Turvallisuuskomitea
Säkerhetskommittén
The Security Committee

FINLAND'S CYBER SECURITY STRATEGY 2019

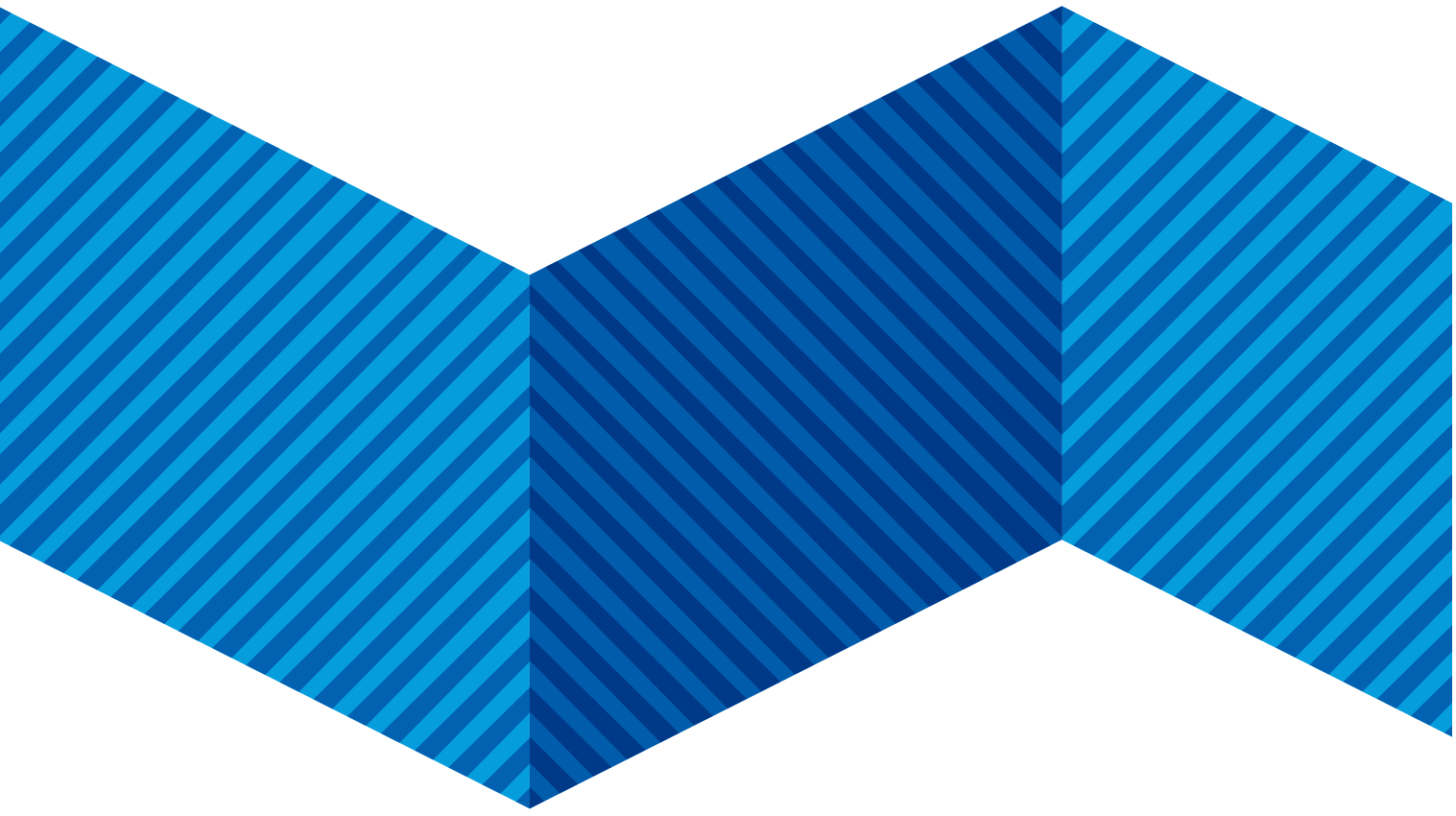
Government Resolution 3.10.2019

FINLAND'S
CYBER SECURITY
STRATEGY 2019

Secretariat of the Security Committee
Eteläinen makasiinikatu 8
PO BOX 31, FIN-00131 HELSINKI, FINLAND
www.turvallisuuskomitea.fi

ISBN: 978-951-663-054-3 (print)
ISBN: 978-951-663-055-0 (pdf)

CONTENTS



INTRODUCTION

The Finnish Cyber Security Strategy 2019 sets out the key national objectives for the development of the cyber environment and the safeguarding of related vital functions.[1] The strategy also aims to support the development of accessible and reliable digital services and business development. The strategy is based on the general principles of Finland's cyber security strategy of 2013. Finland's goal remains to be among the top experts in cyber security internationally. The implementation of national cyber security is linked to the Security Strategy of the Society (2017) and to the general principles of preparedness and security coordination as described in the Security Strategy, as well as to the principles of the competent authority. The strategy and its implementation are also part of the implementation of the EU Cyber Security Strategy.

The need to update the cyber security strategy has been influenced by significant changes in the operating environment and identified development needs in the work at the national level. The development of the digital operating environment offers new significant opportunities associated with, for example, with platform economy, ecosystems, new service production models and the development of terminal equipment and telecommunications. On the other hand, the operating environment faces not only known risks, such as human mistakes, but also evolving and changing threats that may endanger the vital functions of society, in particular cyber crime, espionage, state intelligence and various forms of hybrid influencing. Several studies have been conducted on the state of national cyber security in Finland.[2] The proposals that were made as a result were taken into account in this strategy and they will also be taken into account in the development programme that will be prepared on the basis of the strategy.

The cyber security strategy 2019 will launch the preparation of the National Cyber Security Development Programme. A new management coordination model supports the preparation of the development programme, taking into account the planning and cooperation for cyber security for public administration and the business community. The programme will improve the cyber security situation picture and integrate planning with other activities, such as economic planning.

[1] Cyber security is understood as a space in which the cyber environment can be trusted and its functioning is secured (Vocabulary of Cyber Security 2018). The cyber environment, on the other hand, can be understood in the same way as the digital environment, which evolves rapidly as part of society and as services.

[2] The VTT report on cyber competence in Finland (2016) presents 12 measures to further develop and strengthen cyber security competence in Finland. A report by Jyväskylä University and Aalto University on the current state of cyber security in Finland (2017) highlights the identified shortcomings and development needs, and these have been divided into 12 areas. In addition, the National Audit Office of Finland has published a report on the organisation of cyber protection in Finland (2017), containing five positions and four recommendations for the development of the whole. The Ministry of Justice's report on the preconditions for online voting in Finland (2017) examined how to conduct online voting. The working group does not recommend the introduction of online voting in Finland, as its risks currently outweigh its benefits. Prepared by Jyväskylä University and Aalto University, a report on the strategic management of cyber security in Finland (2018) proposed measures to manage strategic cyber security in society and public administration, to manage major disruptions in the cyber environment and to measure the state of cyber security.

STRATEGIC GUIDELINES

1. **DEVELOPMENT OF INTERNATIONAL COOPERATION** – protection of the cyber environment without borders

Finland strives to secure its cyber environment while enjoying active support internationally and through EU cooperation.

International cooperation is vital for Finland's cyber security as it benefits Finland to closely cooperate with international actors multilaterally, regionally and bilaterally. This is true for cooperation and dialogue on both technical and political levels.

International cooperation relies on the existing international law, international treaties and respect for human rights also in the cyber environment. Finland wants to maintain a universal, free and stable internet and to enable its safe use. Finland does not accept the aim of restricting the freedom and openness of the internet and, consequently, the fundamental rights and freedoms of individuals. In all cooperation on cyber security, Finland emphasises the rule of law, democracy and transparency.

To solve international cyber security challenges, Finland plays an active role in the European Union and in key international organisations (UN, OECD, OSCE, Council of Europe, the framework of NATO partnership programmes). This is part of strengthening the international rules-based system, which is a key objective in Finland's foreign policy.

The decisions of the European Union and cooperation within the EU provide the backbone for Finland's national cyber security policy and its development. Finland is actively involved in developing the EU's Common Foreign and Security Policy on Cyber Security. In addition, the EU's renewed cyber security strategy and key legislative projects, such as the EU Network and Information Security Directive (NIS), have a strong impact on the development of cyber security also at national level.

The cyber environment is protected by increasing the threshold for different types of cyber attacks, for example by improving the observation and attribution capacity of cyber attacks and the ability to respond. Counter-measures may consist, for example, of law enforcement measures, diplomatic measures or active cyber counter-measures. The EU's guidelines for the development of strong cyber defence are taken into account in the development of counter-measures. Within the framework of the EU, Finland contributes to the fight against cyber crime through international cooperation by justice and law enforcement authorities and by contributing to the development of international law and agreements.

2. BETTER COORDINATION OF CYBER SECURITY MANAGEMENT, planning and preparedness

The overall state of national cyber security will improve through a development programme and by promoting cooperation in planning and monitoring.

So far, the implementation programmes of the 2013 cyber security strategy have been based solely on proposals from actors committed to its development and the partly sectoral work of the competent authorities. Effective cyber security planning requires that the necessary financial resources and cooperation are taken into account with sufficient precision in each administrative branch. This will be improved by a cyber security development programme extending beyond government terms; this will replace the earlier implementation programme. The programme will concretise national cyber security policies and clarify the overall picture of cyber security projects, research and development programmes.

The post of Cyber Security Director will be established at the Ministry of Transport and Communications to coordinate the national development of cyber security.

The role of the Cyber Security Director is to ensure the coordination of the development, planning and preparedness of cyber security in society. The setting up of this post does not change the cyber security related responsibilities and powers of the ministries and competent authorities. The Cyber Security Director also acts as an adviser to the central government in cyber security related matters. Under his or her leadership, the overall picture and development programme of cyber security will be developed, drawing on the expertise of ministries, the Security Committee and cyber security actors.

When drawing up the development programme, it will be ensured that representatives of the cyber security industry, cyber research institutes and key organisations responsible for important public sector services participate in its preparation. The aim of this network structure is to deepen cooperation between the public administration and the business community.

The management of incidents affecting the cyber environment and cooperation at the operational level will be developed between cyber security actors. In the management of incidents, a general incident management model will be used and, where necessary, the meeting of the heads of preparedness will be used.

Cyber security preparedness requires cooperation among various actors in society, the central government and the business community sa well as

skills strengthening in different sectors. Interdependencies in the digital operating environment require a comprehensive architecture that takes cyber security into account. Continuity of operations and preparedness for incidents require expertise in procurement and tendering, implementation assessment of contractual obligations and comprehensive management of the supplier network and supply chains.

Other strategic measures for developing a sub-area:

- The information resources, digital services and infrastructure that are necessary for the vital functions of society will be defined. Target levels will be set for functions and service chains that are related to managing continuity of activities at the national level.

- Requirements management will be improved and harmonised in security-critical services as required by national security and in compliance with standards. The verification, testing, evaluation and recommendations for use of products and entire solution environments related to critical functions will be developed to ensure that requirements are met.

- With regard to new legislation on intelligence and other sectors, cyber security cooperation among the authorities will be developed in the development programme. Key development areas include cyber defence and the prevention of cyber threats that endanger national security. In addition, legislation enabling the fight against cyber crime will be developed in such a way that it enables effective prevention and investigation.

- The Cyber Security Centre's ability to compile 24/7 situational awareness and cooperation among the authorities and the business community will be further developed. This will promote Finland's ability to identify and warn against information security threats and to improve the opportunities of the business community and public administration to prepare for information security threats.

- The use and development of digital services by security authorities and critical actors in the business community will be secured by specially protected solutions that utilise and complement commercial services in accordance with the existing legislation.

- The businesses that provide critical services and continuity management for society's vital functions will be supported. The position of businesses is clarified when the target level of tasks is defined and the support mechanisms provided by the authorities are developed. Clear targets will be set for the responsible authorities to develop cyber security. For example, the authorities can promote the achievement of cyber security targets by including them in commercial agreements and, as far as the most important parts are concerned, they must make legislation more specific when necessary.

Interdependencies in the digital operating environment require a comprehensive architecture that takes cyber security into account.

3. DEVELOPMENT OF CYBER SECURITY COMPETENCE – everyday skills and top skills as cyber security safeguards

National cyber security competence will be ensured by identifying requirements and strengthening education and research.

Finnish society needs cyber security competence both in public administration and in the business community. National cyber security will be built in cooperation among the authorities, the business community, organisations and citizens, when everyone can contribute to our shared cyber security. Each individual is therefore an important cyber security actor who can improve cyber security through his or her actions on a daily basis and thus impact his or her own cyber security and that of others. At the national level, it must be ensured that everyone has sufficient capacity to operate safely in a digital environment.

In order to manage cyber security risks, the authorities and companies need wide-ranging expertise from both employees and subcontractors. At the national level, it must be ensured that companies have both top-level experts and other competent personnel. Skills development is also emphasised in the cooperation between the business community and research. Close cooperation, exchange of information on customer needs and development of services can create significant new skills on the national market alone.

As far as competences and the competitive edge are concerned, it is important for national companies to find new ways to keep their top talents as international competition increases. Finland's competitive edge is improved when international information security standards support products that are manufactured by Finnish companies. It is therefore important to continue to actively contribute to standardisation work and to produce products that have built-in security; this is how Finnish businesses can have better opportunities to succeed in international competition in areas where they are strong.

From the perspective of cyber security in society and the business community, it is essential to integrate cyber security into the activities of businesses which are not involved in producing cyber security related products, services and solutions. Companies whose actual business is outside the cyber security sector but whose activities are significantly affected by cyber security and related incidents will play an increasingly important role in the future. In particular legislative projects relating to network and information security have identified, for example, telecommunications, production and distribu-

National cyber security will be built in cooperation among the authorities, the business community, organisations and citizens, when everyone can contribute to our shared cyber security.

tion of energy, the financial and insurance sector, and health care as such areas.

The development of cyber security imposes competence requirements and cooperation obligations on public administration. Cyber security related guidelines, support and control responsibilities of the authorities who are in charge of critical functions, as well as the resources and tools required by them, will be improved in all administrative branches and at all administrative levels.

Other strategic measures to promote cyber security competence include:

- Training programmes related to cyber and information security, software and application development, information networks and telecommunications in vocational education, universities of applied sciences and universities will be strengthened.

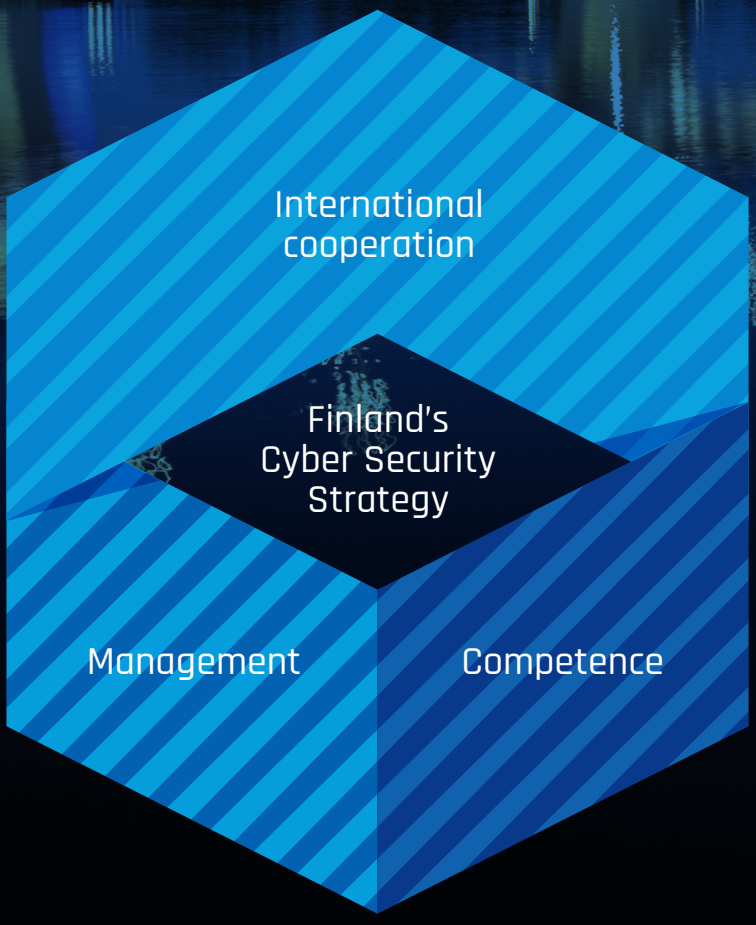
- The high level of education required by nationally critical cyber competence areas will be ensured. This is supported by both national and international training and exercises.

- National research, development and testing on cyber security will be strengthened.

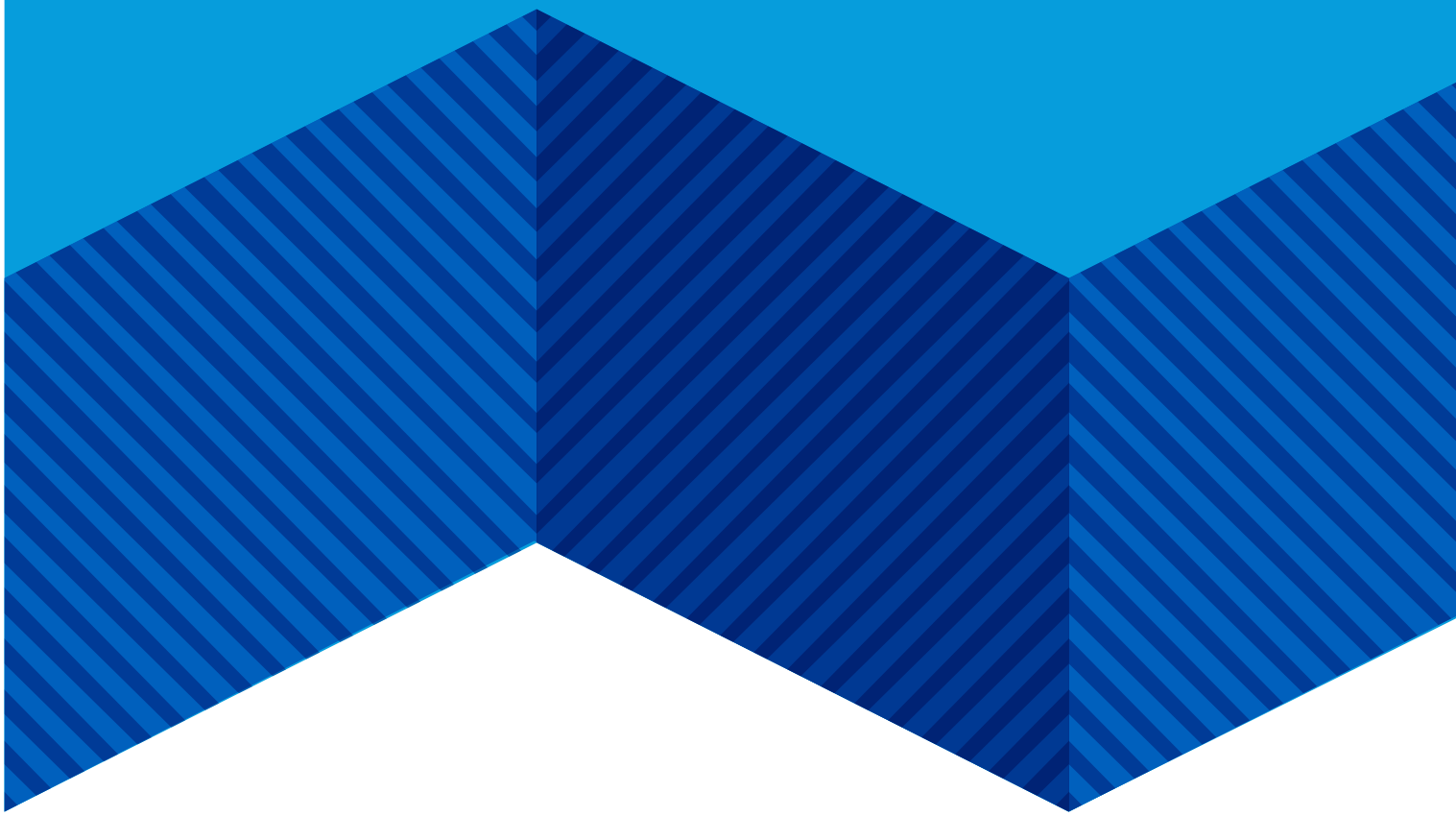
- The national system for training and exercising digital security will be strengthened as part of digital security training in the public administration. This will develop the skills of personnel in public administration, businesses and other stakeholders as well as of citizens.

- The public administration, the business community and private individuals will be made more aware of information security for new services and products. Cyber security is an essential element in the data economy and for applications based on artificial intelligence. This requires that manufacturers and service providers trust each other and that citizens trust the services and products that are offered to them.

FINLAND'S CYBER SECURITY STRATEGY 2019



www.turvallisuuskomitea.fi



Turvallisuuskomitea
Säkerhetskommittén
The Security Committee