Finland´s Cyber security Strategy

Government Resolution 24.1.2013

TABLE OF CONTENTS

Secretariat of the Security and Defence Committee
Eteläinen Makasiinikatu 8
PO BOX 31
FIN-00131 HELSINKI, FINLAND

www.yhteiskunnanturvallisuus.fi

Layout: Tiina Takala/Ministry of Defence
Translation: Katri Suvanto/Ministry of Defence
Print: Forssa print, 2013

ISBN: 978-951-25-2437-2 nid.
ISBN: 978-951-25-2438-9 pdf

1. INTRODUCTION

Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured.

Ensuring the security of society is a key task of the government authorities and the vital functions of our society must be secured in all situations. As an information society Finland relies on information networks and systems and, consequently, is extremely vulnerable to disturbances which affect their functioning. An international term for this interdependent, multipurpose electronic data processing environment is the cyber domain.

Society's growing information intensity, the increase of foreign ownership and outsourcing, integration between information and communications technologies, the use of open networks as well as the growing reliance on electricity have set totally new requirements for securing society's vital functions in normal conditions, during serious disturbances in normal conditions and in emergency conditions.

Threats against the cyber domain have increasingly serious repercussions for individuals, businesses and society in general. The perpetrators are more professional than before and today the threats even include state actors. Cyber attacks can be used as a means of political and economic pressure; in a serious crisis pressure can be exerted as an instrument of influence alongside traditional means of military force.

The cyber domain should also be seen as a possibility and a resource. A safe cyber domain makes it easier for both individuals and businesses to plan their activities, which in turn boosts economic activity. A properly working environment also improves Finland's appeal for international investors. In addition to these, cyber security itself is a new and strengthening business area. In addition to the increasing job opportunities and tax revenue, society accrues benefits from this strengthening business sector in many ways. National cyber security is interconnected with the success of Finnish companies.

This Strategy defines the key goals and guidelines which are used in responding to the threats against the cyber domain and which ensure its functioning. By following the Cyber Security Strategy's guidelines and the measures required, Finland can manage deliberate or inadvertent disturbances in the cyber domain as well as respond to and recover from them.

The arrangements of comprehensive security are defined in the Government resolution of 5 December 2012 on comprehensive security while the Security Strategy for Society (2010) defines the principles of ensuring the functions vital to society. Vital functions include the management of Government affairs, international activity, Finland's defence capability, internal security, functioning of the economy and infrastructure, the popula-

tion's income security and capacity to function, and psychological resilience to crisis. The Cyber Security Strategy process is an element in the implementation of the Security Strategy for Society. The process of cyber security strategy is a part of the implementation of the Security Strategy for Society; the Cyber Security Strategy complies with the principles and definitions in the Security Strategy for Society and the Government Resolution on Security of Supply. The Government Resolution (2013) defines the focus areas and goals for the security of supply. The Strategy takes into account the forthcoming Government resolution on the arrangements of comprehensive security.

Cyber security is not meant to be a legal concept the adoption of which would lead to granting new competences to authorities or other official bodies. In this respect no changes are proposed to the bases of contingency arrangements or to regulations concerning the competences of authorities.

The Strategy presents the vision, approach and strategic guidelines of cyber security. The Strategy's background dossier depicts the entities relevant to the strategic guidelines, such as the cyber domain, its rapid development and potentially ensuing threats as well as the required countermeasures for securing the functions vital to society. In addition, the dossier describes the principles of cyber security management and disturbance control arrangements as well as the provisions related to cyber security and the principles for preparing the action plan for the Cyber Security Strategy.

The action plan which is being prepared will cover the practical measures tasked to administrative branches and actors. This creates the conditions for the materialisation of the strategic guidelines as well as the vision for achieving the desired end state, including the jointly agreed cross-cutting measures in society.

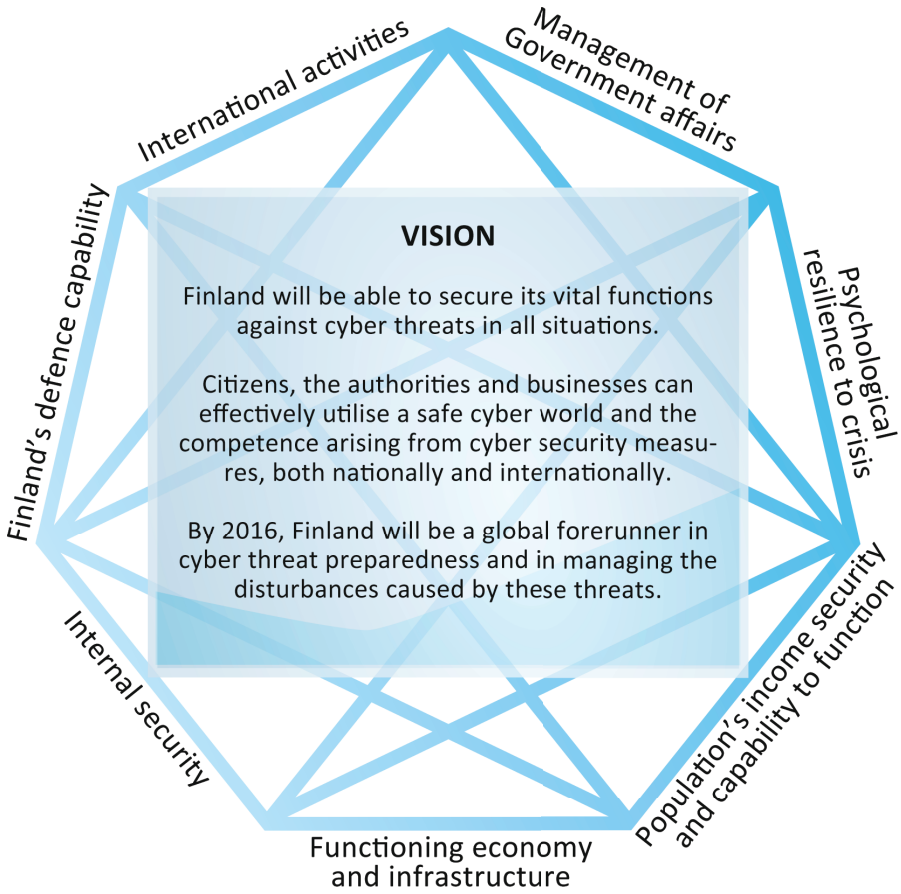
2. VISION FOR CYBER SECURITY

As a small, capable and collaborative country Finland has excellent chances of rising to the vanguard in cyber security. We have an extensive knowledge base and strong expertise, a long tradition of close public-private cooperation, built on trust, as well as intersectoral collaboration.

The vision of Finland's cyber security is that:

- Finland can secure its vital functions against cyber threats in all situations.
- Citizens, the authorities and businesses can effectively utilise a safe cyber domain and the competence arising from cyber security measures, both nationally and internationally.
- By 2016, Finland will be a global forerunner in cyber threat preparedness and in managing the disturbances caused by these threats.

FIGURE 1 Vision for cyber security



3. CYBER SECURITY MANAGEMENT AND THE NATIONAL APPROACH

The changes that take place in the cyber domain are fast and their effects are difficult to predict. The Software Development Life Cycle for information technology is short and the same trend applies to different forms of cyber attacks and malware. Cyber threat preparedness and cyber defence require increasingly swift, transparent and better coordinated action from all parties in society, both individually and collectively.

The Government represents the highest level of cyber security management. The Government is responsible for providing political guidance and strategic guidelines for cyber security as well as for taking the required decisions regarding the resources and prerequisites to be allocated to it.

Cyber security management and disturbance management require that the Government and different actors have a reliable, real-time cyber security situation picture of the condition of society's vital functions as well as disturbances which affect their functioning. Each ministry and administrative branch is responsible for cyber security and disturbance management within their mandate. The cyber domain and the nature of threats highlight the importance of cooperation as well as efficient and flexible coordination. The strategic cyber security tasks of ministries and the related development requirements are based on the analysis of identified cyber threats as well as the disturbance management requirements established on the basis of said analysis. Each ministry, within its sphere of responsibility, must see to it that the strategic tasks determined on the basis of the desired end states are carried out.

National cyber resilience will be tailored so as to ensure the preparedness and predictive capabilities required by the goals of comprehensive security, and to facilitate its operating capability during cyber disturbances as well as post-disturbance recovery.

The national approach for Finland's cyber security management is built on the following principles.

1. In line with the Government decree on the tasks assigned to ministries, matters which relate to cyber security as a rule fall within the remit of the Government. Each ministry is in its sector responsible for preparing cyber security related matters and appropriate arrangement of administrative matters.

2. As cyber security is an essential part of the comprehensive security of society the approach for its implementation follows the principles and procedures established in the Security Strategy for Society.

3. Cyber security relies on the information security arrangements of the whole society. Cyber security depends on appropriate and sufficient ICT and telecommunication network security solutions established by every actor operating in the cyber world. Various collaborative arrangements and exercises advance and support their implementation.

4. The approach for the implementation of cyber security is based on efficient and wide-ranging information-collection, an analysis and gathering system as well as common and shared situation awareness, national and international cooperation in preparedness. This requires the establishment of a Cyber Security Centre as well as the development of 24/7 information security arrangements for the entire society.

5. Cyber security arrangements follow the division of duties between the authorities, businesses and organisations, in accordance with statutes and agreed cooperation. Rapid adaptability as well as the ability to seize new opportunities and react to unexpected situations demand strategic agility awareness and compliance from the actors as they keep developing and managing the measures which are aimed at achieving cyber security.

6. Cyber security is being constructed to meet its functional and technical requirements. In addition to national action, inputs are being made into international cooperation as well as participation in international R&D and exercises. The implementation of cyber security R&D and education at different levels does not only strengthen national expertise, it also bolsters Finland as an information society.

7. Cyber security development will heavily invest in cyber research and development as well as in education, employment and product development so that Finland can become one of the leading countries in cyber security.

8. In order to ensure cyber security development, Finland will see to it that appropriate legislation and incentives exist to support the business activities and their development in this field. Basic know-how in the field is gained through business activity.

4. STRATEGIC GUIDELINES FOR CYBER SECURITY

A national cyber strategy will be developed in accordance with the strategic guidelines. They create the conditions for the materialisation of the national cyber security vision. A separately prepared action plan will outline the measures which ensure the materialisation of national cyber security goals. The implementation programme will include the plans of different actors and administrative branches as well as the intersectoral measures that result from the plans.

The implementation of the strategic guidelines will strengthen public-private cooperation, which is regarded as a forte of the Finnish security community. Such collaboration can best serve the entire society and support the actors who provide its vital functions. The objective is to maintain the uninterrupted and safe flow of different functions in everyday life and during disturbances.

Cyber security is built on sufficient capabilities development over the long term, their well-timed and flexible use and the resilience of society's vital functions against disturbances in cyber security. Competent ministries will develop the cyber security capacities of authorities within their respective administrative branches and, for example, by outlining the strategic cyber security tasks of the ministries. Most strategic cyber security duties and the development of associated capabilities also require action and resources from the other ministries, regional and local administrations as well as the business community and organisations. Ministries must always take into account the different levels of administration as well as the role of the business community and organisations when it comes to developing and using the capabilities. A Security Committee which will be set up to play an active role in the field of comprehensive security will act as a permanent cooperation body for contingency planning. Separate provisions regarding the tasks of the Security Committee will be issued.

STRATEGIC GUIDELINES:

1

Create an efficient collaborative model between the authorities and other actors for the purpose of advancing national cyber security and cyber defence.

The strategic guidelines of the Cyber Security Strategy are advanced by intensifying active collaboration between actors whose aim is to achieve a shared situation awareness and effective defence against the threats. Different sectors' preparedness in securing the vital functions in disturbed conditions will be improved by organising regular exercises. Each actor will develop its national and international participation in exercises. The actors will improve the utilisation of best practices and lessons-learned accrued through international exercises by improving the exchange of information and mutual coordination. The goal of exercises is to enhance the participants' chances of exposing the vulnerabilities of their own actions and systems, in developing their capabilities and training their personnel. Cyber defence will be advanced by promoting the exchange of information and regulations as well as through cooperation between the authorities and the business community.

2

Improve comprehensive cyber security situation awareness among the key actors that participate in securing the vital functions of society.

The goal is to improve the situation awareness of different actors by furnishing them with real-time, shared and analysed information regarding vulnerabilities, disturbances and their effects. The situation picture will include threat assessments arising from the cyber world. Cyber threat prediction requires the analysis of the political, military, social, cultural, technical and technological as well as economic situation. In order to compile and maintain a combined cyber security situation picture, a Cyber Security Centre will be established under the Finnish Communications Regulatory Authority (FICORA).

The Cyber Security Centre will collect information on cyber incidents and disseminate it to different actors. The actors will then estimate the effects of the disturbance on the activity they are responsible for. Their analyses are relayed back to the Cyber Security Centre to be included in a combined cyber security situation picture. The combined situation picture will be replicated among different actors to support decision-making.

The Government situation centre must have a reliable, comprehensive and real-time total assessment of the cyber security situation at its disposal. The assessment encompasses the combined situation picture compiled by the Cyber Security Centre as well as the different administrative branches' estimates of the consequences of cyber incidents to society's vital functions. The state leadership has access to the total situation assessment as well as the estimate of the developments in the operating environment.

3	**Maintain and improve the abilities of businesses and organisations critical to the vital functions of society as regards detecting and repelling cyber threats and disturbances that jeopardise any vital function and their recovery capabilities as part of the continuity management of the business community.** In their security and contingency plans as well as related service structures the businesses and organisations critical to the vital functions of society will comprehensively take into account the cyber threat factors related to the vital functions, and maintain the required cyber defence capabilities. The goal is to detect and identify any disturbances to the vital functions appearing in risk assessments and to respond to them in a manner which minimises their detrimental effects. The key actors will improve their tolerance, including contingency planning and exercises, so as to be able to operate under cyber attacks. The security of supply-organisation will support this activity through reports, instructions and training.
4	**Make certain that the police have sufficient capabilities to prevent, expose and solve cybercrime.** The police are the competent authority for carrying out investigations related to cybercrime. The police will generate an analysed, high-quality cybercrime situation picture and disseminate it as part of the combined situation picture detailed in guideline 2. The police will closely cooperate with the Cyber Security Centre. It must be ensured that the police have sufficient powers, resources and motivated personnel for cybercrime prevention, tactical police investigations as well as for processing and analysing the digital evidence. International operational cooperation and the exchange of information will be continued and intensified with the EU and with other countries' corresponding law enforcement officials, such as the Europol.
5	**The Finnish Defence Forces will create a comprehensive cyber defence capability for their statutory tasks.** A military cyber defence capacity encompasses intelligence as well as cyber attack and cyber defence capabilities. The Defence Forces will protect their systems in such a manner that they are able to carry out their statutory tasks irrespective of the threats in the cyber world. Guaranteeing capabilities, intelligence and proactive measures in the cyber world will be developed as elements of other military force. Under the leadership of the Ministry of Defence the required provisions on powers will be prepared for the Defence Forces to facilitate the implementation of the aforementioned tasks. Any identified short-comings in the provisions will be corrected through legislation. Cyber defence will be exercised and developed together with the key authorities, organisations and actors in the business community, both nationally and internationally. The Defence Forces will provide executive assistance within the constraints of legislation.

6	**Strengthen national cyber security through active and efficient participation in the activities of international organisations and collaborative fora that are critical to cyber security.** The goal of international cooperation is to exchange information and lessons-learned as well as take in the best practices so as to raise the national quality of cyber security. The implementation of preparedness and other cyber security measures will fall short of the goal without effective and systematically coordinated international cooperation. All authorities, within their field of competence, will cooperate, especially with those states and organisations that are global forerunners in the field of cyber security. Active collaboration takes place through R&D, pre-agreement consultations and the teamwork efforts of organisations as well as through participation in international exercises. In the development of cyber security, the European Union as well as many international organisations, such as the UN, the OSCE, NATO and the OECD are important venues for Finland. The EU is increasingly active in the field of cyber security and it also engages in cooperation with third countries. Finland is actively participating in this development.
7	**Improve the cyber expertise and awareness of all societal actors.** In support of continuously improving the competence and awareness of the actors of society, inputs will be made to developing, utilising and training common cyber security and information security instructions. In order to develop the comprehensive preparedness of society the exercises will also incorporate businesses and non-governmental organisations (NGOs) critical to the vital functions of society. A strategic cyber security centre of excellence will be established under the existing ICT-SHOK (TIVIT). It will provide an opportunity for top research teams and companies who utilise the results to engage in effective mutual cooperation over the long term. The centre of excellence will facilitate the conditions for the establishment of a robust national cyber security cluster. Inputs into R&D and education will be increased as well as action to improve cyber security know-how in the whole of society.

8	**Secure the preconditions for the implementation of effective cyber security measures through national legislation.** Working together, the administrative branches and the business community will chart the legislation, including any needs to review the provisions relevant to the cyber domain and cyber security. The results of this action will comprise the proposals for legislative review which will advance the achievement of the goals of the Cyber Security Strategy. The charting will take into account the rapidly changing phenomena in the cyber domain. One of the purposes is to provide the competent authorities and other actors with the sufficient means and powers through legislation to implement cyber defences for the functions vital to society and, especially, the security of the state. Any possible legislative hurdles, restrictions and obligations related to data protection, as well as those arising from international obligations, that impede the obtainability, disclosure and exchange of information useful for effective cyber defence purposes, will be taken under review. When it comes to the assessment of information-gathering and other data processing one should also estimate whether the competent authorities should have improved possibilities for gathering information, data processing, or being informed of cyber threats and their sources, while simultaneously paying attention to ensuring the basic rights of privacy and confidentiality in electronic communications. Most of the critical infrastructure in society is in private business ownership. Cyber know-how and expertise as well as services and defences are for the most part provided by companies. National cyber security legislation must provide a favourable environment for the development of business activities. This would, for its part, enable the creation of an internationally recognised, competitive and export-capable cyber security cluster. At the same time Finland would become an appealing and cyber secure environment worthy of business investments and companies' operations.
9	**Assign cyber security related tasks, service models and common cyber security management standards to the authorities and actors in the business community.** The development of cyber security requires the clear allocation of responsibilities and tasks in accordance with the strategic guidelines. In practice this presupposes that each administrative branch make its risk assessment and maturity analysis, which help identify any significant vulnerabilities and risks from the standpoint of cyber security, and the level of their management. The results will be used in preparing action plans for each administrative sector and, together with the security of supply-organisation, support the drafting of action plans for the business community.

10 The implementation of the Strategy and its completion will be monitored.

Ministries and agencies are responsible for implementing the Strategy within their respective administrative branches, carrying out the tasks related to cyber security, and implementing and developing the security of supply. The future Security Committee monitors and coordinates the implementation of the Strategy. The goals of cyber security coordination include the avoidance of unnecessary duplication, identification of possible shortcomings and determining the competent entities. The competent authorities will make the actual decisions subject to the provisions. The Government Information Security Management Board (VAHTI) will process and coordinate the central government's key information security and cyber security guidelines. Ministries, agencies and establishments are to include the resources for the implementation of the Cyber Security Strategy in their operating and financial plans.

APPENDIX 1: TERMS AND DEFINITIONS

Term	Definition
Information infrastructure	Information infrastructure means the structures and functions behind information systems that electronically transmit, transfer, receive, store or otherwise process information (data).
Critical information infrastructure	Critical information infrastructure refers to the structures and functions behind the information systems of the vital functions of society which electronically transmit, transfer, receive, store or otherwise process information (data).
Critical infrastructure	Critical infrastructure refers to the structures and functions which are indispensable for the vital functions of society. They comprise physical facilities and structures as well as electronic functions and services.
Cyber	The word 'cyber' is almost invariably the prefix for a term or the modifier of a compound word, rather than a stand-alone word. Its inference usually relates to electronic information (data) processing, information technology, electronic communications (data transfer) or information and computer systems. Only the complete term of the compound word (modifier+head) itself can be considered to possess actual meaning. The word cyber is generally believed to originate from the Ancient Greek verb κυβερεω (kybereo) "to steer, to guide, to control".
Cyber risk	Cyber risk means the possibility of an accident or vulnerability in the cyber domain which, if it materialises or is being utilised, can damage, harm or disturb an operation that depends on the functioning of the cyber domain.
Cyber domain, cyber environment	Cyber domain means an electronic information (data) processing domain comprising of one or several information technology infrastructures. *Note 1* Representative to the environment is the utilisation of electronics and the electromagnetic spectrum for the purpose of storing, processing and transferring data and information via telecommunications networks. *Note 2* Information (data) processing means collecting, saving, organising, using, transferring, disclosing, storing, modifying, combining, protecting, removing, destroying and other similar actions on information (data).

Term	Definition
Cyber security	Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured.. Note 1 In the desired end state the cyber domain will not jeopardise, harm or disturb the operation of functions dependent on electronic information (data) processing. Note 2 Reliance on the cyber domain depends on its actors implementing appropriate and sufficient information security procedures ('communal data security'). These procedures can prevent the materialisation of cyber threats and, should they still materialise, prevent, mitigate or help tolerate their consequences. Note 3 Cyber security encompasses the measures on the functions vital to society and the critical infrastructure which aim to achieve the capability of predictive management and, if necessary, tolerance of cyber threats and their effects, which can cause significant harm or danger to Finland or its population.
Cyber threat	Cyber threat means the possibility of action or an incident in the cyber domain which, when materialised, jeopardises some operation dependent on the cyber world. *Note* Cyber threats are information threats which, when materialised, jeopardise the correct or intended functioning of the information system.
Information system	Information system means the system comprising the personnel, information processing equipment, data transfer equipment and software programs intended to make some operation more efficient, easier or even possible by means of information (data) processing.
Protection of privacy	Protection of privacy means the protection against the unlawful or hurtful invasion of personal privacy. Protection of privacy includes the right to privacy and other associated rights in the processing of personal data. Personal data means any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household.
Information (data) security	Information security means the administrative and technical measures taken to ensure the availability, integrity and confidentiality of data.
UTVA	Cabinet Committee on Foreign and Security Policy.
VAHTI	Government Information Security Management Board.
YTS	The Security Strategy for Society, Government Resolution 16 December 2010.

www.yhteiskunnan turvallisuus.fi/en