PUBLICATIONS OF THE PRIME MINISTER'S OFFICE 2024:13

Finland's Cyber Security Strategy 2024–2035

PRIME MINISTER'S OFFICE

Publications of the Prime Minister's Office 2024:13

Finland's Cyber Security Strategy 2024–2035

Prime Minister's Office Helsinki 2024

Publication distribution

Institutional Repository
for the Government
of Finland Valto

julkaisut.valtioneuvosto.fi

Prime Minister's Office

ISBN pdf: 978-952-383-462-0
ISSN pdf: 2490-1164

Layout: Government Administration Department, Publications

Helsinki 2024 Finland

Description sheet
25 October 2024

Finland's Cyber Security Strategy 2024–2035

Publications of the Prime Minister's Office 2024:13

Publisher	Prime Minister's Office		
Author(s)	Chair Rauli Paananen, Vice-Chair Mikko Soikkeli, Secretariat Chair Mari Starck, Secretariat Members Mari Aro, Tuija Kuusisto, Tuomo Rusila, Tiina Tuulensuu.		
Group author	Ministry of Transport and Communications		
Language	English	**Pages**	59

Abstract

Finland's Cyber Security Strategy has been revised in response to an evolving operating environment in accordance with the programme of Prime Minister Petteri Orpo's Government. This revision accommodates the requirements imposed in the cybersecurity directive (NIS2) and other relevant key strategies and reports. The aim is to integrate the information defence entries of the Government Programme into the strategic communications model and the Government Defence Report.

The goals of the cybersecurity strategy extend to 2035. The strategy includes strategic objectives defined under four pillars, and common development measures for these objectives.

The strategy was prepared under the leadership of the National Cyber Security Director on a subcommittee of a project initiated by the Prime Minister's Office on 8 March 2024 to develop an operating model for government security management. This subcommittee included appointees from the Prime Minister's Office, Ministry for Foreign Affairs, Ministry of Justice, Ministry of the Interior, Ministry of Defence, Ministry of Finance, Ministry of Education and Culture, Ministry of Agriculture and Forestry, Ministry of Transport and Communications, Ministry of Economic Affairs and Employment, Ministry of Social Affairs and Health, and Secretariat of the Security Committee.

Nearly 100 organisations from the public and private sectors, the scientific community and civil society participated in strategy preparation workshops.

Keywords cyber security, comprehensive security, data security, digitalisation, know-how, technology, research and development operations, innovation activity, preparedness, security of supply, international cooperation, cyber crime

ISBN PDF	978-952-383-462-0	**ISSN PDF**	2490-1164
Reference number	VN/36693/2023	**Project number**	VNK007:00/2024
URN address	https://urn.fi/URN:ISBN:978-952-383-462-0		

Kuvailulehti
25.10.2024

Suomen kyberturvallisuusstrategia 2024–2035

Valtioneuvoston kanslian julkaisuja 2024:13

Julkaisija	Valtioneuvoston kanslia		
Tekijä/t	Puheenjohtaja Rauli Paananen, varapuheenjohtaja Mikko Soikkeli, sihteeristön puheenjohtaja Mari Starck, sihteeristön jäsenet Mari Aro, Tuija Kuusisto, Tuomo Rusila, Tiina Tuulensuu		
Yhteisötekijä	Liikenne- ja viestintäministeriö		
Kieli	englanti	**Sivumäärä**	59

Tiivistelmä

Suomen kyberturvallisuusstrategia on uudistettu pääministeri Petteri Orpon hallitusohjelman mukaisesti vastaamaan muuttunutta toimintaympäristöä. Kyberturvallisuusstrategian uudistamisessa on otettu huomioon kyberturvallisuusdirektiivin (NIS2) vaatimukset sekä muu aiheeseen liittyvä keskeinen strategia- ja selontekotyö. Hallitusohjelmaan kirjattu informaatiopuolustus on tarkoitus huomioida osana strategisen viestinnän toimintamallia ja puolustuspoliittista selontekoa.

Suomen kyberturvallisuusstrategian tavoitetila ulottuu vuoteen 2035. Strategia sisältää neljän pilarin alle muodostetut strategiset tavoitteet ja näille yhteiset kehittämistoimet.

Strategia on valmisteltu valtion kyberturvallisuusjohtajan johdolla valtioneuvoston kanslian 8.3.2024 asettaman Valtioneuvoston turvallisuusjohtamisen toimintamallin kehittäminen -hankkeen alatyöryhmässä. Työryhmään kuuluivat nimetyt jäsenet valtioneuvoston kansliasta, ulkoministeriöstä, oikeusministeriöstä, sisäministeriöstä, puolustusministeriöstä, valtiovarainministeriöstä, opetus- ja kulttuuriministeriöstä, maa- ja metsätalousministeriöstä, liikenne- ja viestintäministeriöstä, työ- ja elinkeinoministeriöstä, sosiaali- ja terveysministeriöstä ja Turvallisuuskomitean sihteeristöstä.

Strategian valmistelutyöpajoihin on osallistunut lähes 100 julkisen ja yksityisen sektorin, tiedeyhteisön sekä kansalaisjärjestön organisaatiota.

Asiasanat	kyberturvallisuus, kokonaisturvallisuus, tietoturva, digitalisaatio, osaaminen, teknologia, tutkimus- ja kehittämistoiminta, innovaatiotoiminta, varautuminen, huoltovarmuus, kansainvälinen yhteistyö, kyberrikollisuus

ISBN PDF	978-952-383-462-0	**ISSN PDF**	2490-1164
Asianumero	VN/36693/2023	**Hankenumero**	VNK007:00/2024

Julkaisun osoite https://urn.fi/URN:ISBN:978-952-383-462-0

Presentationsblad
25.10.2024

Strategi för cybersäkerheten i Finland 2024–2035

Statsrådets kanslis publikationer 2024:13

Utgivare	Statsrådets kansli		
Författare	Ordförande Rauli Paananen, vice ordförande Mikko Soikkeli, sekretariatets ordförande Mari Starck, sekretariatets medlemmar Mari Aro, Tuija Kuusisto, Tuomo Rusila, Tiina Tuulensuu		
Utarbetad av	Kommunikationsministeriet		
Språk	engelska	**Sidantal**	59

Referat

Strategin för cybersäkerheten i Finland har reviderats i enlighet med regeringsprogrammet för statsminister Petteri Orpos regering för att motsvara den förändrade verksamhetsmiljön. I revideringen av Strategin för cybersäkerheten i Finland har man beaktat kraven enligt cybersäkerhetsdirektivet (NIS 2) samt annat centralt strategi- och redogörelsearbete som anknyter till ämnet. Informationsförsvaret som skrivits in i regeringsprogrammet ska beaktas som en del av verksamhetsmodellen för strategisk kommunikation och den försvarspolitiska redogörelsen.

Målsättningen för strategin för cybersäkerheten i Finland sträcker sig till år 2035. Strategin innehåller strategiska mål som formulerats under fyra pelare och gemensamma utvecklingsåtgärder för dessa.

Strategin har beretts under ledning av statens cybersäkerhetsdirektör i underarbetsgruppen för projektet för utveckling av verksamhetsmodellen för statsrådets säkerhetsledning som statsrådets kansli tillsatte 8.3.2024. Arbetsgruppen har bestått av utsedda medlemmar från statsrådets kansli, utrikesministeriet, justitieministeriet, inrikesministeriet, försvarsministeriet, finansministeriet, undervisnings- och kulturministeriet, jord- och skogsbruksministeriet, kommunikationsministeriet, arbets- och näringsministeriet, social- och hälsovårdsministeriet och Säkerhetskommitténs sekretariat.

I de förberedande workshopparna för strategin deltog nästan 100 aktörer inom den offentliga och privata sektorn, vetenskapssamfundet samt det civila samhällets organisationer.

Nyckelord cybersäkerhet, övergripande säkerhet, informationssäkerhet, digitalisering, kompetens, teknologi, forsknings- och utvecklingsverksamhet, innovationsverksamhet, beredskap, försörjningsberedskap, internationellt samarbete, cyberbrottslighet

ISBN PDF	978-952-383-462-0	**ISSN PDF**	2490-1164
Ärendenummer	VN/36693/2023	**Projektnummer**	VNK007:00/2024
URN-adress	https://urn.fi/URN:ISBN:978-952-383-462-0		

Contents

PREFACE

Our revised cybersecurity strategy responds to evolving geopolitical circumstances and technological development. It continues a tradition of more than 20 years of ensuring cybersecurity in Finnish society. While the cybersecurity situation in Finland remains good, staying abreast of continual change requires continuous improvement.

Cybersecurity is a vital component in the Finnish model of comprehensive security. Our society is almost entirely digitalised, and as part of a trust-based society, we also want to continue ensuring that people in Finland can rely on the cybersecurity of digital services. Cybersecurity calls for responsible leadership and commitment from all stakeholders in society. The EU cybersecurity directive also requires stronger participation from various sectors of society to ensure the reliability of all digital services.

The European Union is Finland's most important political and economic frame of reference and community of values in cybersecurity. Most current cybersecurity regulation and other policy measures originate in the European Union. Finland actively influences these policies. While NATO membership strengthens Finland's cybersecurity and cyber defence, it also imposes new obligations. We seek to be a strong cybersecurity partner in the European Union and NATO. The forthcoming cyber defence doctrine will provide national operating principles for responding to state-sponsored threats and threats against national security. We shall prepare nationally for active cyber defence and the possibility of attribution and countermeasures.

The strategy is, and necessarily must be bold and ambitious. The core of the Finnish cybersecurity operating model is cooperation between various stakeholders. Implementing the strategy will require a review of official powers, and of conditions for exchanging information. Trust-based cooperation between public authorities and the private sector must be maintained. We can combat ever-increasing and diversifying cybercrime through cooperation and adequate resourcing of public authorities.

Emerging and disruptive technologies are a global challenge. We have the necessary expertise to become a leading quantum security society. The time to take action is now. This will require an even stronger Finnish ecosystem of cybersecurity and cooperation between government and the business community.

The strategy envisages a time frame of ten years, facilitating future investment in strategy implementation. Various European Union and NATO funding programmes will form an important instrument for developing national capabilities, innovating new kinds of export products, and supporting national preparedness.

Involving and listening to various stakeholders has been fundamental to our strategy. Hundreds of specialists and stakeholders from the public and private sectors, the scientific community and civil society organisations have participated in formulating the strategy. This is an excellent illustration of the commitment of Finnish society and the Finnish model of comprehensive security.

Petteri Orpo, Prime Minister

October 2024

1 Introduction – cybersecurity is part of comprehensive security

Cybersecurity is part of Finland's comprehensive security and digitalising society, helping to ensure operating conditions for national security, national defence, security of supply, business community and civil society. A shift in geopolitical conditions has further underlined the importance of national and international cooperation in ensuring cybersecurity, with an increased need in particular for cooperation between public authorities and the business community, supporting the resilience of society, and responding to hostile activity. The operating environment is strongly characterised by accelerating digitalisation, the development of new technologies and associated global competition, continually growing interdependencies, and other megatrends that affect the future, such as climate change and demographic change. Basic societal structures and services, such as information and communication networks and associated infrastructure, must function under all circumstances.

The national cybersecurity strategy has been revised in response to the evolving operating environment as outlined in the Government Programme of Prime Minister Petteri Orpo. Cybersecurity generally means protective measures taken against cyber threats to communication and information systems and other electronic systems, to the data stored, processed or transferred in them, and to their users, appliers and other concerned parties. Cybersecurity has traditionally been viewed from a more technical perspective, and not so much as a matter of national security. This strategy particularly relates to national cybersecurity, meaning the measures that enable a digital society to prepare for, identify, combat and withstand incidents in electronic and networked systems and their impacts on vital functions and services of society, to recover from them, and to ensure the operating conditions for national security, national defence and security of supply.

The European Union cybersecurity directive (NIS2) and its national implementation have also required a revision of the cybersecurity strategy. Finland's revised cybersecurity strategy is the third of its kind, and continues to promote the cybersecurity ecosystem philosophy that was introduced in a development programme based on the previous cybersecurity strategy. Preparation of the strategy has accommodated other pertinent strategy and reporting work, most notably on the following government resolutions: Finland's Cybersecurity

Development Programme, the TITUKRI resolution to improve information security and data protection in critical sectors of society, Digital Security in the Public Sector, and the Digital Compass Government report and associated implementation plan. The preparation work also considered a 2023 report on the authorities' capacity to act in cyber security matters and the observations and areas for development that this report exposed. The preparations also collaborated with other ongoing projects that were initiated under the Government Programme.

The target state for Finland's cybersecurity strategy extends to 2035. The need to update the strategy will be assessed at five-yearly intervals, with the strategy developed or updated more frequently as required.

Finland currently spends nearly EUR 300 million annually to ensure cybersecurity in central government, while the sum spent by the business community is at least ten times larger. Current basic funding levels nevertheless remain insufficient to respond to the evolving operating environment.

Development proposals arising from the target state of the strategy will be implemented according to a separate implementation plan.

The key terms used in this document are defined at the end of the strategy. A description of the national cooperation model for cybersecurity is also appended to the strategy.

2 Target state and structure

The strategic objectives fall within four areas, or pillars: **I Competence, technology, and research, development and innovation activities (RDI); II Preparedness; III Cooperation; and IV Response and countermeasures.**

Figure 1. Target state and structure of the cybersecurity strategy.

3 Changes in the operating environment

The security environment of Finland and Europe has changed radically since the previous national cybersecurity strategy was published in 2019. Accelerating digitalisation further boosted by the Covid-19 pandemic, the Russian invasion of Ukraine, the increasingly tense global geopolitical situation, Finnish membership of NATO, and rapid development of EU regulation affecting cybersecurity all highlight the importance of cybersecurity as part of safeguarding society.

3.1 Challenges posed by diverse threats

An evolving operating environment is challenging the international rules-based system. Threats have become increasingly diverse, with the cyber environment used extensively in hybrid influencing efforts, crime, terrorism and warfare. Hybrid influencing efforts are also used between states to advance political objectives. Nor is the threat posed by state-sponsored cyber espionage confined solely to formulating foreign and security policies. Unlawful data acquisition may also target the intellectual capital of Finnish businesses, jeopardising the competitiveness of the economy.

Cyber domain incidents may also be caused by various physical threats, such as power supply disruptions, floods, earthquakes, other natural disasters or solar activity, and damage due to human error. These may also disrupt data connections or the functioning of information systems, and subsequently threaten cybersecurity.

3.2 Hostile cyber operations targeting Finland are likely to increase

Various hostile cyber operations against Finland are likely to continue and increase in future. The digitalisation of society creates new kinds of opportunity for state-sponsored operators, including the ability to conduct intelligence collection and exploit vulnerabilities with no significant risk of exposure.

Besides technical incidents, the impact of hostile operations abroad may reach into Finland and spread unpredictably, even when Finland is not the primary target. The need for cross-border cooperation increases when hostile cyber operations grow and also more extensively target governments, democratic institutions, businesses and individuals. Familiarity with the operating environment, with information systems, and with their interdependencies in particular then becomes increasingly important.

3.3 Technological progress increases everyone's responsibility for cybersecurity

Breakthroughs in technology and the digitalisation of societies increase the number of information systems and services connected to the Internet, thereby making society increasingly vulnerable and susceptible to cyber incidents. The number of devices connected to the global public information network is expected to grow by the billions before the end of 2030. The causes of technological incidents include human error in software development and related supply chains, and intentional vulnerabilities, such as security backdoors that allow criminals and state-sponsored operators to access information systems. Rapid progress in emerging and disruptive technologies, such as artificial intelligence, quantum computing, cloud services, 6G technology and satellite technologies, creates challenges for cybersecurity. Regulation can promote the development of secure technology. Even as security measures are being implemented, attackers are also developing new ways to circumvent them.

3.4 International cooperation strengthens Finnish cybersecurity

While NATO membership strengthens Finland's security and defence, it also imposes new challenges and obligations. The deterrence effect of NATO membership may lead to an increasing shift in the focus of hostile operations from traditional threats to the cyber domain where perpetrators may more plausibly deny involvement. Technological progress, data-driven systems, international collaboration and analysis of the geopolitical connections of cyber operations nevertheless provide better prospects of attribution to state-sponsored operators in particular.

EU regulation on cybersecurity has progressed rapidly in recent years, strengthening the cybersecurity of Finland and other EU countries. National implementation of this regulatory framework and operational adaptation by organisations will accordingly challenge both public authorities and businesses in coming years. Competence and training needs, and the costs of establishing adequate safeguards will increase, with additional measures required to manage cyber risks. Regulation will establish conditions for improving the cybersecurity of critical societal actors and the integrated security of devices and software. Public authorities will also enhance their work in preparedness and incident management, and in responses and countermeasures.

Alongside EU and NATO membership, other bilateral or multilateral international cooperation in cybersecurity and cyber defence has expanded and deepened. The initiatives and cooperation of like-minded countries will help in responding to key cyber threats and improving collective cybersecurity. The UN and various regional organisations recognise the importance of cybersecurity to international security.

3.5 Developing a national cooperation model

The national cooperation model for cybersecurity is based on the ability to continually enhance the operation of information systems and organisations, so that they can withstand and recover from cyberattacks and technical incidents. The evolving operating environment and cyber threats are a challenge to previous ways of operating, with a greater need to improve preparedness measures and responses, and to take increasingly proactive coordinated countermeasures. The model of comprehensive security also enables the cybersecurity sector to prepare and develop cooperation in accordance with the Security Strategy for Society.

3.6 Increased cybercrime affects society as a whole

Serious cybercrime can disrupt the vital functions of society, threaten national security, or otherwise cause incidents that have a broad impact on society. Growing cybercrime and a rapid escalation of threats affect society as a whole. Cybercrime can jeopardise fundamental rights, erode trust in services, and cause considerable financial losses. It is increasingly linked to organised crime and state-sponsored operators. States often outsource hostile operations to various types of intermediary, such as criminal groups. By purchasing services from criminals, hostile states may seek such goals as hampering attribution or varying the intensity of their cyber operations.

It should be noted that a substantial proportion of the infrastructure that is critical for the functioning of society is owned by the private sector. Besides the framework of regulation, agreements and services, cooperation between public authorities and the private sector in Finland is voluntary and relies on trust, tending to facilitate the flow of information on such aspects as various threats and incidents. Continually increasing and diversifying cybercrime can also be tackled through cooperation and adequate resourcing of public authorities.

3.7 Highlighting the security of service and supply chains

The susceptibility of global supply chains to disruption has become part of our threat environment. An increasingly interdependent global economy also enables weaponisation of such elements as energy, raw materials, logistics and infrastructure for geopolitical purposes in cyberspace. Service and supply chains have become longer, more complex, and increasingly hard to manage. Supply chain attacks hack into the information systems of an organisation through the services that it purchases or through the hardware or software of its service providers. While it may be hard to endanger some service or system proper, or to secure unauthorised access to it, the disruptive aims of an attacker may be achieved equally well by influencing the associated supply chain. Actors that are critical for the functioning of society must therefore ensure the cybersecurity of their service providers and supply chains.

3.8 Cybersecurity enables business growth

The digitalisation of society generates significant business opportunities that boost growth, ranging from streamlining processes to implementing new learning methods or other opportunities provided through R&D work. Emerging and disruptive technologies such as artificial intelligence and quantum computing enable the emergence of new kinds of solution to future challenges in cyberspace. Such technologies are nevertheless also available to and usable by hostile operators, posing problems for current protection methods. Evolving conditions have also increased the need for new and effective innovations that reinforce cybersecurity.

4 Current state

Finland is a highly digitalised society. A continually growing proportion of daily human activity and use of public services is happening in a digital setting. Public administration and services in Finland accordingly often secure first place in international digitalisation rankings.

Security of the digital operating environment has been continually strengthened in Finland. International assessments and national self-evaluations suggest that Finland has achieved a relatively good standard of cybersecurity. Finnish technical expertise, understanding of cybersecurity, and collaboration between the public and private sectors (which also works well by international standards) in the field of cybersecurity may be considered an asset internationally and a potential export product.

4.1 Cybersecurity and the digitalisation of society

Finland's Digital Compass is a national strategic roadmap for developing digitalisation in Finland that extends to 2030. It seeks a consistent and determined reform of public administration that will reduce the workload of businesses and individuals in using public services. The Digital Compass describes the key objectives and outcomes of the cyber and digital security development that is required in order to achieve this.

While some major security breaches affecting the daily lives of ordinary people have also occurred in Finland, we have nevertheless been spared from cyberattacks with long-term debilitating impacts on the functioning of society. Hostile state-sponsored operations, cybercrime, denial-of-service attacks, data leaks and various malware and other incidents have nevertheless also become more common in Finland. New data scamming approaches enabled by artificial intelligence are already threatening both cyberspace and the information environment. There is a threat of new serious impacts that will be even more far reaching.

It may not be possible to fully repair the damage caused by cyber incidents that result in such outcomes as destruction or permanent disclosure of data. Some small businesses have even had to discontinue operations after cybersecurity risks materialised. Personal data breaches can have a massive impact on human welfare and on the trust of individuals in the functioning of society. These prospects further highlight the importance of adequately resourcing cybersecurity, and of collaboration and shared operating methods.

4.2 The significant role of businesses in ensuring national cybersecurity

Maintaining and developing the digital infrastructure and its services in Finland are largely the responsibility of the business community. The national sector-specific information exchange networks are dynamic. Business competitors actively share cybersecurity information with one another and with the public sector.

A global trend that divides businesses and sectors can also be noticed in Finland, with an increasingly clear gulf between organisations that have ensured their own cybersecurity and those that have not. This is risky for society as a whole in an interdependent world.

4.3 Wellbeing services counties and municipalities must consider cybersecurity

The most significant recent reform in public administration was the establishment of autonomous wellbeing services counties that began operating at the beginning of 2023. This reform also had a considerable impact on the critical infrastructure and public services of the regions that it affected. Wellbeing services counties oversee their own services and related cybersecurity. The average standard of cybersecurity in municipalities, by contrast, falls short of that realised in national and regional administration, although municipal actors vary in size and resources. Both wellbeing services counties and municipalities need more support to ensure cybersecurity, for example in the form of centralised cybersecurity services. The response to cyber threats must be seamless between actors of varying size, and it must be prompt at all levels of public administration.

4.4 Building trust through cooperation

Finland is a trust-based society in which the public, private and third sectors work closely together. Public authorities combat cyber threats in society, while the cyber professionals of businesses, organisations and civil society work with them in their respective contexts. Public authorities must function reliably, with services ensured for everyone. Members of the public must be treated equitably, with public authorities ensuring that both users and service providers can have confidence in digital technology and services. Challenges for society may arise due to such factors as demographic change. Digitalisation should be accessible and convenient to use, and available to everyone.

Favourable experiences of mutual interaction build trust, and the cyber domain also needs reliable digital procedures for identifying individuals or other parties involved in interactions. Users must know whose service they are using or where information comes from. It is important to be certain about the parties to a communication, and about its factual accuracy and security.

4.5 Rapid development of quantum technology challenges national cryptographic capabilities

National cryptographic technology capabilities combine protecting operating conditions for national security and national defence, ensuring security of supply and knowledge capital, and international cooperation. Some sectors in Finland have solid expertise in creating and applying cryptographic technologies. This profound expertise is nevertheless constrained by the limited overall number of skilled specialists, affecting the development and deployment of these technologies.

Rapid progress in quantum technology poses further challenges to the current national cryptographic capability. Finland has fallen behind its peer countries in developing national cryptographic solutions, with no binding legislation on the use of approved cryptographic technologies. The slow pace of official assessments and approvals of cryptographic technologies and the absence of a national cryptographic technology laboratory may even obstruct the development and use of quantum technology.

4.6 Increased importance of shared situational awareness

Besides political decision-making, the information gathering and influencing efforts of state-sponsored operators in the cyber environment target public authorities, vital functions of society, services and their supporting critical infrastructure, the knowledge capital of businesses and research institutions, and innovations. Hostile state-sponsored operators may also coordinate their operations to pursue their goals more effectively. The key aim of offensive cyberoperations is to disrupt or debilitate the operating capacity of critical infrastructure, such as energy and water supplies or healthcare. A further goal is usually to influence national government and the capacity for political decision-making. One of the most important lessons learned from the Russian invasion of Ukraine, for example, concerns the key importance of applying the capabilities of public authorities and businesses in the cybersecurity sector, and close cooperation between them in defending infrastructure operations against state-sponsored threats.

The competent authorities oversee incident management in accordance with their respective duties and powers whenever cybersecurity is threatened. While cooperation currently functions well, there are indications that the operating conditions of public authorities are currently inadequate to effectively prepare for and combat the most serious cyber threats to national cybersecurity and national defence. Challenges to cybersecurity cooperation arise from the decentralisation of regulation and duties across multiple actors, the diversity of operating models applied in cooperation, and a lack of suitable shared information systems. Cybersecurity data from public services is also insufficiently shared at present with all public administrative and business actors from the perspectives of strategic, normative, resource and information guidance.

An incident that compromises security in a cyber domain can simultaneously be an information security threat, a criminal offence, and a threat to national security and national defence that affects foreign and security policy. This means that investigating such an incident becomes the responsibility of several public authorities. Finnish provisions governing coordination and cooperation between public authorities in the cyber domain are nevertheless still inadequate, with too little consideration given to the special characteristics of the cyber domain when exchanging information and responding to cyber threats.

Public authorities, businesses and organisations currently formulate situational awareness pictures for discharging their functions at varying levels, for differing purposes and with diverse content. Administrative branches also generate their own situational pictures for the needs of government. The National Cyber Security

Centre of the Finnish Transport and Communications Agency Traficom is jointly responsible with various partners for maintaining national cybersecurity situational awareness and analysing the situation. A cybersecurity coordination group works at the strategic level to ensure that ministries and cybersecurity authorities share comprehensive situational awareness regarding the state of cybersecurity in society. The National Cyber Security Director advises the government on matters related to cybersecurity.

5 The pillars and their strategic objectives

TARGET STATE FOR NATIONAL CYBERSECURITY

Cybersecurity is an integral part of Finland's comprehensive security. The functions of our digitalised society are dependable and reliable.

We seize the technological opportunities and understand the associated threats to the cyber domain and society. We develop competence extensively.

Finland detects, identifies, combats and withstands cybersecurity incidents, recovers from them, and responds to incidents decisively.

Finland promotes cybersecurity actively and purposefully through close national and international cooperation.

Sufficient resources are ensured and efficiently applied to realise the target state.

5.1 Pillar I: Competence, technology and RDI

A competent, innovative and inventive cyber ecosystem.

STRATEGIC OBJECTIVES OF THE AREA:

- Cybersecurity competence is strong at all levels of education and training, and of society and work.
- Everyone recognises their responsibility for cybersecurity.
- Finland harnesses the benefits of emerging and disruptive technologies and requires integrated security in devices, software and services.
- Cybersecurity knowledge capital is protected, with Finland pursuing self-sufficiency in critical cryptographic technology.
- Finland ensures the appeal of the RDI environment and promotes the competitiveness of businesses in the cybersecurity sector.
- Opportunities for cooperation and funding through the EU and NATO are fully applied.

An evolving cybersecurity ecosystem

The cybersecurity ecosystem broadly encompasses private and public sector actors, the competence and capacities of various levels of society, cooperation between actors and their operating methods, and a strong Finnish cyber industry and research institutions. The cyber ecosystem seeks to generate vitality and growth, provide more jobs in the cybersecurity sector, create the required expertise, and strengthen the resilience and self-sufficiency of the digital society and its resistance to various cyber domain phenomena. A functioning and inventive cyber ecosystem increases productivity and efficiency and improves the quality of services. A balance between threats and opportunities is sought in partnership with cybersecurity ecosystem actors to enable sustainable economic growth.

Strong domestic research, development and innovation (RDI) and successful commercial operations in the cybersecurity sector are crucial for developing and maintaining a functional cybersecurity ecosystem. This is also required for strengthening the reliability of societal functions and competitiveness.

Strong knowledge and skills at all levels

Overall cybersecurity competence is ensured in Finland by strengthening the role of cybersecurity extensively in education, training and teaching, and at all levels of society and work. The ability of teachers to educate school students in critical media literacy and cyber risk awareness must be improved to reinforce societal crisis resilience. To achieve these goals, cybersecurity must be considered an aspect of digital competence when preparing curricula, with cybersecurity competence fostered in the teaching profession. Civil society organisations play a significant role in developing the competence of individuals in later life. Besides courses leading to degree qualifications in cybersecurity, opportunities for competence development should be enlarged through greater provision of continuous learning. The responsible operations of organisations include developing staff competence, identifying threats, responding to harmful activity, and reporting incidents in the cyber domain.

The availability of skilled staff is vital in ensuring preparedness for cyber threats, evolving safeguards, and business growth in the Finnish cybersecurity sector. Supporting basic research and education in the sector provides a foundation for innovative and socially impactful R&D. The cybersecurity expertise of staff in public administration and associated responsibilities should be enhanced to ensure an adequate level of competence. An innovative cyber domain will be supported through active sharing of information and expertise.

All individuals, businesses and organisations will benefit from a secure operating environment in which predictability improves with greater competence. This will also improve the appeal of Finland as both an investment target and competence cluster.

Everyone recognises their responsibility for cybersecurity

Cybersecurity competence is a basic civic skill, and every member of the public should be able to assist in realising a more secure cyber domain. Ways of encouraging a cyber safe daily life include strengthening media literacy and increasing awareness of good cybersecurity hygiene, meaning that good routine information security practices should be considered an inherent aspect of individual social responsibility. The security of communities and organisations also increases considerably when people act responsibly in the cyber domain.

Society must prepare for the emergence of new and disruptive technologies

Finland is seeking to be a leader in boldly implementing emerging and disruptive technologies in support of ensuring cybersecurity. Large-scale application of the technologies to be implemented requires such technologies and software to be designed for security from the outset and regularly serviced for security throughout their life cycle. This principle of integrated security should be considered when drafting all national technology statutes and when lobbying the EU.

Standardisation and certification are aspects of new EU cybersecurity legislation. It is in Finland's interest to participate actively in developing and deploying cybersecurity standards and certification systems. It is also important to seize the business opportunities afforded by this field.

Emerging and disruptive technologies, such as artificial intelligence and quantum technology, and new mobile network generations will introduce new cybersecurity threats that have yet to become wholly evident. The combined impacts of these technologies are also extremely hard to forecast. Addressing these challenges will call for in-depth and diverse technological competence, coupled with continual monitoring and assessment of changes taking place in society. For example, preparations should now be made for the impacts of developing quantum technology.

Promoting business competitiveness in the cybersecurity sector

International cooperation and funding opportunities available from the EU and NATO are applied when planning RDI investments in cybersecurity, with special attention paid to the processes, resources and proactive cooperation that these opportunities require. Participating in international funding programmes (such as the NATO innovation initiative DIANA, the EU Horizon Europe and Digital Europe (DEP) framework programmes, or the European Defence Fund programmes) improves the profile of Finland as a specialist in high technology and cybersecurity, improving national and international commercial opportunities for Finnish businesses. It is important for Finland to actively influence the content of these programmes at their planning stage. Cooperation and funding opportunities provided by the European Space Agency (ESA) may also be taken to accommodate cybersecurity in the rapid development of space technology.

The objective is for Finland to be capable of delivering globally competitive, growth-driving technological solutions for the cybersecurity sector. The Finnish RDI environment should encourage and support the development and application of solutions that strengthen cybersecurity, and the international competitiveness of

businesses that commercialise such solutions. This will also increase the appeal of Finland's cybersecurity sector, and of its secure RDI and business environment more generally, to Finnish and international specialists, businesses and investors.

Cybersecurity knowledge capital is protected

The critical knowledge capital of the public and private sectors must be identified and protected. Knowledge capital in cybersecurity includes services, information systems, expertise, processes, patents, trademarks and partnerships. Active information exchange and informed decision-making by various actors is an effective way to decide the cybersecurity development measures that are required to protect knowledge capital and ensure that society functions.

Aiming for self-sufficiency in cryptographic technology

The confidentiality, integrity and availability of nationally important data repositories under all circumstances is an important aspect of cyber resilience. Progress in quantum technology threatens to break modern encryption algorithms and endanger datasets that should be protected nationally. One of Finland's strategic objectives is to be self-sufficient in critical cryptographic technologies and prepared for the quantum threat by the beginning of 2030. This requires the development of quantum-proof cryptography solutions and other nationally critical cryptographic technologies in Finland, coupled with reinforcement of comprehensive cryptographic technology capabilities in such fields as manufacturing, research, computing, reverse engineering and organisation. National work to develop quantum-proof cryptography will also accommodate common EU policy measures and regulations, and requirements imposed by NATO.

5.2 Pillar II: Preparedness

Strong societal cyber resilience and operational reliability

STRATEGIC OBJECTIVES OF THE AREA:

- Vital functions of society, critical infrastructure, public services and actors that are critical for security of supply are cyber resilient.
- Individuals, businesses, organisations and public authorities have jointly prepared for cyber incidents and threats.
- Finland promotes its cybersecurity preparedness model as an export product.
- Cybercrime is prevented.
- Preparedness is based on comprehensive shared situational awareness and long-term resourcing.
- Environments and practices are developed for cybersecurity exercises, with more exercises conducted between various sectors.

We can trust the functioning of society

Finland takes a proactive approach to cyber threats. People must have confidence that society will function under all circumstances. Adequate and timely preparation for cyber incidents is the cornerstone of operational reliability in a digital society. A proactive approach and long-term preparation promote the availability and incident resistance of societal services in all circumstances. Ensuring the functionality and incident resistance of vital functions is crucial. Vital functions include infrastructure that is critical for the cyber domain, data repositories, public services and security of supply. The goal of work done to ensure security of supply as part of preparedness is to protect the functioning of critical infrastructure, manufacturing and services, so that they can also satisfy the necessary basic needs of the population, the economy and national defence under all circumstances in the cyber domain.

Public administration must consider the evolving operating environment when imposing preparedness requirements on businesses from the perspective of security, and when supporting the preparedness of businesses. Developing and extending cyber exercise operations is an important aspect of ensuring

functionality and improving incident resistance, particularly when considering cybersecurity and various service and supply chain interdependencies. Secure information systems are a foundation for societal cyber resilience. Attention must be paid to procuring, developing and maintaining such systems in both the public and private sectors.

Public services are secure

It is important for public services to be secure in use, and for individuals and organisations to have confidence in their operational reliability. The cybersecurity of public services is managed proactively based on knowledge of circumstances and on threat and risk assessments. Comprehensive and reliable situational awareness is needed concerning the standards and shortcomings of cybersecurity in public services in order to manage risks and reinforce cybersecurity. The impact, benefits and costs of cybersecurity are monitored with focus areas prioritised. Technologies and service provision must comply with cybersecurity, information security and data protection requirements throughout their life cycle. The assessment and approval of compliance in public services and the associated evaluation criteria must be developed, streamlined, and made mandatory where necessary. It is also important to develop and require automatic monitoring and supervision of the technical environment. Prioritisation of service functionality according to circumstances must be ensured, with preparations made for potential incidents, and for minimising their impact on the operations of public authorities and society.

Preparedness is a joint endeavour

Cybersecurity preparedness is implemented in close partnership according to the model of comprehensive security. Identifying cyber threats and preparing for them must be based on systematic management by information, and on shared situational awareness derived from anticipation, observation, intelligence collection and the application of research findings. Intelligence supports preparedness and anticipation in order to safeguard national security by collecting and sharing intelligence information on the abilities of hostile cyber operators, and on the goals and targets of cyberattacks.

Finland also pursues a preparedness operating model that emphasises collaboration and dialogue within the EU and NATO, promoting application of the cybersecurity preparedness model and best practice in partner countries. Mutual trust between various stakeholders in society and trust in public institutions and

their services help to build strong national resilience. Trust is required for successful national cybersecurity work, preparedness, shared situational awareness and timely responses.

Preventing cybercrime

Preventing cybercrime requires determined and active measures from all stakeholders in society, with the focus on early prevention and identifying threats. Services provided to the public must accordingly be planned, implemented and maintained in ways that minimise potential avenues of attack for cybercriminals.

Users must have confidence in the security of services, and sufficient expertise to recognise bogus services and fraud. The development of artificial intelligence is making cybercrime more targeted and impactful, and it will accordingly become increasingly important to recognise the impacts of artificial intelligence and other disruptive technologies on cybersecurity, and to develop ways of responding to them.

Cybercrime-related threats must be communicated in an intelligible way, with instructions and guidance provided on correct procedures. Prompt official reporting of offences that target individuals and businesses enables prevention of similar offences and more extensive damage. Cybercrime prevention must be supported through legislation to enable information sharing between public authorities, regional and local administration, wellbeing services counties and businesses.

Preparedness based on long-term resourcing

The action plans and financial plans of public administration, businesses and organisations include cybersecurity resourcing to meet needs specified in a comprehensive threat and risk assessment and in statutory obligations. Effective use of cybersecurity resourcing requires cybersecurity functions to be planned and implemented efficiently in comprehensive national and international cooperation between central and regional administration, wellbeing services counties and municipalities, and businesses and organisations.

Shared strategic-level resources for managing cybersecurity in central government are allocated to the Office of the National Cybersecurity Director. Resource allocation to other public authorities discharging centralised cybersecurity functions depends on the duties assigned to those authorities. Centralisation

of cybersecurity functions must also be appropriately promoted in regional administration, wellbeing services counties and municipalities for optimal use of resources.

Centralised project funding from the General Government Fiscal Plan may be allocated to launch new cybersecurity operations, functions or services. The feasibility of providing a new official cybersecurity service to clients for a fee must always be examined when a public authority implements such a service.

It is important to actively monitor and improve the productivity and impact of a cybersecurity operation, both at the level of society and in each organisation. Use of funding is planned, monitored and supervised through a common resourcing scenario as part of general government fiscal planning. The operating models required for formulating and maintaining this scenario must be implemented.

Developing exercise activities

Cyber exercises provide a foundation for strong cyber resilience in society as a whole. Cybersecurity exercise environments and operating models must be continually developed to respond to evolving operating environment. Organisations are encouraged to develop their own long-term exercise activities with the support of public authorities where required.

The importance of arranging and increasing exercises that transcend sectoral boundaries is particularly acknowledged nationally. National cybersecurity exercises simulate various cyber incident scenarios, creating conditions in which the impacts of cyber incidents can be identified and recovery from them can be tested and practised. These exercises enhance competence and the ability and capacity of individuals and organisations to prepare for various cybersecurity incidents and threats. Active and regular exercises under normal conditions reinforce competence in all situations.

International cyber exercises support preparations for and responses to cross-border cyber threats, and associated decision-making. It is important for Finland to participate in international cyber exercises, to contribute to them actively, and to develop and provide cyber exercise competence to partner countries.

Improving the resilience of terrestrial systems with space services

The availability of space services such as time and geospatial data, telecommunications and remote sensing is important for the functioning of society. The cybersecurity of space systems is monitored as part of maintaining space-related situational awareness, and should also be considered in the conditions for authorising space activities and in life cycle management of systems. Alternative operating models and backup arrangements may be used to prepare for potential incidents and recovery from them, and to minimise the impact of incidents on the operations of public authorities and societal functions.

5.3 Pillar III: Cooperation

A solid national and international cooperation model

STRATEGIC OBJECTIVES OF THE AREA:

- Finland actively influences and participates in normative international cooperation concerning the cyber domain, such as cyber diplomacy and the development of regulations.
- Finland actively participates in, and proactively influences cooperation on cybersecurity, cybercrime prevention and cyber defence, and supports its partner countries.
- Cybersecurity opportunities provided by the EU and NATO are ensured.
- The public and private sectors develop a model of closer cooperation that reinforces trust.
- Information required for cooperation between public authorities is shared seamlessly.
- The public sector develops and provides centralised cybersecurity services in partnership with the private sector.

Finland actively influences and participates in cooperation

The Government Report on Foreign and Security Policy, the Government Defence Report, the Government Report on Internal Security, and the Cyber Security Strategy impose national long-term objectives for responding to cyber threats. They also accommodate EU and NATO cybersecurity and cyber defence objectives and obligations. These objectives are specified through the national cyber policy. Monitoring of the implementation and effectiveness of the objectives assigned for cyber diplomacy, cybersecurity and cyber defence is harmonised through comprehensive cooperation at the strategic level.

Finland continues its intensive participation in normative international cooperation concerning the cyber domain, and in exchanging views on how international law on certain issues regulates the use of information and communication technologies by states. Finland is updating its position on the application of international law in the cyber domain and influencing political decision-making on cybersecurity,

cybercrime and cyber defence at the UN, the EU, NATO and other key international organisations and networks. Finland is also a reliable partner in Euro-Atlantic cooperation, a provider of security, and a responsible state actor with respect to the cyber environment. Cybersecurity cooperation is extensive, and particularly profound with key like-minded EU Member States, the Nordic and Euro-Atlantic countries, and certain countries in the Indo-Pacific region on the basis of shared values.

Finland promotes multilateral cyber diplomacy with a view to creating and maintaining an open, free, secure and stable cyber environment. The EU Cyber Diplomacy Toolbox provides instruments for responding to and preventing cyber threats. Finland shields itself against potential cyber threats originating in third countries through cyber defence, cybersecurity and cyber diplomacy. The methods of cyber diplomacy include reinforcing the multilateral system on the basis of international law, partnerships, dialogue and trust-building measures. The common cyber policy and regulations of the EU concerning cybersecurity also provide a framework for Finnish cybersecurity legislation. Attention must be paid to assessing the impact and implementation of new regulations, and to allocating sufficient resources to public authorities.

Finland as a member of the EU and NATO

The European Union is Finland's most important political and economic frame of reference and community of values. Finland participates in and actively influences EU cybersecurity work, including the work of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Competence Centre and Network. By exerting influence in the EU, Finland promotes projects and decisions that are important for comprehensive security, and which enhance the preparedness of the EU and its Member States, including the field of cybersecurity.

Finland actively influences the development of EU cybersecurity policy and regulation, promoting its own national model based on comprehensive security and proactive preparedness in the EU and other Member States. Strengthening and establishing the new cybersecurity functions and bodies set up at the EU in recent years is an important way to reinforce EU cybersecurity and national situational awareness. The objective is to help develop a shared EU commitment and thereby fortify incident resistance in the cyber environment. One key outcome is the achievement of EU strategic autonomy and the preservation of an open economy.

Finland is a constructive, reliable and capable NATO ally, maintaining a strong national defence capability as part of shared NATO deterrence and defence, and actively participating in the development of NATO cyber defence. As a NATO member, Finland seeks to work at the core of cyber capability building with a view to becoming an important provider of cybersecurity and cyber defence solutions within the alliance.

As a member of the military alliance, Finland will continue to promote the development of NATO cyber defence and apply alliance capabilities. This is supported by systematic development and maintenance of cyber defence as part of national cybersecurity. Finnish infrastructure will be developed as part of alliance infrastructure, boosting cooperation and cyber defence. Most of the seven baseline requirements of resilience defined by NATO also impose requirements for developing national cybersecurity.

It is important to harmonise national EU and NATO views on cybersecurity and cyber defence. Mutual compatibility of EU and NATO cyber operations complements and reinforces both international cybersecurity and Finnish national cybersecurity.

Shared situational awareness based on information exchange as a basis for measures

Close cooperation, establishing shared situational awareness, and ensuring conditions for acquiring information are crucial for realising the target state. Shared situational awareness based on information exchange enables public authorities, businesses and organisations to cooperate effectively and reliably in the cyber domain. This increases trust and supports the realisation of sectoral responsibilities.

Information gathering should be systematised with respect to the cyber domain in order to form a more comprehensive understanding of serious cyber threats against Finland. Specifying and legislating the conditions and parties involved is a requirement for expanded information exchange, as is reassessing the grounds for current restrictions. Information exchange must also be enhanced by harmonising and specifying current statutory interpretations and modifying shared operating models.

Information exchange must be adequate, trust-building, balanced, conformed to purpose, and based on the right to disclose and receive information and on an interest in sharing and an authorisation to share information between parties that need it. Situational understanding should enable producers or custodians

of information to identify and share it on their own initiative. It must be possible to share information on serious cyber threats more effectively with businesses critical for security of supply, municipalities, the service providers that they own, and wellbeing services counties within the constraints of restrictions on sharing. Better methods and conditions for collecting, analysing and sharing information on the level of cybersecurity and cyber resilience are needed with respect to public services.

Sharing highly classified information requires the development and deployment of suitable systems. The 2023 report on the authorities' capacity to act in cyber security matters should be considered when developing information exchange between public authorities.

Smooth cooperation between public authorities

Implementation and responsibilities in operational cooperation, and preparedness for and responses to serious cyber threats and incidents, will be coordinated in a closer and more inclusive agency-level cooperation structure comprising the Finnish Transport and Communications Agency Traficom, the National Bureau of Investigation, the Defence Forces and the Finnish Security and Intelligence Service. Coordination will be based on shared situational awareness. The cooperation structure and associated public authorities must be adequately authorised to disclose and receive information. The cooperation structure will also bring a need for closer tactical and technical collaboration between public authorities.

The operating culture of cybersecurity should be reformed in line with the model of comprehensive security by boosting international and national cybersecurity cooperation between central and regional administration, wellbeing services counties, municipalities, local administration and organisations. Use of the operating models of international partners and of technologies that provide cybersecurity solutions would be enlarged to achieve this. It is important for wellbeing services counties, as new actors, to promote a cybersecurity culture and cybersecurity competence in partnership with other actors.

Centralised cybersecurity services

Centralised cybersecurity services are currently provided by the Finnish Transport and Communications Agency Traficom, the Digital and Population Data Services Agency, other central government parties, and businesses owned by wellbeing services counties and municipalities, working together with the private sector. Such services include the HAVARO serious information security threat detection

and HYÖKY attack surface mapping services provided by Traficom, and online information security and cybersecurity training provided by the Digital and Population Data Services Agency. These centralised services are used by national, regional and local administration, wellbeing services counties and municipalities, and businesses, organisations, institutes of higher education and research institutions as applicable.

Coordinated development and use of centralised cybersecurity services will be promoted. These services must be reliable, cost-effective, efficient and user-friendly. Cooperation will seek to avoid reduplication, and to provide common materials and training, information and services.

5.4 Pillar IV: Response and countermeasures

Timely responses to cyber threats and assured sovereignty

STRATEGIC OBJECTIVES OF THE AREA:

- Actors in public and private sector have clear roles and powers, and the ability to respond to cyber incidents in a timely and appropriate manner.
- Responses and countermeasures are based on comprehensive situational awareness.
- Organised and serious cybercrime is combatted.
- A cyber defence doctrine provides national operating principles for responding to state-sponsored threats, and to threats against national security.

Ensuring opportunities and capacities to respond to cyber threats

Breaching the sovereignty of a state is a violation of international law. This also applies to cyberspace. Finland holds that international law and the norms of responsible state behaviour establish the essential framework for the operations of states in the cyber environment.

The response to cyber threats must be comprehensive, long-term and timely. This requires extensive and determined application of measures that strengthen cybersecurity and prevent cyber threats. Finland responds to the challenges of the geopolitical situation for the cyber environment through active cyber diplomacy, cyber defence and cybersecurity measures, both independently and as part of multilateral activities. Finland must also ensure national sovereignty in the cyber domain.

The opportunities and capacity of societal actors to respond to cyber threats must be assured in all circumstances. For society to be able to function without incidents, organisations must be capable of swiftly recovering from cyber incidents and attacks, and restoring their systems promptly and securely.

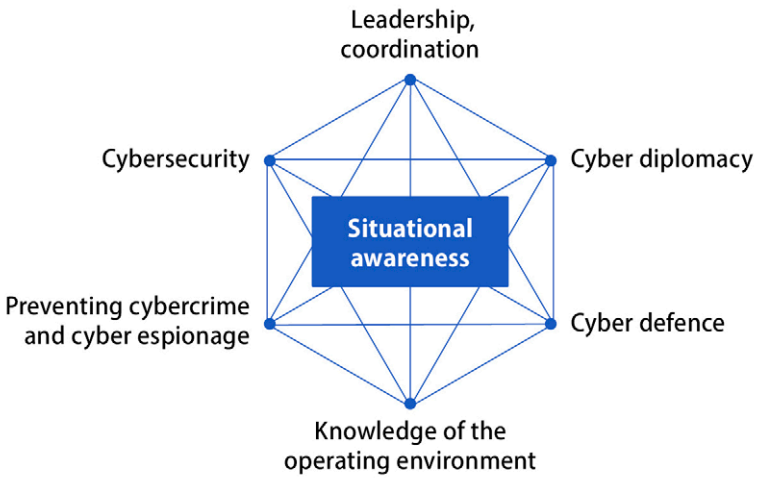
Operative authorities are required to prevent, respond to and investigate cyber threats, and to generate situational awareness concerning them. The nature of cyber threats imposes requirements on cooperation between authorities. The responses to, and measures taken against state-sponsored cyber operations differ from those that are applied against regular cyber threats. Responding to state-sponsored hostile cyber operations by imputing criminal liability to the perpetrator is not necessarily the most effective method. Threat responses combine various methods and measures in the cyber domain as a whole and at varying levels of operation, and assessing perspectives of international law. The threats of a continually evolving cyber domain require comprehensive specification of the roles and responsibilities of various actors in order to respond to cyberattacks.

The ability to apply a comprehensive and broad range of methods is particularly highlighted in responding to state-sponsored operations and serious cybercrime. Specifying roles and responsibilities solely in terms of technical and operational protection of operations and infrastructure does not suffice in a new operating and threat environment. It must also be possible to respond to hostile operations across the operating environment as a whole. Besides applying regular measures to ensure resilience and information security, the target-oriented approach must be supplemented to incorporate more extensive and comprehensive measures. It no longer suffices to protect information systems through information security alone, for example, and new methods, such as international information exchange, sanctions or active cyber defence, are instead required.

Developing a coordination model for cyber incidents and threat situations

Operative authorities will formulate a jointly analysed situational awareness picture to support timely responses and countermeasures. This supports a common understanding of circumstances enabling the planning, preparation and deployment of measures. The coordination model for responses and countermeasures will be formulated within the agency-level cooperation structure described above in Pillar III. Shared situational awareness ensures coordinated measures for the in-house operations of each authority. National cybersecurity and the necessary information gathering, access to information and information exchange by authorities will focus on preventing and combatting serious cyber threats and cybercrime that targets the vital functions of society, national security, national defence and security of supply at all levels of government.

Figure 2. Shared situational awareness as a basis for coordinated measures.



Combatting organised and serious cybercrime

Cybercrime will be combatted by detecting, preventing and investigating suspected offences, and by applying effective criminal intelligence based on management by information. The authorities will seek in particular to combat organised and serious cybercrime, to incapacitate the perpetrators, and to ensure that organised criminal groups or other operators posing a danger to society do not expand their operations into the structures of society, the economy or political decision-making.

The operating conditions for judicial and law enforcement authorities, for national and cross-border cooperation, and for the required information exchange will be enhanced in response to an evolving security environment. Cross-border combatting of cybercrime relies on common international investigation groups. The information gathered through crime prevention and its methodological range should also be applied more effectively in support of cyber defence, attribution and countermeasures.

Developing national attribution operations

Finland develops national guidelines and a process for goal-oriented and consistent cyber attribution that accommodates the needs of key allies and partners. Attribution means collecting and analysing facts, conducting a technical, judicial and political assessment, making decisions and, ultimately, communicating such decisions to various parties. A comprehensive attribution process must be capable of using all information related to attribution that is procured by intelligence, cybersecurity, investigative and other public authorities in the course of their statutory duties. The ability of Finland to combat state-sponsored cybersecurity operations targeting Finland or her interests will be secured by ensuring that the intelligence and security authorities have fully updated powers and conditions for discharging their functions.

Specifying the functions and role of cyber defence

A cyber defence doctrine specifying the aims of cyber defence is drawn up to support cyber defence implementation. The doctrine describes how cyber defence is effected by applying national capabilities and those of the alliance and partners. Cyber defence is developed in a balanced manner in parallel with the development of national cyber resilience, cybersecurity and cybercrime prevention. The role of national and military cyber defence in peacetime, crises and conflict is specified to the level required by the security environment. National cyber defence is developed as part of the development and implementation of comprehensive national defence.

Finland reviews its position and approach to hostile operations occurring in the cyber domain, preparing nationally for active cyber defence and the possibility of attribution to an opponent and countermeasures. Cyber defence operations are harmonised with foreign and security policy operations and actors.

The goal is for Finland to respond to cyber threats caused by third countries through both preventative, reactive and long-term measures, and to apply the entire palette of national methods and performance appropriately. These include the methods of diplomacy, intelligence, information management and strategic communication, military capability, crime prevention and the financial sector, and economic, judicial and other cybersecurity methods. A state can be held liable for any cyber operation that violates international obligations if its own organs (or private groups or individuals acting on its behalf) can be identified as perpetrators.

It is in Finland's interests to work closely with international actors multilaterally, regionally and bilaterally. This applies to technical, operational and strategic cooperation, the development of international norms and standards, and political dialogue, and to attribution capability and the ability to take countermeasures. Finland also fully participates in the operations of NATO cyber defence and avails itself of opportunities provided by the EU with regard to capability cooperation, information exchange, coordinated countermeasures and regulation to support national cyber defence. Cyber defence is part of Finnish and NATO deterrence and defence.

6 Resource allocation, implementation and monitoring

6.1 Resource allocation

Cybersecurity actors combat threats in Finland on a daily basis. The evolving operating environment increases and diversifies cyber threats and risks. Current resource allocation for cybersecurity has been inadequate in relation even to the need to maintain the current state. New resource allocation will be needed to ensure and strengthen future cybersecurity in an evolving operating environment with the implementation of new legislation and supervisory functions in various sectors.

Finland currently spends nearly EUR 300 million on ensuring cybersecurity in central government. Regional administration, wellbeing services counties, municipalities and local administration also use resources for their own cybersecurity, and there is a need for more effective monitoring of such resources. It should be noted that a significant share of Finnish critical infrastructure is owned by businesses that are responsible for ensuring its cybersecurity. A conservative estimate suggests that businesses invest at least ten times more in cybersecurity than the funds allocated by central government for this purpose. The resources that businesses devote to cybersecurity are also increasingly important from the perspective of security of supply. Indirect investments are also made in cybersecurity. For example, investments in cyber competence are made at all educational levels, and in various research projects in Finland. The reinforcement of cybersecurity provided by funds invested in cybersecurity education and research often takes time to manifest.

Current difficulties in central government finances, the technology maintenance backlog, the labour shortage caused by a skills shortfall in the cybersecurity sector and growing EU regulation will affect the prospects for developing cybersecurity. The relative competitiveness of the public sector as an employer is declining compared to the private sector. These factors pose challenges to implementing the Finnish cybersecurity strategy and the plan for doing so, and for national growth in the cybersecurity sector.

More resources must be allocated to implementing all strategic objectives and development measures. A change in the cyber profile of Finland will not only require increased resources, but also more focused planning and monitoring and more efficient use of resources.

Building a functioning and vital cybersecurity ecosystem means making considerable financial investments at the level of society as a whole. A functioning ecosystem generates vitality and growth, increases jobs in the sector, fosters the required competence, and improves the resilience and resistance of a digital society against harmful phenomena in the cyber domain.

More extensive and profound application of the model of comprehensive security in ensuring cybersecurity, and the associated preparedness, responses and countermeasures, are necessary measures that help to avoid the costs of serious cyber incidents. The model of comprehensive security applies existing resources more efficiently and increases general resilience, as competence, operating models and best practices can be shared between organisations at varying levels of preparedness.

High-standard R&D in emerging and disruptive technologies and investments in national cybersecurity are key instruments for preserving a society that is cyber safe and resistant to cybersecurity crises. Supporting RDI is also important for increasing national competitiveness. Competence is required at all levels, with resources required in such areas as the education and advice provided by organisations to a substantial segment of the public, and the cyber exercises arranged by various actors.

Use of NATO innovation funding and EU development funding are essential aspects of developing the Finnish cyber ecosystem. This will require co-financing by Finland and resource coordination between administrative branches. NATO membership also requires additional investment in cybersecurity and cyber defence, and in developing infrastructural cyber resilience. It will call for new kinds of capability and resourcing from Finland in support of allies.

One key aspect of determining national resources is estimating the alternative costs, or the costs that could be incurred if strategic development measures prove ineffective. Besides the staffing and ICT costs arising from cyberattacks, these expenses include the consequences of data leaks, cybercrime or reputational damage.

Resources may be applied more efficiently through agile cooperative sharing of competence and resources between public authorities, for example by enabling public authorities to agree on the discharge of cybersecurity functions on behalf of another authority where this is deemed appropriate.

Decisions on resources and their allocation and coordination are made through the decision-making processes of the state budget, with resources allocated within a framework of appropriations and person-years according to general government fiscal plans and budgets.

6.2 Strategy implementation and monitoring

The EU cybersecurity directive (NIS2) and its national implementation require reassessment of the need to update the national cybersecurity strategy at five-yearly intervals. The strategy will be developed and updated more frequently as required. Updates will be made in collaboration with public authorities, businesses, research institutions, associations and individual members of the public.

Implementation of the strategy will be monitored nationally on an annual basis. Responsibility for coordinating monitoring is vested in the Office of the National Cyber Security Director, for which administrative branches produce cybersecurity implementation reports within their respective purviews according to the schedule of the general government fiscal planning process. The Office then prepares a digest of these reports for public authorities and political decision-makers.

After the cybersecurity strategy revision has been completed, the working group appointed to revise the strategy will continue its work as a strategy implementation monitoring group. This monitoring group will prepare a strategy implementation plan within six months of completing the strategy. The implementation plan will specify the implementation responsibilities and schedule for each administrative branch and detail the metrics used annually for monitoring and assessing implementation. The implementation plan will be approved by a steering group comprising the state secretaries of the government security management operating model development project. Strategy monitoring will be reported to this steering group and to the ministerial working group on reforming society. The ministerial working group on internal security and administration of justice and the Security Committee will also be informed of progress concerning the implementation plan.

The basis for determining performance indicators for cybersecurity will include cyber surveys conducted by the EU cybersecurity agency ENISA, the OECD and NATO, the annual digital security survey of the Digital and Population Data Services Agency (public administration), the cyber maturity survey of sectors conducted by the National Emergency Supply Agency (business community), and the digital security barometer formulated by the Digital and Population Data Services Agency (cyber resilience of citizens), as appropriate.

The goal is to expand cyber resilience indicators to include preventative cyber preparedness efforts. Finland will seek assistance from ENISA where necessary when determining key performance indicators, as provided in the NIS2 directive. The international success of Finland will be monitored by reference to international indices (ITU: Global Cybersecurity Index [GCI] and e-Governance Academy: National Cybersecurity Index [NCSI]).

Implementation of the strategy will stress the identification of best practices, with extensive application of practices based on lessons learned from incidents. This will promote the establishment and maintenance of consistent practices and support the resilience of society as a whole. The purpose of assessing the implementation is to support political decision-making, the operations of public authorities, and public debate.

7 Strategic development proposals

A scheduled implementation plan with assigned responsibilities should be prepared based on the strategy. Its implementation will seek to realise the strategic objectives of the pillars. The key development proposals identified in the strategy work are listed below, and will be specified and supplemented in the implementation plan as required. One essential aspect of each development measure is an assessment of statutory provisions and norms, potentially leading to the repeal or specification of provisions. The division into pillars set out below is indicative, as many development measures fall under more than one pillar.

7.1 PILLAR I: Competence, technology and RDI

- Developing public and private sector competence and workplace skills, together with cybersecurity resilience and the preparedness of individual members of the public and civil society.
- Preparing for threats and opportunities arising from the emergence of new disruptive technologies, and accommodating them in forecasting work and in implementing and using technologies.
- Promoting development of the cybersecurity ecosystem and technological sovereignty by strengthening RDI and business operations in the Finnish cybersecurity sector. Benefiting from national and international cooperation and funding opportunities.
- Considering the prospects for civil society organisations to communicate matters of cybersecurity to the general public and provide related guidance.

7.2 PILLAR II: Preparedness

- Deepening the common preparedness of cybersecurity actors as part of the model of comprehensive security.
- Assessing cybersecurity perspectives in all legislative projects.

- Planning and monitoring the cybersecurity resources of public administration in the long term.
- Applying cybersecurity and information security standards to develop common operating methods and resilience in the cyber domain, and actively influencing international standardisation.
- Developing assessment and approval methods related to the operations and information systems of organisations, and related requirements.
- Developing exercise operations and environments to increase preparedness and competence.

7.3 PILLAR III: Cooperation

- Clarifying the international status of Finland in cybersecurity and cyber defence, developing participation in international cybersecurity cooperation, and establishing the required national coordination.
- Strengthening mutual cooperation and common situational awareness of security authorities by establishing the required cooperation structures and coordination models, clarifying roles and responsibilities, and ensuring conditions for information exchange and access to information. The development measures proposed in the 2023 report on the authorities' capacity to act in cyber security matters will be implemented in this respect.
- Strengthening cooperation between the public sector, the private sector and civil society, their information exchange, and common situational awareness in cybersecurity in accordance with the operating model of comprehensive security.
- Maintaining and improving trust through secure and reliable public services.

7.4 PILLAR IV: Response and countermeasures

- Developing the ability of wellbeing services counties, municipalities and the private sector to prepare for and promptly respond to cyber incidents.

- Improving awareness of the operating environment by such measures as ensuring the national observation capacity and the opportunities of security and intelligence authorities to collect information on the cyber domain.
- Promoting the comprehensive prevention of cybercrime.
- Developing cyber defence as part of comprehensive national defence, measures to secure Finnish sovereignty in the cyber domain, and integration into the defence of the alliance.

8 Concepts and definitions

The terms and definitions set out below describe concepts used in this document. These terms have been used in order to explain the strategy more concisely and avoid repetition, and the definitions are provided to help the reader understand the intended context. The recognised need to update terminology related to concepts designated by cybersecurity terms used in this strategy has caused some divergence from the accounts that are already available in existing glossaries, such as the TEPA Term Bank or the Vocabulary of Cyber Security. This divergence arises in particular from the need for concepts that are internationally harmonised, and the need to include concepts that are now used in EU regulation.

Attribution

Detecting and locating a party conducting a hostile cyber operation, and identifying that party, through an analytical process using various information sources. Nationally this process involves both technical analysis and the duties of public authorities, and discretion related to foreign and security policy. Attribution is the outcome of the analysis process, regardless of whether that outcome is public or non-public. Attribution is often a condition for holding a party legally or politically liable, for measures in accordance with international obligations (retorsion), and for permitted countermeasures. Attribution, such as public attribution, may also serve as a method of retorsion in itself.

Critical infrastructure, critical infrastructure of society

An asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, or an important service, which is essential for maintaining the vital functions of society or for providing some other key service.

Cyber domain

The cyber domain comprises one or more information systems intended for processing digital data or information, their physical and logical structure, and the actors of an operating environment with their natural and digital identities. The cyber domain stresses the use of cyberspace from the perspective of goal-oriented activities.

Cyber ecosystem, cybersecurity ecosystem

A network of interdependencies established and maintained between businesses, research, public administration and the third sector, described in the 2021 Cyber Security Development Programme. The objective of the network is to generate innovations, vitality, growth, jobs and competence, and to improve the sustainability and resilience of the digital society against harmful phenomena in the cyber domain.

Cyber environment, cyberspace

The cyber environment refers to a global space created and managed by people, which is based on information technology and use of the electromagnetic spectrum to create, modify, change and use information through both interconnected and separate networks that apply information technology.

Cyber hygiene

A security-oriented mindset, or a sophisticated security culture in an organisation, combined with the regular daily routines, practices and processes that help to enable a community and an individual to develop and maintain cybersecurity when using information systems, computers or other devices.

Cyber resilience

The ability of a state, organisation, community or individuals to maintain their functional capacity in the evolving conditions of the cyber domain, and the preparedness to face incidents and threats, to recover from them, and to respond to them as necessary.

Cybersecurity

The measures for protecting communication and data systems and other electronic systems, the data to be stored, processed or transferred therein, and their users, appliers and other relevant persons from cyber threats.

Cyber threat

A potential situation, event or activity that may harm or disrupt communication networks and information systems, users of such systems and other people, or that may otherwise harmfully affect them.

Infrastructure critical for defence capability

The structures, services and related functions of the defence system and critical infrastructure, and the vital functions of society that are essential to the operating conditions of national defence in all states of preparedness.

Military cyber defence

The measures taken to protect the systems and the stakeholders in various sectors that affect Finland's defence capability, particularly against state-sponsored hostile operators and their agents, in order to ensure defence capability, and to safeguard the sovereignty of Finland and implement military cyber operations.

National cyber defence

The national and international military and civilian measures that secure the sovereignty of Finland and the living conditions of its population against external state-sponsored cyber threats and incidents, and the required countermeasures taken in all states of preparedness.

National cybersecurity

The measures that enable a digital society to prepare for, identify, combat and withstand incidents in electronic and networked systems, and the impacts of these incidents on vital functions and services of society, to recover from them, and to assist in ensuring the operating conditions of national security, national defence and security of supply.

Resilience; crisis resilience; crisis tolerance

The ability of a state, organisation, community or individuals to maintain their functional capacity in evolving circumstances, and preparedness to face incidents and crises, and to recover from them.

Vital function of society

A function that is essential for the functioning of society.

Appendices

Appendix 1: National cooperation model for cybersecurity

This appendix describes the current state and actors of the national cooperation model for cybersecurity, and provides a national perspective on the requirements of the cybersecurity directive (NIS2).

The Finnish national cooperation model for cybersecurity (hereinafter referred to as the cybersecurity cooperation model) is decentralised. It corresponds in principle to the cooperation model for comprehensive security (hereinafter referred to as the model for comprehensive security). Cooperation is based on statutory duties, cooperation agreements, and the Security Strategy for Society, which accommodates cybersecurity in each strategic task. The cybersecurity cooperation model is scalable to all levels of society, meaning that it can be applied from the national level to regional and local levels, or to wellbeing services, counties and municipalities, while taking international partners into consideration.

The model of comprehensive security guarantees the vital functions of society through cooperation between the public sector, business community, civil society and citizens under all circumstances and at all levels. Ongoing development of the cybersecurity cooperation model will conform to the model of comprehensive security while accommodating the special characteristics of cybersecurity.

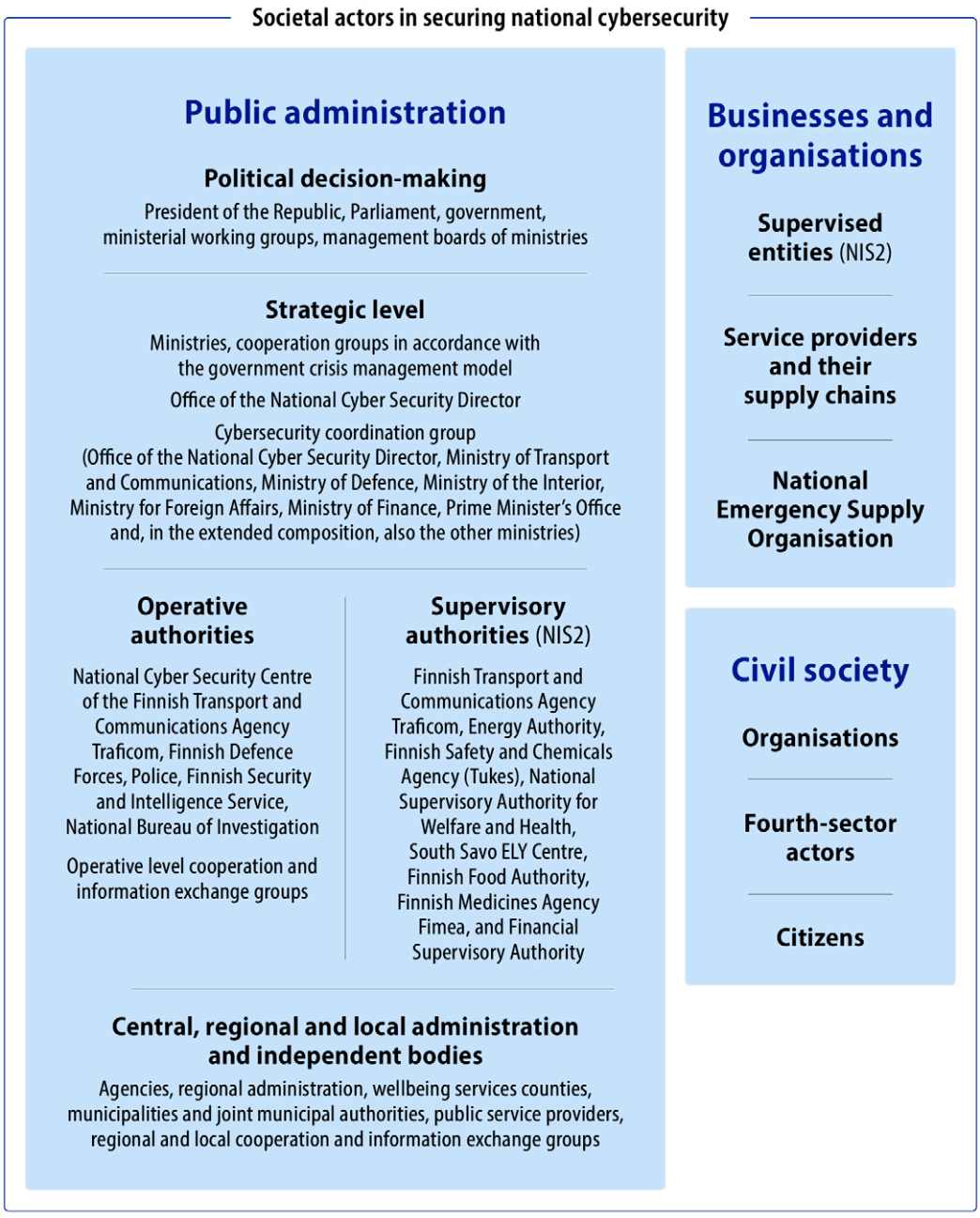
The competent authorities will direct incident management in accordance with their respective duties and powers under the cybersecurity cooperation model, and in a cyber crisis referred to in the cybersecurity directive. The societal crisis management model will determine these authorities, and the harmonisation of, and support for operations where necessary. Each operator will be responsible for its own preparedness, and as required under the Emergency Powers Act and sectoral legislation to ensure that critical services function under all circumstances, for example by imposing requirements on service providers and by supervising their implementation. The public sector, business community and civil society will collaborate closely in preparing for, and responding to cyber incidents. The centralised cybersecurity services that are jointly provided by the public sector and businesses will support organisations and citizens in preparedness and incidents. This will harmonise operations, help prevent cost duplication, and ensure that generally required services, such as online exercises, cybersecurity

situational awareness and guidelines are available to all. Public authorities, such as the National Cyber Security Centre at the Finnish Transport and Communications Agency Traficom (hereinafter referred to as the National Cyber Security Centre) and public service providers will actively communicate cybersecurity incidents and vulnerabilities to citizens, business community and public actors.

The National Cyber Security Centre serves as the designated coordinator of public authorities managing cyber crises referred to in the cybersecurity directive. It is also responsible for preparing the national cyber crisis management framework required under the NIS2 directive to manage large-scale cybersecurity incidents and cyber crises in collaboration with other public authorities.

Various societal actors engaged in ensuring cybersecurity are described below. Preparedness, response and countermeasures are implemented through extensive cooperation, which also includes exchanging information in order to formulate a common understanding of conditions and to coordinate common measures.

Figure 3. Societal actors engaged in ensuring national cybersecurity.



Political decision-making

Political decision-making resolves significant issues related to cyber preparedness and incident management, such as legislative policies and decisions in accordance with the foreign and security policy process. Public authorities report on the state and measures of cybersecurity to the President of the Republic, Parliament, the

government and ministerial working groups. The key body in matters of foreign and security policy significance is the Ministerial Committee on Foreign and Security Policy of the President of the Republic and Parliament (TP-UTVA).

Strategic level

The government and its ministries oversee the preparation of legislation concerning national cybersecurity, general policies, resource allocation, operating principles, strategic steering, preparedness, and countermeasures and cooperation.

The Office of the National Cyber Security Director bears national responsibility for coordinating and harmonising cybersecurity development, planning and preparedness, and for the preparedness of critical ICT infrastructure. The National Cyber Security Director coordinates and harmonises national cybersecurity development, planning and preparedness, and advises the government in matters of cybersecurity.

A cybersecurity coordination group appointed by the Ministry of Transport and Communications also works strategically to ensure that the national ministries in charge of cybersecurity, cyber defence and cyber diplomacy, and the cybersecurity authorities share consistent situational awareness concerning the state of cybersecurity in society, events that affect cybersecurity, and the evolution of the cybersecurity environment.

Supervisory authorities (NIS2 and others)

The supervisory authorities are defined as such in national legislation implementing the NIS2 directive, meaning the upcoming Cybersecurity Act and the Act on Information Management in Public Administration. The supervisory authorities monitor compliance with statutory duties in the private and public sectors. Finland applies a decentralised model, whereby sectoral public authorities supervise actors in their respective sectors. The National Cyber Security Centre also serves as a national coordination point. The supervisory authorities include the Finnish Transport and Communications Agency Traficom, the Energy Authority, the Finnish Safety and Chemicals Agency (Tukes), the National Supervisory Authority for Welfare and Health, the South Savo ELY Centre, the Finnish Food Authority, the Finnish Medicines Agency Fimea, and the Financial Supervisory Authority.

Hacking and other cyberattacks can, for example, enable an attacker to access personal data, which constitutes a personal data breach. The national supervisory authority for personal data breaches is the Office of the Data Protection Ombudsman, which supervises compliance with data protection legislation.

The Safety Investigation Authority, Finland (SIAF) is empowered to conduct a safety investigation of any cybersecurity incident that causes fatalities or considerable financial or tangible damage. Safety investigations seek to prevent the recurrence of similar events, to learn from them, and to foster a proactive safety culture.

Operative authorities

Operative cybersecurity authorities play a key role nationally in both preparing for cybersecurity incidents and in responding to them and deploying countermeasures. There are also several voluntary national information exchange networks in Finland.

The key function of the National Cyber Security Centre is to maintain national cybersecurity situational awareness and coordination with respect to national vulnerabilities. The Centre gathers and analyses data on information security threats and breaches, and assists in investigating technical information security incidents targeting Finland. It is also responsible for making the public more aware of cybersecurity. Its clients may apply situational awareness information when arranging and prioritising their own preparedness. The Centre also engages in extensive trust-based operational collaboration and information exchange with key national and international networks. It serves as the Finnish National Coordination Centre (NCC-FI) for the European Cybersecurity Industrial, Technology and Research Competence Centre.

The criminal investigation authorities seek to prevent crime and to investigate the parties involved and the details of offences for the purpose of criminal processes. These processes include the work of the police, public prosecutor and courts. The police investigate information network offences, seeking to apply information received to prevent potential future offences. The police maintain national situational awareness concerning information network offences. Active involvement by the National Bureau of Investigation focuses particularly on preventative operations that seek to enhance public awareness.

The intelligence authorities include the Finnish Security and Intelligence Service and the military intelligence authorities (Defence Command Finland and the Finnish Defence Intelligence Agency). These authorities are responsible for collecting, analysing and reporting information to support the work of the security authorities and the government. Intelligence is an asset in anticipating cyber threats that target Finland, and helps the competent authorities to combat these threats. The purposes of intelligence collection by the intelligence authorities include identifying the perpetrators of online cyberattacks and determining their backgrounds and motives in order to protect national security, supporting

government decision-making (including in respect of the attribution process), and discharging other statutory duties of authorities working in the field of national security.

The duties of the Defence Forces may also be considered to cover the cyber domain (cyber defence and intelligence in the cyber domain). These duties accordingly include military defence, supporting other authorities and providing international assistance, engaging in cooperation, and conducting other international operations. The Defence Forces protect the territory of Finland, the living conditions of its population, the freedom of action of top-level government and the lawful order of society, applying military force as necessary whenever Finland is subject to any threat of armed attack or any similar external threat.

Central, regional and local administration and independent bodies

Central, regional and local administration, wellbeing services counties, municipalities and independent bodies play a key role in ensuring cybersecurity in the daily work of authorities. Actors include government agencies, publicly owned undertakings and businesses, regional administration actors, wellbeing services counties, municipalities and joint municipal authorities, businesses and public service providers owned by wellbeing services counties and municipalities, and independent bodies. Some of these are required to direct, supervise, instruct, assist, coordinate, support and alert, and also to gather, analyse and share information on cybersecurity to support decision-making and operational development. They also provide public services in cooperation with the business community, and ensure the security, risk and continuity management and preparedness of services.

Businesses and organisations

The operations, competence and resources of the private sector form a significant element in Finland's national cybersecurity, with the business community owning most of the country's critical infrastructure. Safeguarding critical infrastructure and security of supply as part of the vital functions of society is crucial for societal functionality and continuity management. Besides their technological capacity, businesses have a strong competence base and the commitment and resources to prepare for cybersecurity threats to their operations, both in Finland and in international markets.

The preparedness of the business community is partly based on legislation, but also on voluntary preparedness and work to ensure security of supply. The public and private sectors collaborate on a daily basis to maintain awareness of conditions,

and through active information exchange and long-term development work. The business community is closely involved in various cooperation groups, increasing trust between the public and private sectors and providing an opportunity for impactful cooperation internationally as well.

Businesses generate most of the information and cybersecurity services in society. Private ICT service providers play a key role in the cybersecurity of citizens and businesses, and of national and regional government.

National Emergency Supply Organisation

The National Emergency Supply Organisation is a network that includes the National Emergency Supply Agency and its Board, the National Emergency Supply Council, and sectors and pools in various industries. The organisation also works with regional actors, including Regional State Administrative Agencies, municipalities and cities, and several regional commissions.

The National Emergency Supply Organisation cooperates with the public sector, several hundred businesses, organisations and third sector actors to maintain and develop national security of supply. The objective is to ensure the operating conditions of organisations that are critical for security of supply, and thereby those of society as a whole under all circumstances.

Supervised entities (NIS2)

Risk management and incident reporting obligations under the NIS2 directive are applied to the essential and important entities specified in the directive, which operate in sectors that are critical for the functioning of society and whose size must usually exceed certain threshold values. These parties are here referred to as supervised entities.

Annexes I and II to the NIS2 directive list the types of entities that fall within the scope of the directive, which covers the following sectors: energy, transport, banking, financial market infrastructures, social affairs and health drinking water, wastewater, digital infrastructure, ICT service management, public administration, and space (Annex I), as well as postal and courier services, waste management, manufacture, production and distribution of chemicals, production, processing and distribution of food, manufacturing, digital providers and research (Annex II).

Service providers and their supply chains

Service providers are organisations that provide services or products for society. A service provider is responsible for cybersecurity in the life cycle of its service and product throughout the value chain. The cybersecurity of the supply chain is ensured through risk management methods in accordance with the upcoming Cybersecurity Act or by agreement.

Service providers also include research institutions and institutes of higher education, and some civil society organisations. These generate competence and knowledge capital and innovations in cybersecurity, and support preparedness and crisis recovery.

Organisations and fourth-sector actors

Finland is internationally renowned for its numerous civil society organisations and the willingness of people to participate in the activities of civil society. Civil society organisations and volunteers are playing an increasingly important role in ensuring national cybersecurity. Integrating these organisations into cybersecurity networks promotes national resilience, and they also need the support of other actors in developing cybersecurity. Civil society organisations are approachable and trusted, strengthening their role in developing civic skills. The National Defence Training Association of Finland (MPK) in particular provides support for enhancing cyber defence by arranging courses and developing and increasing the cyber reserve. Organisations are nevertheless not yet an established part of the cybersecurity ecosystem.

Both organisations and actors in the fourth sector of unorganised civil activity have a great deal to contribute in supporting incident management, and there is already experience of the support that they provide to authorities in managing significant incidents.

Citizens

Individual competence strengthens the cyber resilience of organisations and society. The fact that new technology solutions are an increasingly integrated part of daily life also highlights the role of individual members of the public in national cybersecurity. Vigilance is needed both at home and at work, and everyone can influence how incidents in the cyber domain impact their lives through their own actions. There is a need for continuous development and maintenance of competence when cybersecurity is a natural part of every citizen's social responsibility. Support provided to family and friends and timely reporting of personal observations help to maintain and develop national cyber resilience and facilitate cybercrime investigations.

PRIME MINISTER'S OFFICE

SNELLMANINKATU 1, HELSINKI
PO BOX 23, 00023 GOVERNMENT, FINLAND
Tel. +358 295 16001
info.vnk@gov.fi
vnk.fi/en

ISBN pdf: 978-952-383-462-0
ISSN pdf: 2490-1164