacks, Russia is carrying out large-scale information influencing. It generates an average of 166 million scam messages per week, while more than 50,000 fake social media accounts consistently generate disinformation.

Russia's security agencies GRU, SVR and FSB have been active in Ukraine before and during the war. They have all carried out phishing, but the GRU has been primarily responsible for data-destroying operations. Threat actors linked to the GRU have also been linked to many cyber and information operations. Russia intensified its phishing efforts about a year before the start of the war of aggression, likely with the aim of gathering information about Ukraine's state government, armed forces, critical infrastructure and critical information infrastructure. In addition, Russia has been interested in the political decision-making of countries supporting Ukraine and their relations with Ukraine.

Russia's information and cyber operations have been closely intertwined throughout the war. Personal data of Ukrainians has been leaked as part of an information operation, denial-of-service attacks have been openly motivated by political motives, and email addresses hacked from information systems have been used as target lists for information operations.

2.2 OBSERVATIONS FROM UKRAINE

Colonel Maksym Pavlyuk, **head of the cyber security department of the General Staff of the Ukrainian Armed Forces,** has analysed Russia's hybrid operations. According to him, Russia is constantly testing the resilience and cyber security of the national electricity infrastructure. The well-known Black Energy (2015), Viasat (2022) and Kyivstar (2023) have been among the most effective cyberattacks. Russia favors kinetic strikes against the power grid and critical infrastructure, which have resulted in daily power outages in Ukraine. In addition to traditional attacks, it also seeks to carry out attacks on the power grid in cyberspace.

In ICT systems, the impact of cyberattacks is more complex and dynamic. In its hybrid operations, Russia has targeted not only civilian infrastructure, but also Ukraine's military systems, data centers, and even military personnel's personal devices. After Russia's large-scale invasion, the strength of Ukraine's armed forces quadrupled due to mobilization. Right from the start, the BYOD policy was introduced (Bring your own device). This use of own devices has required effective cyber hygiene, which has been implemented through a mandatory online course. The training includes descriptions of enemy phishing methods, advice on servicing personal devices, and instructions on legitimate software and antivirus updates. According to the feedback received, the system works quite well.

In Ukraine, the focus of Russia's cyberattacks has been on the command and control system of the armed forces, situational awareness, logistics, healthcare, artillery, electronic warfare and other information systems of weapons systems. The Russians are targeting both servers located on computer networks and end users. Cyber defence in Ukraine implemented as efficiently as possible with the support of partner countries, which is why for the time being, there have been no catastrophic effects on the systems. Nevertheless, the performance of cyber defence needs to be strengthened.

In conclusion, Pavljuk notes that its opponents (not only Russia, but other rogue states) are not dilettantes in operations below the threshold of war, even if missiles and bombs are better in practice. This leads to two main findings and recommendations:

1. In the current digital era, conflicts are not excluded, and the cyber environment plays a significant role alongside other traditional areas of activity of the armed forces. Therefore, effective cybersecurity across critical infrastructure is key to its resilience and stable operation.

2. The war in Ukraine shows that even highly protected targets in terms of cyber defense can be reached with kinetic force. A NATO umbrella is a good start, but for Russia's neighbors, Pavljuk recommends considering physically protecting important targets. Air defence and electrical warfare (EW) systems are needed to defend electricity networks. Where possible, data centers should be mobile or located underground.

2.3 COMMUNICATION SYSTEMS AS A TARGET

Despite the war and Russia's disruptive activity, Ukraine has managed to keep the telecommunications network (4G) functioning relatively well. This has required a joint effort by telecom operators and network equipment suppliers. The importance of seamless cooperation has been seen as a basic prerequisite for crisis resilience. The first lesson is that the arrangements for disruptions and emergencies must be planned and rehearsed in advance. Furthermore, they must be part of commercial agreements drawn up under normal conditions. When defining contingency obligations, account shall be taken of the need to rapidly increase preparedness and the physical and asymmetric operations of hybrid warfare. Ukrainians emphasize the importance of supplier reliability and the difficulty of assessing it when concluding contracts. It should be possible to use clear criteria such as reliability, maturity level, auditing and resilience in the event of disruptions. Promises alone are not enough, but the capability and reliability of operators and network equipment suppliers should be verified with sufficient certainty.

The war in Ukraine has highlighted the importance of telecommunications in maintaining the nation's and its citizens' mental resilience and ensuring the functioning of critical infrastructure. It must be possible to quickly increase capacity and keep networks operational despite disruptions. This requires, for example, releasing licences and enabling and optimising the sharing of all networks. Operators have played a key role in this acting as coordinators. The storage of spare parts by network equipment suppliers in the area where they are needed and the ability to deliver them are basic prerequisites for repairing damage quickly.

Many small details have been learned during the war, such as the arrangements for rapid testing of networks, the removal of signal lights from masts, and ensuring the supply of electricity in various ways, including from outside the country's borders. Networks have also been prioritised, for example, to secure payment transactions and the operation of the electricity network. It has also been observed that logistics and storage arrangements must follow the same logic as for munitions, which means storing them close to targets and ensuring the reliability of logistics chains. Duplicated backbone networks have also proved necessary.

Since the cyber-attacks at the beginning of the war, communication systems have been one of the main targets of Russian activity. In Ukraine, it has been considered important for the resilience of society that there has been dispersion across several operators and network equipment suppliers the country. A well-functioning market in normal times lays the foundation for resilience in crisis situations. A comprehensive risk analysis makes it easier to understand the interdependencies between critical functions of society, such as the electricity grid and telecommunications systems; Neither works without the other.

2.4 CYBER SECURITY MANAGEMENT BECOMES HIGHLIGHTED

At the strategic level, governments should base cyber security management on knowledge-based decision-making. The significance of the situational picture formed on the basis of collected data is absolutely critical. The necessary rapid strategic decisions are based on available real-time information, multiple alternative solutions, technology opportunities and expert support. Strategic management can be used to combine, involve and coordinate cooperation between different national actors in cybersecurity-related activities and preparedness. In addition, strategic management creates the conditions for both political decision-making and operational activities. The strategic management system must interact closely with political decision-makers. Strategic management of cyber security means securing the digital operating environment, identifying and setting derived goals, coordinating operations and preparedness, and managing the management of large-scale incidents. Strategic management of cyber security is also securing the capabilities and vital functions of the state, because this also enables the private sector and the third sector to build their operations on functional and secure information networks.

At the operational-tactical level, cyber security management includes a set of processes focusing on managing and sharing information, organisational management and decision-making in addition to technological measures that are needed for cyberthreat and risk assessments and in achieving cyber resilience.

Different models have been developed for cyber security (CS) management, which emphasize different issues according to the purpose for which the model was developed. The model below consists of seven components of management:

1. Management of CS resources: awareness of the security structures and solutions of systems, their vulnerabilities and weak points.
2. Management of the CS organisation: management of operations in the prevention, preparedness and planning of incident management.
3. CS technology management: defining the cyber security solutions for the software, telecommunications and networks used. Defining the cyber security solutions for the software, telecommunications and networks used.
4. CS culture management: leading the organisation's personnel to operate in a cyber secure manner, managing cyber security competence and increasing awareness of the individual responsibility in cyber security.
5. CS legal management: understanding national and international legislation related to cyber security and especially its impact on the organisation's operations.
6. Management of CS incidents: managing cyber incidents in accordance with the pre-determined plans and instructions of incident management and continuity assurance.
7. CS strategy management: leading the organization's cyber security strategy process from its preparation to implementation and updates.

Serious cyber incidents can occur in both normal and emergency conditions. Disturbances in normal conditions are managed with the normal jurisdiction of the authorities and the resources of organisations. Systems and contingency measures built under normal conditions lay the foundation for operations in emergency conditions. Correspondingly, it must be possible to utilise the arrangements made for emergency conditions in the management of disturbances in normal conditions. It has been predicted that traditional management models of the industrial age will be replaced by those of the digital world surprisingly quickly.

3 CRITICAL STRUCTURES OF SOCIETY

3.1 CRITICAL INFRASTRUCTURE

Critical infrastructure is not unambiguously defined. According to a 2023 report by German Foreign Policy Society (Deutsche Gesellschaft für Auswärtige Politik, DGAP) the 193 UN member states and Taiwan do not have a common definition for critical infrastructure. There are at least a hundred different national definitions of the subject. Many countries lack a list of critical infrastructure or critical information infrastructure sectors. Only one hundred out of 194 countries have published the sectors they consider to be critical sectors. The sectors most frequently mentioned in the reports are energy (96%), ICT (95%), transport (93%), economy and finance (89%), public services (84%) and health sector (83%).

3.1.1 COMPREHENSIVE APPROACH AND DEFINITION

The main target of cyberattacks is critical infrastructure. Despite national variances a definition has arisen in the context of new legislation on internal security. Critical Infrastructure (CI) comprises of structures and functions that are necessary for the continuous functioning of society. It includes both physical entities and electronic functions and services. Securing these means finding and securing individual critical points within the larger infrastructure. There are three dimensions to securing critical infrastructure: political, economic and technical.

The political dimension includes national legislation and national security needs, as well as international cooperation around them. International cooperation aims to aligning solutions in countries with similar needs. Uniform legislation and security policy enable technical cooperation, especially in situations where the infrastructure spans several countries.

The economic dimension includes all companies and other economic operators which build, own and manage infrastructure systems and installations and which act in accordance with economic interests. The economic dimension also includes a fair distribution of security costs between the various actors. In many countries, private companies are responsible for the functioning of critical infrastructure.

The technical dimension encompasses technology, as well as all practical solutions and measures taken by governments and companies to safeguard the functioning of their critical infrastructure in the event of disruption. These networks are not separate entities, but form a national critical infrastructure network with a high degree of interdependencies. The paralysis or collapse of one system affects other parts of the network.

Critical infrastructure thus consists of tools and equipment, services and information systems that are so vital to nations that their inoperability or destruction would have a debilitating effect on security, the economy, health care and the efficient functioning of state administration.

3.1.2 EU STEPS UP CRITICAL INFRASTRUCTURE PROTECTION

Through its regulation, the EU aims to strengthen the resilience of Member States. Directive on the Resilience of Critical Entities (CER) entered into force 16.1.2023. Member States must adopt national legislation to implement the Directive by 17.10.2024. The aim of the directive is to strengthen the resilience of critical entities against a wide range of threats.

In 2022, the EU adopted Directive on Security of Network and Information Systems, (NIS 2), which replaced the 2016 NIS Directive. The new regulation aims to ensure a common, high level of cyber security across the Union, in response to the changing threat landscape and taking into account the accelerated digitalisation following the pandemic. In Finland, the national implementation will take the form of a new cyber security act by the end of 2024. It aims to strengthen both the EU's common and Member States' national levels of cyber security in critical sectors of society. In the NIS2 Directive, the operators are divided into essential, important and other actors. Key sectors include digital infrastructure, ICT service management and the energy sector.

Since describing the level of criticality of industries (and actors) is particularly relevant in terms of differing requirements and challenges, this report refers to critical functions of the society and defines the core of critical infrastructure.

3.2 CORE OF CRITICAL INFRASTRUCTURE

The entities covered by the NIS2 Directive need to take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the network and information systems. These steps must be taken to prevent or minimise the impact of incidents on the recipients of their services and other services. A three-level model of critical infrastructure could be built, for example according to the significance of interdependencies. The core of critical infrastructure consists of the most critical functions for societies, which are the electricity grid and digital infrastructure, as well as the satellite systems needed to generate spatial data and accurate time.

3.2.1 POWER GRID

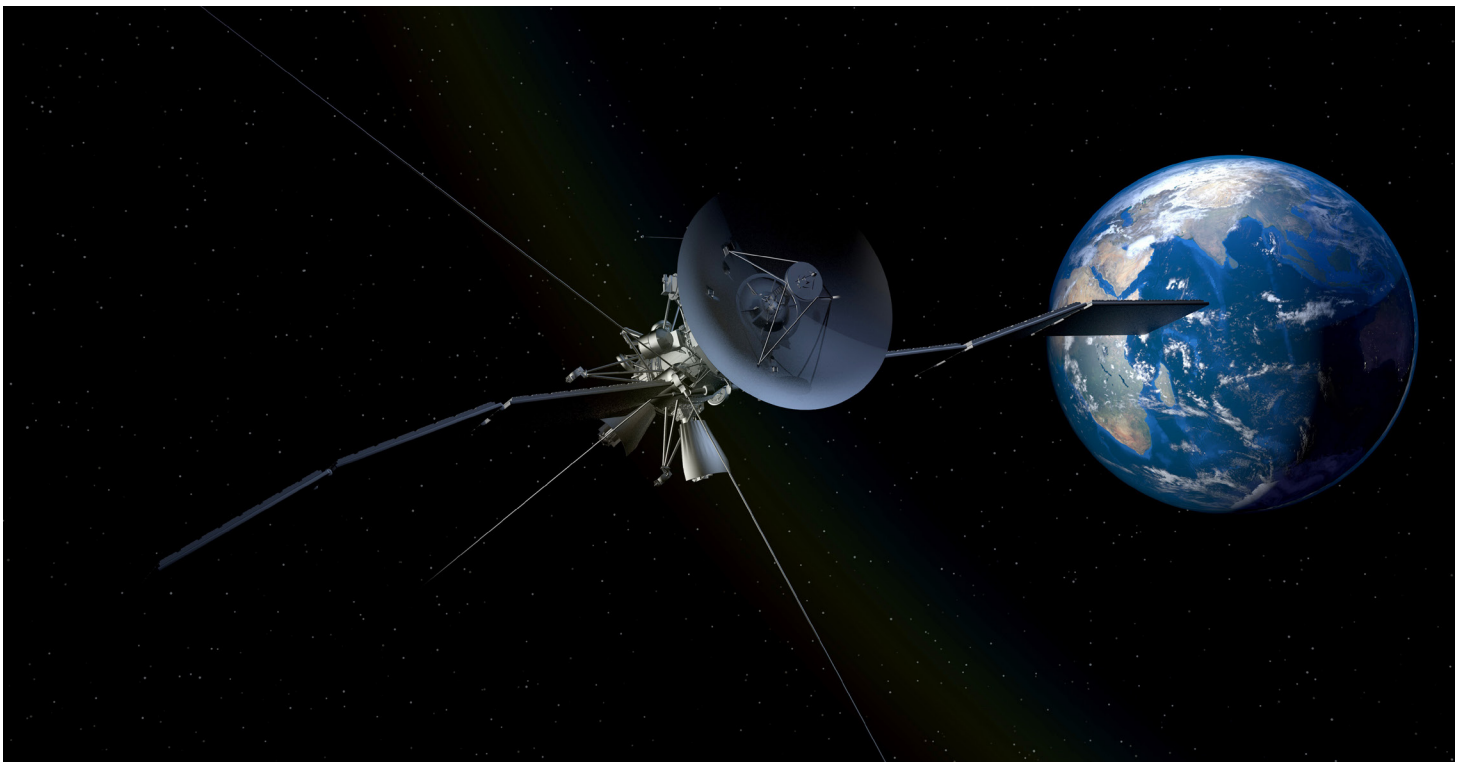
The Finnish electricity system consists of power plants, the main grid, high-voltage distribution networks and electricity consumers. The electricity network includes numerous substations and distribution substations. Substations are nodes in the network where power lines of different voltages converge. The stations can be used to convert, distribute and centralise the transmission and distribution of electricity. There is an industrial automation network for controlling the power grid, which manages the components of the power system. Energy suppliers must secure both operational and information systems (OT and IT) and ensure that they work with trusted partners in their supply chains. Notwithstanding, operating systems used by Europe's electricity grids are up to 40 years old, making their cyber-securing a difficult task.

The elements of critical infrastructure include an industrial control system (ICS), supervisory control and data acquisition (SCADA), distributed control system (DCS) and operational technology (OT). These systems are key components of the infrastructure. Industrial Control System (ICS) is an umbrella term that includes both SCADA and DCS. ICSs are interfaces where virtual commands create physical reality in industrial environments. SCADA systems are the software-based elements of these ICSs. ICS and SCADA systems provide real-time, two-way communication between sensors, workstations and other networked devices throughout the system. They enable continuous and decentralised monitoring and control.

3.2.2 DIGITAL INFRASTRUCTURE

Network and information systems have developed into a central part of everyday life as the digitalisation and networking of societies have progressed rapidly, including cross-border communication. Cyber-attacks are increasing in number, scale, sophistication, frequency and impact and pose a significant threat to the functioning of network and information systems. Fast, functional and secure communications networks are the foundation of modern society and a prerequisite for digitalisation. The Internet is a global system of interconnected networks that uses Internet Protocol (TCP/IP) to connect IT devices to each other. It is a network of networks consisting of millions of private, public, academic, business and government information networks of various sizes, which are interconnected by various technical equipment (e.g. wireless and optical network technologies). The Internet offers a wide range of information resources and services, such as websites, e-mail, telephone services, online banking and peer-to-peer file sharing networks.

Well-functioning telecommunications connections are the "bloodstream" and backbone of resilience in the digital society. The electricity network and telecommunications connections enable the functionality of other critical services and infrastructure. Moreover, they are interdependent; One does not work without the other. These form the core of critical infrastructure vital to the functioning of the digital society.



3.2.3 SATELLITE SYSTEMS

Space has become vital to humanity and, in particular, critical to the global economy and the telecommunications network that supports it. Most of the satellites are telecommunications satellites. With the help of earth remote sensing satellites, the Earth and objects on its surface are imaged, measured and observed in various ways for different purposes. Weather satellites are used to make meteorological forecasts. Reconnaissance satellites are used to monitor activities on the territory of other states (e.g. troop deployments and movements or the construction of missile bases and industrial facilities). Research satellites are used to study space and objects in it.

Satellite navigation refers to navigating using a local or globally comprehensive satellite system - GNSS (Global Navigation Satellite System). National satellite systems are also vital: the United States has GPS, Russia has Glonass, Europe has Galileo and China has BeiDou.

Modern societies are increasingly dependent on satellite-based positioning, navigation and time services (PNT). Of the PNT signals, accurate time service in particular supports critical infrastructure. Without an accurate time, financial institutions, would not be able to create timestamps for transactions, which would affect the use of ATMs and credit cards. Neither electricity companies would be able to transmit electricity efficiently. The PNT signal also supports sea, land and air traffic, in route planning and congestion management. In addition, rescue and police operations need reliable location information.

For the military, this information makes it possible to accurately target missiles and ammunition, as well as navigate aircraft, ground units and ships. The critical nature of GNSS has become clear during the war in Ukraine with continuous GNSS jamming. In the future, it must be possible to detect attempts for manipulation of time and location data, the consequences of which would be truly fatal for society's critical services.

Protected against malfunctions, interference, and distraction the public regulated satellite service, PRS) aims to ensure the availability and reliability of location and time information for authorities and critical infrastructure operators. Positioning services and time information have become a crucial part of society that other critical functions rely on. Satellite systems are also necessary for modern weapon systems, which further highlights their necessity in national defence.

The importance of satellites as part of the telecommunications backbone networks will increase significantly in the near future. Wireless communications 5G NTN (5G Non-terrestrial Networks) - concept is close to implementation and will use low-orbit LEO satellites as base stations for data transmission (Low Earth Orbit) and other unmanned aerial vehicles. The goal of 5G NTN development is to combine currently separately operating terrestrial and satellite-based telecommunications networks.

In the next few years, consumers' mobile phones will smoothly use both terrestrial base stations and satellites. IoT sensors can be installed in production facilities in the middle of the wilderness or ocean when access to 5G NTN networks can be relied upon. At the same time, satellite systems will become an integral part of the functionality of energy and electricity production and part of the digital infrastructure, and simultaneously their importance at the core of critical infrastructure is increasing.

4 FACTORS OF CHANGE IN THE OPERATING ENVIRONMENT

4.1 DIGITALISATION

The digitalisation of societies continues at a rapid pace. Digital services are based on an ecosystem of people, innovative operators and intelligent machines. The aim is to make the services more functional, flexible and cost-effective. Digitalisation must enable better and more reliable service chains and systems for the needs of citizens, the public sector and companies. Digitalisation also creates new kinds of threats. The digital world attracts criminals looking for new opportunities to steal, exploit and sell information. The transfer of information and the vast availability of information online has also brought intelligence organisations there. For terrorists, the cyber world is an operating environment for communication and influencing, and it is also an attractive target for attacks. The digitalisation of the armed forces has created a military cyber world in which not only networked soldiers, but also intelligent and increasingly autonomous weapon systems are working. For these reasons, as digitalisation continues and ramps up, information and cyber security should be brought increasingly into focus.

4.2 THE MILITARISATION OF THE DIGITAL SOCIETY

Electronic warfare, information warfare and cyber warfare operations form a framework for non-kinetic network-based operations in the cyber age. In warfare, these operations form a networked entity in which different forms of operation are used to achieve the objectives set for warfare, often as part of hybrid influencing. The cyber environment has become an integral part of both modern warfare and the national cyber environment. Digitalisation is increasing the possibilities for state and non-state actors to conduct increasingly sophisticated cyber operations with military, political and economic objectives. At its most extreme, society's vulnerabilities are exploited in cyber operations to sabotage, cripple and destroy critical infrastructure. This has become clear in the war in Ukraine.

4.3 SHIFT OF PARADIGM IN WARFARE

With the development of digitalisation, the traditional peace-war set-up has changed from a traditional Clausewitzian model with precise boundaries to a vague, unpredictable and unstable operating environment for foreign and security policy. Warfare is organised hostile influence between two independent actors, in which physical violence is the central and traditional mean to submit the opponent to your will. According to Clausewitz, war continues state policy by other means. Alongside this traditional division, a crisis phase has emerged in the foreign and security policy, known as the grey phase between peace and war. It can be described as a preparatory stage, which describes the activities preceding the start of the war. The grey phase encompasses a wide range of activities currently defined as hybrid influencing or hybrid warfare.

Figure 1. The traditional peace-war set-up.

Russia has stated in his own rhetoric that it is at war with the West. This way of thinking changes the perspective described above. In it, war is the default state of being with varying degrees of intensity. Figure 3 below depicts the new Cold War peace-war setting.

Figure 2. Peace-war set-up of the new cold war.

A new paradigm of warfare is replacing the traditional model of declaring war and agreeing on peace, creating a space where war is not declared, and peace is not concluded. This set-up, together with the digitalisation of society, enables a space where various kinds of non-kinetic influencing can be carried out at different stages before an active war, remaining below the threshold of war and out of reach of the attribution of actors. During open war, non-kinetic operations are carried out alongside land, sea, air and space operations and as their support and enabler.

In this setting, the concept of warfare and related operations require open war between actors, so activities outside of it must by definition be distinguished from open war activities. Non-kinetic activities can be defined as influencing during peace and conflict, and operations during active war. At a high level of abstraction, influencing and operations are functionally similar; differences can be seen in the targeting and in the intensity of operations.

Non-kinetic operations, in particular, allow major powers to justify their presence, influence and create disorder. The justifications for these actions can be peacekeeping, maintaining balance, protecting one's own interests and citizens, or supporting allies. The digital environment has created a new space to influence the territory of another state by exploiting various military and non-military means of pressure to achieve political and military objectives. The digital operating environment is well suited to hybrid warfare and its various forms, especially when operations can be carried out unexpectedly and without revealing the perpetrator.

5 NON-KINETIC INFLUENCING AND OPERATIONS

In particular, this report examines non-kinetic activities at a high level of abstraction, therefore peace time influencing and military operations are treated as a single entity. In the digital operating environment, hybrid, information and cyber influencing and operations, as well as electronic and cognitive influencing, form a multi-level, complex and merged entity in which phenomena are not strictly defined by definition or function. Hybrid warfare, electronic warfare, information warfare, cyber warfare and cognitive warfare operations form a web of non-kinetic network-based operations in the cyber age.

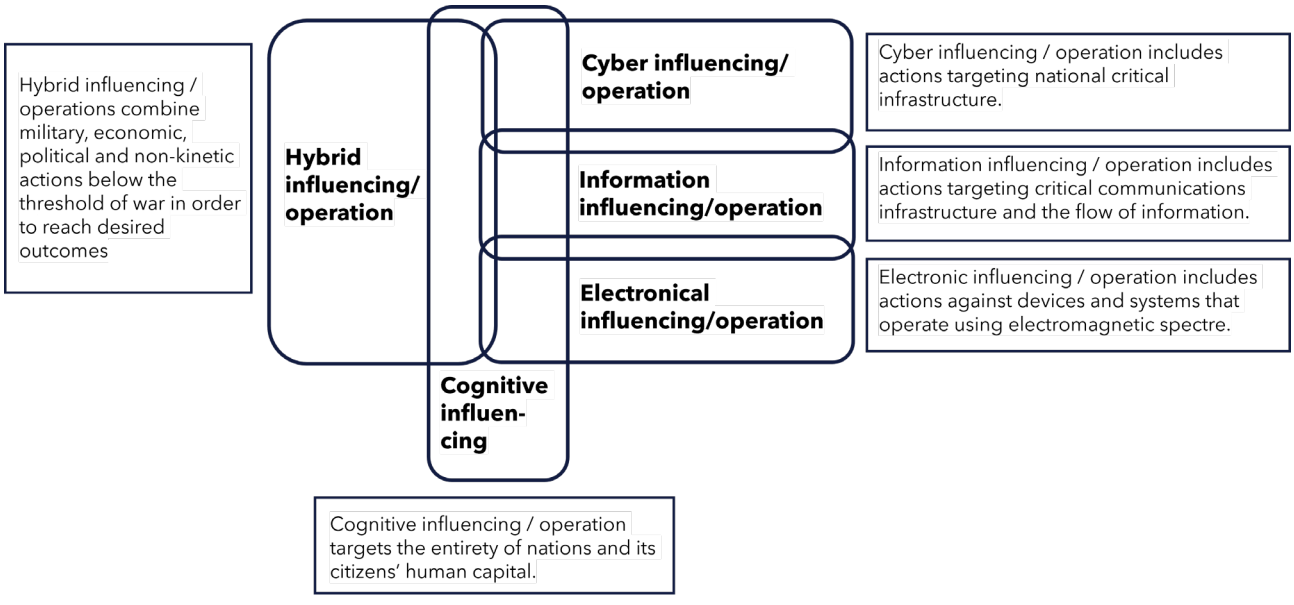


Figure 3. Non-kinetic operating environment, (source Dr Martti Lehto)

5.1 HYBRID INFLUENCING AND OPERATIONS

Hybrid influencing involves the systematic integration of military, political, economic, civilian and media influencing and often manifests itself below the threshold of conventional war. Hybrid operations are used in an unconventional and innovative way to avoid attribution, i.e. identification of the operator and allocation of responsibility. The range of hybrid influencing tools includes, economic and military means, as well as information and cyber influencing. Hybrid operations are primarily carried out by state actors. It is tempting to test different methods of hybrid operations because they carry a relatively low risk of detection and escalation compared to traditional military operations or other methods of influence.

In hybrid warfare, a hostile state may use state (military/security services) or non-state actors (various criminal or activist groups) in the non-visible part of warfare to deny any involvement in attacks often on civilian targets, but with the aim of achieving its strategic objectives. Hybrid warfare is located between war and peace. Detection and prevention of hybrid operations should be done at an early stage, before an attacker deploys the entire arsenal of hybrid methods. The detection capability of hybrid operations (early warning) must be improved so that the adversary's activities and attempts to influence can be stopped before they have even properly begun.

5.2 CYBER INFLUENCING AND OPERATIONS

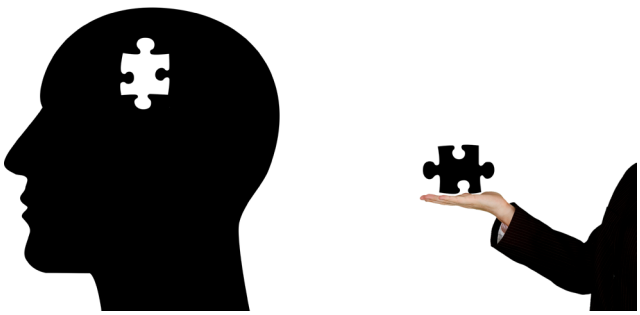
Under normal circumstances, **cyber influencing** means carrying out various cyber sabotage operations in which the attacker tries to stay below the threshold of war. The objectives may include causing instability in the target country, testing offensive cyberattack capabilities, and preparing for hybrid operations or war. The era of cyber sabotage began with the Stuxnet web worm in 2010. It was the first virus to target the Operational Control System (SCADA) targeting Iran's nuclear enrichment facility.

In cyber warfare, not only are armed forces targeted, but critical infrastructure of society and its vital functions are also in focus. Cyber warfare is a factor in enabling the use of physical military force, as has been seen in connection with the war in Ukraine. Society's vital functions must be safeguarded at all times. Finland, as an information society, depends on the functioning of information networks and systems, and therefore cyber-attacks can be used as a means of exerting political and economic pressure. In the event of a serious crisis, it can be used as means of influencing alongside traditional military force. In this way, national cyber defence becomes an integral part of overall national defence.

5.3 INFORMATION INFLUENCING AND OPERATIONS

Under normal circumstances, **information influencing** aims to systematically influence public opinion and decision-makers, and thus society's ability to function. The aim is to manage the information space especially through the use of social media platforms. Information operations can generate and distribute disinformation on these platforms, thereby mobilising large numbers of people and increasing public unrest and confrontation. Different actors in society aim to combat disinformation and aggressive and anonymous influence on the Internet within their respective areas of responsibility. Independent media and the citizens' level of education play a key role and are part of society's information defence.

Information warfare means influencing social and military decision-making and operational capacity as well as citizens' opinions, i.e. gaining information superiority. The purpose of information defence is to protect national defence functions from the effects of externally directed communications and other communications carried out with the intent to cause harm. It is particularly important to identify the need to coordinate different operating methods between authorities, businesses and other actors. In addition, capability development requires cooperation with all authorities and international partners.



5.4 ELECTRONIC INFLUENCING AND OPERATIONS

All frequencies of the electromagnetic spectrum are used in research, government services, military applications and in many everyday applications. One development is the continuous shift towards the use of ever larger frequencies in order to enable the transfer of ever larger amounts of data. The key area of application is communication (satellite, mobile, radio).

By means of electronic influence, the aggressor operates at level lower than the threshold of war. These operations protect the aggressors' systems and produce interference in opposition's devices and systems using the electromagnetic spectrum. A good example of this is Russia's GPS jamming during NATO military exercises. During the war in Ukraine, the practice has expanded.

By means of electronic warfare, the attacker seeks to influence the flow of information in such a way that the reliability of command and fire-control systems deteriorates and the usability of information structures decreases. Electronic warfare operations are linked to information and cyber operations. The purpose of electronic offensive operations is to prevent, slow down or reduce the use of enemy systems that utilise electromagnetic radiation or depend on electronics, or to direct the use to an area that is advantageous for one's own operations.

5.5 COGNITIVE INFLUENCE AND WARFARE

Technological advances in the cyber and information age have taken the next step towards cognitive influence and warfare. Development presents a challenge that is difficult to manage. In it, our understanding of the world and our reactions to its events are gradually disrupted over a long period of time and subtly, producing significant adverse effects over time. Cognitive influence and warfare targets everything from individuals to states and multinational organizations. It feeds disinformation and propaganda techniques designed to saturate and paralyze the recipients of information psychologically. We are all part of this influence, consciously or subconsciously, and open societies in particular are vulnerable.

Cognitive influence and warfare bring a significant new dimension to the digital society and battlefield and challenge our comprehensive security model. In addition to the land, sea, air and information domains, as well as the cybernetic, spatial and electromagnetic domains, a cognitive dimension has emerged. Modern technologies can be used to manage cognitive battlespace globally. This is made possible by the global networking of societies and individuals (hyper-connectivity).

The purpose of cognitive influence is to change the cognitive processes of the adversary, exploit prejudices and mental behaviors, and distort perceptions in order to achieve an impact to distortions of thinking, changes in decision-making and actions, even causing disastrous consequences at both the individual and collective level. The development is enabled by NBIC (Nanotechnology/ Biotechnology/Information Technology and Cognitive Science) development. NBIC can also be used to improve the cognitive capabilities of leaders and combatants, develop human-machine interfaces, and leverage robotics and cognitive technologies (AI/ML) collaboration.

In cognitive influencing, AI can be used to intimidate opponents' decision-makers and manipulate public opinion. Dealing with the direct manipulation of public opinion requires complex action. Various measures are taken to influence, protect and/or interfere with individual and group cognitive sensations. Activities vary greatly depending on operating environments and cultures. In cognitive influence, the human mind becomes a battlefield. The goal is to change not only what people think, but also how they act and influence as a part of digital society. In cognitive influencing, artificial intelligence in its various forms is brought to different levels of society. Generic AI can produce text, sound and images to produce disinformation, fake news and smear campaigns. Continuous advances in artificial intelligence, cognitive sciences, neurotechnology and other related fields further increase the risk of mass manipulation and enable the militarisation of the mind. In future, this must be taken into account when considering measures to maintain citizens' mental resilience to crises.

Cognitive warfare represents also a shift in paradigm in the conduct of military operations. It is the strategic use of artificial intelligence and machine learning to influence the cognitive processes of adversaries. The goal is to manipulate the decision-making process, create confusion and ultimately gain a strategic advantage. This approach is increasingly recognized as a powerful tool in modern warfare as it leverages the power of AI to increase human capabilities. Cognitive warfare combines and synchronizes elements of traditional kinetic and non-kinetic forms of warfare to influence the attitudes and behaviour of actors (soldiers and politicians). It seeks to influence the minds of opponents and shape their decisions, thereby creating a strategically favorable environment or subjugating them without a fight.

6 CYBER-SECURE SOCIETY

6.1 NATIONAL SECURITY

National security is about the common security of the entire Finnish society and Finland's sovereignty. As a concept, national security is dynamic and defined both in time and in relation to Finland's changing threat and operating environment.

In the new non-kinetic threat environment of normal and emergency conditions in the digital world, it makes sense to examine national security through two concepts: comprehensive security and comprehensive national defence. Comprehensive security is a cooperation model for preparedness in Finland, in which the vital functions of society are taken care of in cooperation between authorities, businesses, organisations and citizens. Its operating model is based on an efficient and extensive information acquisition, analysis and collection system, shared situational awareness, and national as well as international cooperation in preparedness. The general principles of comprehensive security are outlined in the Security Strategy for Society, which is being reformed. Comprehensive national defence refers to activities in the civilian and military sectors that safeguard the living conditions and security of citizens against external threats caused by other states or other threats, and ultimately state independence. Comprehensive national defence arrangements enable the entire society to support military defence in emergency conditions. In the future, the content of these concepts will increasingly need to be considered from the perspective of non-kinetic threats, taking into account the resilience of the digital society and changes in it.

6.2 RESILIENCE OF SOCIETY

The resilience of society reflects a new management mentality, where security is linked to preparedness, facing unpredictable risks and living with uncertainty. The definitions of resilience and the meaning of the concept vary depending on the context and operating culture. Finland's security, well-being and security of supply are increasingly dependent on the continuity of society's key functions, which often cross borders and are outside national competence. The security of supply approach has begun to emphasise ensuring the continuity of organisations' operating processes and securing critical infrastructure already under normal conditions. Global logistics chains and partnerships and their cyber security will be emphasised in the future.

It is challenging to prepare effectively for every imaginable threat. It is therefore necessary to create favourable conditions for a resilience-based approach to promote national security, in particular in the protection of critical infrastructure. The concept of resilience describes the ability to withstand sudden shocks and recover from them. Security and related resilience are key factors in ensuring the continuity of society's vital functions, and particularly the functioning of its critical infrastructure. Proactive situational awareness and good risk awareness are increasingly important.

The purpose of the European Galileo PRS service is to produce verified time and location information that is better resistant to disturbances, interference and manipulation from 2026 onwards for the various authorities of the EU member states and operators of critical infrastructure. It reduces dependence on other satellite systems. The service clearly improves Finland's safety and security of supply. Finland's geographical position poses challenges, which is why it is good that the PRS service will be introduced as soon as it is available. The PRS service will produce significantly more secure time and location data compared to open satellite-based time and location services. The PRS service supports comprehensive security in Finland and is part of ensuring Finland's national cyber security. The introduction of the service will also have a positive impact on Finland's security of supply by reducing the dependence of Finnish operators on time and place systems outside Europe. In Finland, the PRS service is intended to be used by the authorities of the Ministry of the Interior and the Ministry of Social Affairs and Health, the Finnish Defence Forces, Finnish Customs and critical infrastructure operators, such as telecom operators and operators in the energy, financial and logistics sectors.

6.3 THE CURRENT STATE OF COMPREHENSIVE SECURITY MANAGEMENT

Finland's comprehensive security operating model is based on an efficient and extensive information gathering, analysis and collection system, shared situational awareness, and preparedness for national and international cooperation. Strategic management of comprehensive security means the implementation of national security and defence reports, strategies and long-term planning. Strategic management takes society towards the set target state. The task of implementing strategic leadership is based on identifying and setting goals derived from securing the digital operating environment.

National management at the strategic level of comprehensive security consists of three parts:

1. Safety management under normal conditions
2. Management of incidents under normal and emergency conditions
3. Management of preparedness and security of supply

Serious disturbances can occur under both normal and emergency conditions. Disturbances in normal conditions are managed with the normal powers of the authorities and the resources of organisations. Systems and contingency measures built under normal conditions lay the foundation for operations under emergency conditions. Correspondingly, the arrangements created for emergency conditions can be utilised in the management of disturbances under normal conditions. Preparedness combines security of supply and ensuring self-sufficiency. This means safeguarding economic activities and related technical systems necessary for the livelihood of the population, the country's economy and national defence in the event of emergencies and comparable serious disturbances. Preparedness is guided by the obligations set for various vital functions and the organisations' own goals, especially in terms of business continuity management.

6.4 DEVELOPING COMPREHENSIVE SECURITY MODEL AND SECURITY OF SUPPLY

Useful experiences have been gained from the war in Ukraine to develop Finland's comprehensive security model. From the perspective of strategic management, and especially as digitalisation increases, it is essential that the measures required to manage large-scale cyber incidents that arise suddenly and quickly in society can be started quickly.

Cyber incidents are characterised by the multidimensional nature of their impact, which is why it is also necessary to mobilise the broadest possible cross-sectoral support for the competent authority where necessary. At the same time, it must be possible to ensure the functioning of society at an appropriate level despite disruptions. The management of disruptions in the cyber environment and the electromagnetic spectrum as well as hybrid, information and cognitive influencing together with preparedness require stronger leadership. The operating model for comprehensive security is highly functional within itself, but when moving to the operational level, one must have the ability to react quickly to rapidly changing threat scenarios.

One example could be the strategic management of US cybersecurity, which is the responsibility of The Office of the National Cyber Director (ONCD), located in the White House. Its tasks are:

- Ensure the implementation of the federal cybersecurity strategy and guidelines
- Improve public-private collaboration Public-Private Partnership (PPP)
- Allocate resources according to federal goals
- Increase existing and future cyber resilience

In Finland, too, the cyber security management model and management responsibilities should be clarified. Cyber-attacks always come unexpectedly and progress faster than before, which challenges our comprehensive security management model. A "national cyber fist" would be needed to maintain society's vital functions and critical infrastructure in the event of unexpected disruptions. Developing cooperation between authorities and companies must be a continuous process.

The operational capabilities and systems of military defence are increasingly based on digitalisation, information and the utilisation of space. The defence system must be able to monitor different operating environments more comprehensively than before, understand cross-effects between them and, if necessary, initiate defensive measures in different environments. It must be possible to detect cyber threats in time and monitor changes in the cyber environment in real time. Effective cyber defence surveillance and situational awareness is used to detect and identify state and other threat actors and prevent

them from accessing systems and information that are essential for the defence system. Military cyber defence is increasingly dependent on the cyber resilience of the hole society. The Finnish conscription system is a valuable success factor, and its significance is emphasised especially in the development of competence in critical areas and in the organisation.

6.5 SECURITY OF CYBER SUPPLY

Security of supply is one of the basic pillars of society's comprehensive security. The operating logic of securing cyber supply differs from traditional security of supply securing. In cyberspace, processes as well as production and supply chains are particularly emphasized. In cybersecurity, several national critical processes are integrated into various global operating processes and logistics chains. Practical examples include servers located abroad, cloud services and financial assurance chains. It is impossible to maintain or manage the security of the supply network through national measures alone. The operations require cross-border network capability as well as international cooperation and partners. Ensuring cyber security and securing cyber supply security are also challenged by the fragmentation of the operating environment, the speed of changes and political developments that are difficult to predict.

Well-functioning national and international markets, a diverse industrial and other production base, and competitive stable public finances form the basis of security of supply. A key part of preparedness is active cooperation and agreements between authorities and companies. The ability of market participants to adapt to disruptions and ensure the continuity of their operations determines the crisis resilience of critical production and services.

Security of supply is built on the ability of companies operating in critical sectors to react to disruptions in normal - emergency conditions and to recover quickly from them. Even in crisis situations in society, the starting point is market-based operations. If the market is unable to maintain the basic economic and technical functions of society during disturbances and emergencies, measures are needed to safeguard society as a whole. Planning and preparation for business continuity management lays the foundation for the ability to operate under emergency conditions. The war in Ukraine has shown the importance of international partnerships and well-functioning logistics chains. This must be taken into account already when considering arrangements under normal conditions. At the national level, it must be ensured that the market functions as efficiently as possible for the benefit of the national economy, consumers and the security of the country. When competition in the market works well, it encourages companies to develop products and services that are affordable for the user and better meet their different needs. The large market offers users of cyber security products and services sufficient options from which they can choose the most suitable one. In the cyber market, this means also the development of dual-use products. A dual-use item is a product that is suitable not only for normal civilian use, but also for military purposes. Public-private partnerships play an important role in the implementation of security of supply measures. Security of supply is also safeguarded in certain sectors by means of binding regulations. Legislation must be developed so that authorities can develop structures and operating models that support security of supply. This is especially important in situations where the market alone is not sufficient to maintain the required level of security of supply.

According to the current Government Programme, the perspective of security of supply will be considered in all decision-making in all administrative branches. The Government will ensure a sufficient level of security of supply so that the production, services and infrastructure necessary for the livelihood, economy and defence of the population can be secured in severe disturbances and emergencies under normal conditions. In addition, the Government will ensure, by means of a government decision on security of supply, that the level of security of supply meets the requirements of the changed security environment and investigate the effects of geopolitical risks and dependencies on security of supply. According to the programme, security of supply will be strengthened by developing international cooperation through the EU and NATO and bilaterally with various states. The Government will further examine the need and possibilities to reform public procurement regulation within the framework of EU regulation so that the needs of security of supply are sufficiently considered. Hopefully, these measures will be implemented and contribute to the development of the resilience of critical functions in our society. Operations always require cross-border networking capabilities as well as international cooperation and partners.

7 COOPERATION BETWEEN PUBLIC AUTHORITIES AND BUSINESS

In the Public-Private Partnership model (PPP) the public and private sectors work together to achieve set common goals. Public-private partnerships create an opportunity to combine the expertise of different parties and create new solutions and services. In the PPP model, attention should be paid to the mutual benefits of cooperation between the private and public sectors. National cyber security requires extensive and close cooperation between authorities, third sector organisations and business life. Cooperation means very different ways of working and it can be long-term, or project based. Clear cooperation structures and long-term enterprise resource planning support the development of cyber security and cooperation between authorities operating in different administrative branches. Mutual trust between national authorities and companies must be strengthened, giving companies a view of a competitive operating environment and the certainty to invest.

The current Government Program states that a strong industrial policy supports the resilience of society as a whole and the development of security of supply. Investments in digital technology and its effective application are at the core of companies' competitiveness and growth. This means developing the cybersecurity sector between state and private actors, including building mutual trust, effective implementation of strategies, comprehensive security of critical infrastructure, standardization and cooperation with partners. Especially in cyber security, a strong and long-term industrial policy is needed to develop Finland's and Europe's strategic competitiveness, self-sufficiency and security of supply. The expansion of digitalisation requires strengthening cybersecurity, with special themes such as quantum computing, high-speed wireless networks and artificial intelligence. This requires a dedicated cyber industry strategy/technology program that:

1. Fosters cooperation that is directly beneficial to authorities and businesses.
2. Creates permanent networking between companies and authorities.
3. Includes public and private education as well research sectors.
4. Links together the different levels of cooperation (national – regional – local).
5. All parties have a real opportunity to influence the operations.

The PPP partnership related to cybersecurity should be clearly described in national policies and/or legislation. This requires recognising the importance of public-private arrangements in national cybersecurity policies and strategies. There will be a growing need for transparent consultation of the private sector on political, legislative and regulatory decisions affecting it.

8 CONCLUSIONS

This study has focused on four areas of addressing lessons learned from the war in Ukraine and the challenges of the modern digital society:

1. Core of critical infrastructure
2. Cyber-secure society
3. Security of cyber supply
4. Public-private partnership

The strategic objective of national security must be to secure the functioning of society's critical services and infrastructure in all circumstances. This must be done by strengthening the resilience of critical infrastructure, especially core of critical infrastructure as part of a cyber-secure society with special attention to cyber security and close cooperation between the public and private sectors. The definition of critical infrastructure should be specified, considering complex interdependencies and extensive asymmetric means of influencing. Crisis management preparedness must be developed both nationally and at the level of individual companies. The importance of security of supply, preparedness and continuity management will be further emphasised.

THE FIGURE BELOW SHOWS THE FOUR PILLARS OF THIS REPORT.

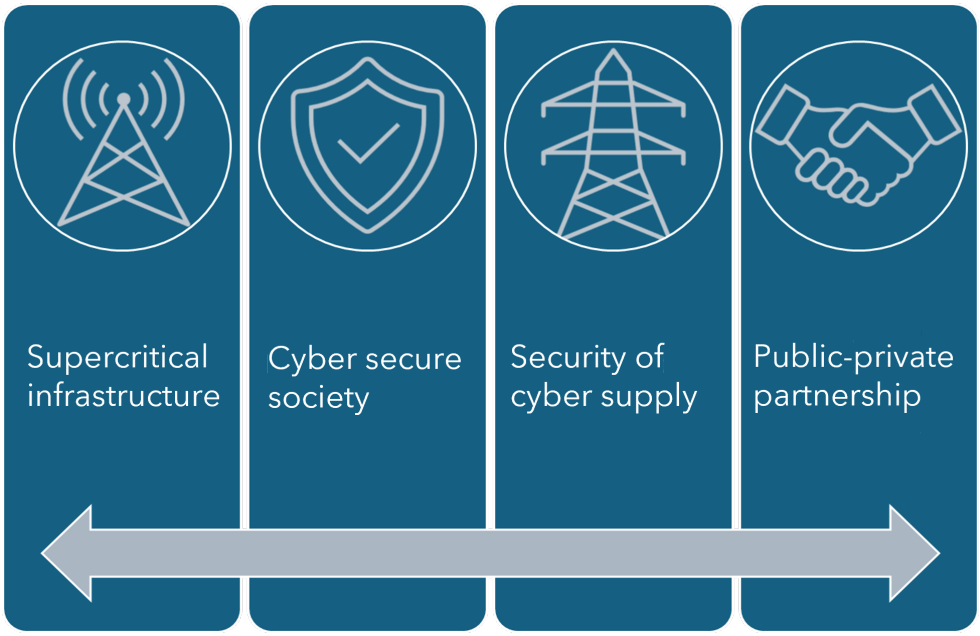


Figure 4. The four pillars of development

CORE OF CRITICAL INFRASTRUCTURE:

- Defining core of critical infrastructure as part of national critical infrastructure and services
- Develop a dedicated cybersecurity program for this critical infrastructure, taking into account both non-kinetic and kinetic influencing in different readiness states and disruptions.
- Intensify measures to implement the requirements of EU regulation regarding core of critical infrastructure, aiming for the highest possible degree of domestic content and well-functioning international partnerships.
- Clarification of critical infrastructure definition, coordination and crisis management arrangements.
- Improve threat and risk awareness among critical infrastructure actors.

CYBER-SECURE SOCIETY:

- Develop a comprehensive action plan that considers the full spectrum of non-kinetic influencing and operations (hybrid-information-cyber-electronic-cognitive).
- Develop a national cyber risk analysis, considering the lessons learned from the war in Ukraine and the change in the operating environment.
- Define a clear national non-kinetic security leadership responsibility and management structures – “cyber fist".
- Strengthen the leadership of non-kinetic warfare by establishing a National Cyber and Information Command.
- Develop cyber security measures to strengthen Finland's digital independence and strategic autonomy as part of the European Union.
- Develop cyber threat intelligence capacity and national cyber situational awareness.

SECURITY OF CYBER SUPPLY:

- A comprehensive and long-term technology/security of supply program will be formed for a non-kinetic operating environment.
- The EU Framework of Reference will define the key principles for strengthening domestic production of cybersecurity products and services.
- Strengthen the national cyber security supply ecosystem and the international partnership network.

PUBLIC-PRIVATE PARTNERSHIP:

- Develop a closer cooperation model between the public and private sectors that strengthens trust and related practical measures.
- Develop and provide centralised, reliable and cost-effective cyber security services together with the public and private sectors.
- Develop more efficient mechanisms for exchanging and analyzing information, risk analysis and situational awareness.
- Develop a joint contingency plan to maintain cyber security of supply, covering normal conditions and various disruptions all the way to emergency conditions.

The war in Ukraine provides a lot of useful information for developing the comprehensive security of our society. A radical change in our operating environment requires clear measures and new thinking, innovation and leadership. Change factors are often surprising and happen quickly. In companies, risk analysis is an ongoing process. In future, this should be the case at national level. The development of situational awareness activities covering the whole of society will focus and should create a clearer basis for national risk analysis. Companies could share their own threat and risk information to complement the activities of the authorities. Similarly, attention should be paid to ensuring that the sharing of critical information is not left unshared due to the "boundaries" of administrative branches. The management of the whole is emphasised, and special attention should be paid to maintaining a risk assessment of core of critical infrastructure and monitoring the threat environment and improving observation capabilities.

Cyber security is always the responsibility of the organisation's management. The management of organisations should regularly review the effects of changed cyber security threats on their own operations, taking into account changes in legislation that contribute to the implementation of cyber security.

The constantly evolving and expanding cyber security environment requires organisations to reserve sufficient resources to ensure cyber security and implement the necessary measures, with particular emphasis on operational management and cyber risk management.

Public and private sector measures and other arrangements related to cybersecurity need to have clearer objectives and approaches. This requires closer ecosystem cooperation, a clear understanding of the national cybersecurity space, identification of key areas where cooperation would be most effective and strengthening mutual engagement. This requires effective strategic management of national cyber security, both in preparedness and in the management and management of disruptions in normal and emergency conditions. Special attention should be paid to developing crisis management capabilities at different levels of government and in the preparedness of companies critical to society.

MAIN SOURCES:

Cyberwatch Finland publications 2022–2024

du Cluzel Francois. 2023. Cognitive Warfare, a Battle for the Brain, ACT Norfolk, Virginia

Huoltovarmuuskeskus. 2024. Website, https://www.huoltovarmuuskeskus.fi/

Koichiro Takagi. 2022. New Tech, New Concepts: China's Plans for AI and Cognitive Warfare, War on the Rocks, April 13, 2022.

Kosola Jyrki & Jokinen Janne. 2004. Elektroninen sodankäynti, osa 1 – taistelun viides dimensio. Tekniikan laitos, julkaisusarja 5, No 2/2004, Helsinki: Maanpuolustuskorkeakoulu.

Lehto Martti & Limnéll Jarno. 2017. Kybersodankäynnin kehityksestä ja tulevaisuudesta, kirjassa Silvasti M (Edit.) Tiede- ja Ase, 2017, sivut 179–212.

Lehto Martti, Limnéll Jarno, Kokkomäki Tuomas, Pöyhönen Jouni, Salminen Mirva. 2018. Kyber-turvallisuuden strateginen johtaminen Suomessa, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018, maaliskuu 2018.

Lehto Martti, Neittaanmäki Pekka. 2016. Digitalisaatio muuttaa yhteiskunnan ja yksilöiden tapaa toimia, Tiedepolitiikka 1/2016, s. 56–64.

Park Jin. 2023. AI in Warfare: The Dawn of Cognitive Combat, 31. May 2023.

Pohjankoski Merja. 2023. Kyberhyökkäyksistä Ukrainassa 2022, pro gradu research, Jyväskylän yliopisto.

Pye Graeme and Warren Matthew. 2011. Analysis and Modelling of Critical Infrastructure Systems, Proceedings of the 10th European Conference on Information Warfare and Security, The Institute of Cybernetics at the Tallinn University of Technology Tallinn, Estonia, 7-8 July 2011, s. 194-201.

Pöyhönen, Jouni. 2020. Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu, JYU Dissertations 270, 67–70.

Tvaronavičienė M., Plėta T., Della Casa S. 2021. Cyber Security Management Model for Critical Infrastructure Protection, International Scientific Conference, 13–14 May 2021, Vilnius, Lithuania.

Valtioneuvoston kanslia. 2017. Valtioneuvoston puolustusselonteko, Valtioneuvoston kanslian julkaisusarja 5:2017.

Valtioneuvoston kanslia. 2018. Valtioneuvoston päätös huoltovarmuuden tavoitteista, Valtioneuvoston päätös 1048/2018.

Valtioneuvoston kanslia. 2020. Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko, Valtioneuvoston kanslian julkaisusarja 30:2020.

Valtioneuvoston kanslia. 2021. Valtioneuvoston puolustusselonteko, Valtioneuvoston kanslian julkaisusarja 28:2021.

Valtioneuvoston kanslia. 2022. Valtioneuvoston huoltovarmuusselonteko, Valtioneuvoston julkaisuja 8:2022.

Valtioneuvoston kanslia. 2023. Vahva ja välittävä Suomi - Pääministeri Petteri Orpon hallituksen ohjelma, Valtioneuvoston julkaisuja 58:2023.

Cyberwatch Finland

PUBLISHER
Cyberwatch Finland
Nuijamiestentie 5 C
04400 Helsinki
www.cyberwatchfinland.fi

CONTENT
CEO
Aapo Cederberg
aapo@cyberwatchfinland.fi

Subeditor
Elina Turunen
elina@cyberwatchfinland.fi

LAYOUT
Elina Turunen
elina@cyberwatchfinland.fi

ILLUSTRATIONS
Gencraft
Pixabay
Shutterstock

ISSN 2490-0753 (print)
ISSN 2490-0761 (web)

PRINT HOUSE
Scanseri Oy, Finland

A PASSION FOR A SAFE CYBER WORLD

Contact

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
myynti@cyberwatchfinland.fi