FINLAND´S CYBER SECURITY STRATEGY

Background dossier

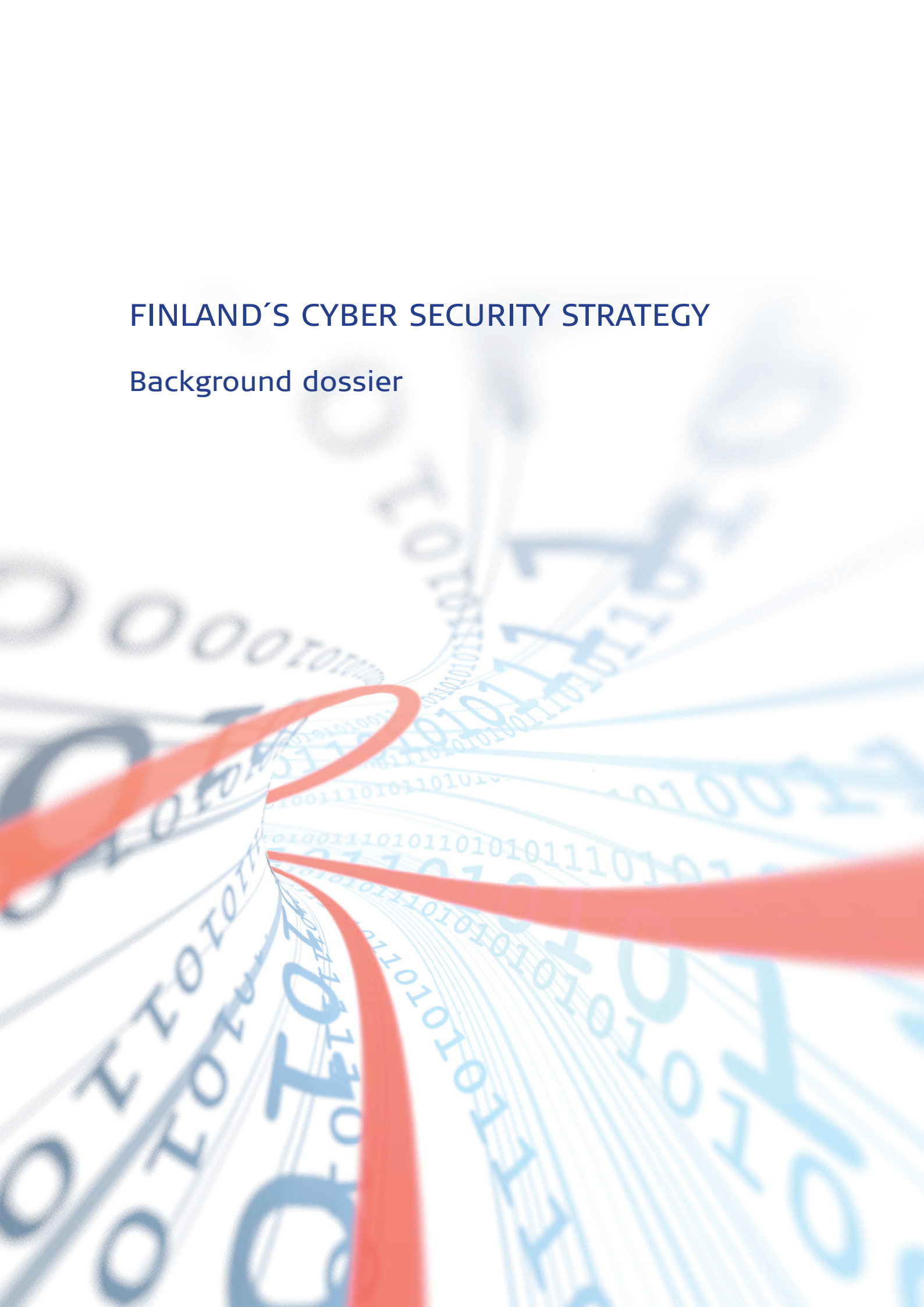

TABLE OF CONTENTS

1. INTRODUCTION

This background dossier is a part of Finland's Cyber Security Strategy. The key purpose of this document is to increase the understanding of cyber security actors of the cyber domain and, consequently, help them improve their cyber security. The background dossier expands the Strategy and explains in further detail the national cyber security approach, the cyber domain and the threat scenario that determines our preparedness. The document elaborates on the measures required by the strategic guidelines as well as national and international cyber security regulation. The principles for drafting the action plans for different administrative branches and other actors are presented at the end of this document.

2. CYBER DOMAIN AND CYBER THREAT

The global cyber domain consist of an elaborate and multi-layered worldwide information network which comprises ICT networks that are operated by national security authorities, other public authorities, the business community, monitoring and control systems of the industry and critical infrastructure. The increasingly high-speed global cyber domain is bringing states, businesses and citizens ever closer together. While this development has significantly fostered well-being, it has also introduced an entirely new set of risks. When IT equipment and systems are down, the ICT infrastructure crashes or serious cyber attacks occur, these can result in extremely negative impacts on public services, business life and administration and, consequently, the viability of society as a whole.

Cyber attacks can seriously disrupt or even paralyse segments of critical infrastructure and society's vital functions. The state or an organisation can be forced to make political, military or financial concessions. The great powers equate cyber attacks with military action which can be met with any available means.

Thus far cyber operations have been interpreted as 'soft measures', for which reason the threshold for using them is estimated to be below that of traditional military operations. The increasing cyber activism, cybercrime and cyber espionage denote growing activity among states and non-state actors. Consequently, the cyber domain has transformed the traditional power structure, providing even small states and non-state actors with an opportunity to have effectual action. In cyberspace, it is no longer size and mass that matter, rather, it is expertise.

The previously described developments in the cyber domain also impact Finland. Finland is one of the most developed information societies whose functioning relies on various electronic networks and services. Finland has already been the target of cyber operations where the focus was on cyber activism, cybercrime and cyber espionage. The international development in cyberspace increases the possibilities of new threats being used against us. The public administration and the business community are continually being targeted by crackers and hackers attempting to exploit system vulnerabilities. That the targets are carefully selected and

studied only serves as an indication of the professionalism of the attacks. Sophisticated malware and techniques are increasingly used in these attacks.

By exploiting system vulnerabilities, the openness of the cyber domain makes it possible to carry out attacks from all over the world. Such vulnerabilities exist in human action, organisational processes and the ICT technology being used. It is very difficult to protect oneself against complex and sophisticated malware, and to identify or locate the perpetrators. The increasing proliferation of information technology in industrial production and control systems has created new vulnerabilities and possible targets for cyber attacks.

Cyber security entered a new era in 2010 when the Stuxnet worm was discovered. It was used to carry out an attack against Iran's nuclear plants: Stuxnet damaged Iran's uranium enrichment centrifuges, holding back its enrichment project for years. Expert skills and considerable resources were needed to write the Stuxnet code. This malware demonstrated that cyber tools can also inflict physical damage on electronic equipment and systems. In this new phase, industrial automation and programmable logic controllers are ever more often the first targets of cyber attacks, when, in fact, the ultimate objective is to impact society's vital functions.

The cyber threat scenario means a description of disruptions caused by cyber threats and their mechanism, source, target and impacts on the target. The threats can directly or indirectly impact society's vital functions, critical infrastructure and/or citizens from within or outside national borders.

Cyber threats included in the cyber threat scenario are:

- Cyber activism (cyber vandalism, hactivism)
- Cybercrime
- Cyber espionage
- Cyberterrorism
- Cyber operations: pressure, Low Intensity Conflict (LIC) or cyber warfare

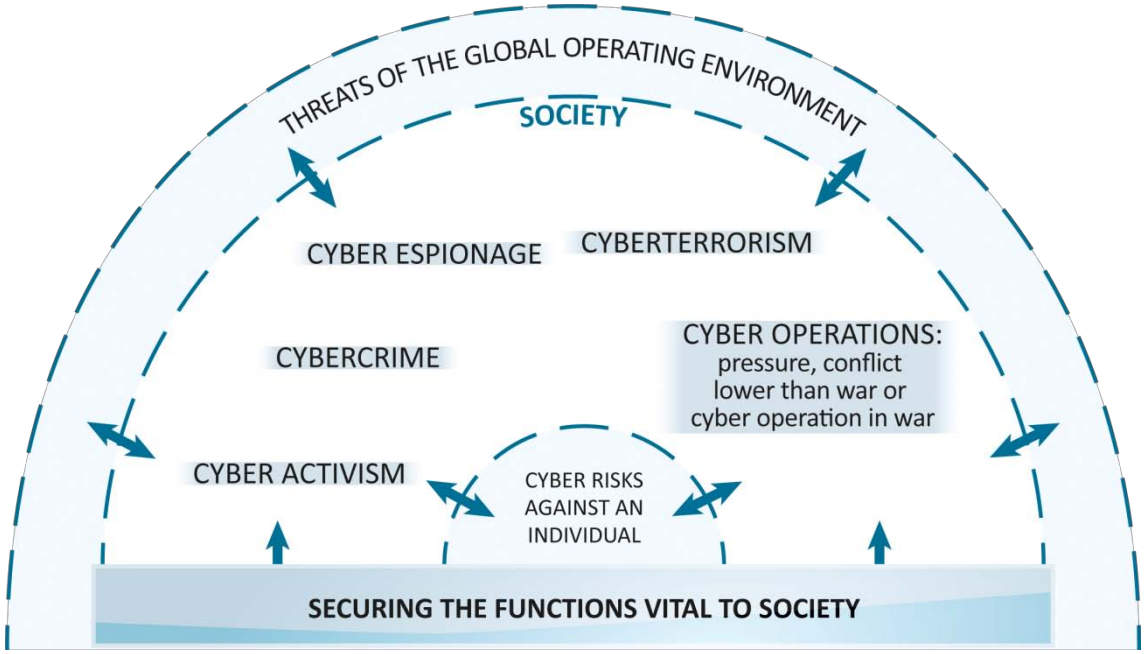

FIGURE 1 Finland's cyber threat scenario

Threats to society's vital functions and critical infrastructure can emerge independently, concurrently or as a sequential continuum. Whereas their escalation varies in speed and endurance, more often than not they make their impact in a short period of time. Due to the nature of the cyber domain, it is difficult to predict the causes of threats, the actors behind them, their exact targets, goals and scope or the consequences of their effects. Other risks can also be associated with cyber threats. For example, terrorist strikes causing physical destruction can also incorporate various cyber operations.

3. PRINCIPLES OF CYBER SECURITY MANAGEMENT AND THE MANAGEMENT OF DISRUPTIONS

3.1 Basic principles of cyber security management

The Government comprises the highest level of cyber security management. The Prime Minister leads the Government and is responsible for preparing and coordinating the handling of the matters that are the purview of the Government. Preliminary deliberation and coordination occurs in ministerial working groups led by the Prime Minister and, as required, the Government's evening session and negotiations. The Government is responsible for providing political guidance and strategic guidelines for cyber security as well as for taking the required decisions regarding the prerequisites and resources allocated to it.

In line with the basic principles of the Security Strategy for Society, the competent authorities are responsible for disturbance management and associated contingency planning. Each ministry sees to the legislative process within its administrative domain, guides the action

within its branch and, when necessary, participates in intersectoral cooperation. The Cyber Security Strategy does not change the tasks defined in the Security Strategy for Society, pursuant to which the Ministry of Transport and Communications is responsible for safeguarding the functioning of electronic ICT systems, and the Ministry of Finance is responsible for safeguarding the state administration's IT functions and information security, and the service systems common to the central government.

The future Security Committee coordinates cyber security preparedness, monitors the implementation of the Cyber Security Strategy and issues recommendations on its further development. The Security Committee closely cooperates with other collaborative bodies that coordinate cyber security-related issues as part of their duties. The future Cyber Security Centre supports and assists cyber security actors within the scope of its tasking. The Government Information Security Management Board (VAHTI) supports the Government and the Ministry of Finance in administrative data security-related decision-making. VAHTI processes and coordinates all of the central government's important matters that relate to data security and cyber security.

The effectiveness of disturbance management will be measured by the successfulness of the pre-emptive measures. Cyber security arrangements in normal conditions will make or break the outcome of cyber incidents in emergency conditions. All administrative branches as well as organisations and companies critical to security of supply are required to make contingency plans against cyber threats. Companies are to include cyber preparedness in their normal continuity management planning.

FIGURE 2
Principles of cyber security management

The prevention of cyber threats calls for proper planning and forecasting. This being the case, our new operating environment demands strong expertise as well as swift, appropriate and consistent reaction from all parties, in other words, strategic agility. Cyber security management embodies all three factors of strategic agility: strategic sensitivity, collective commitment and resource fluidity.

Strategic sensitivity entails the capability to rapidly compile a situation picture and establish situation awareness. *The commitment of the leadership* requires integrated situation awareness, coordinated and networked management and the optimisation of collective benefits. *The flexible use of resources* demands sufficient cyber expertise and the ability to rapidly implement countermeasures and allocate financial resources. The cyber domain must get rid of partial optimisation and rigidity caused by silo structures in management.

The conclusion is that the speed with which the cyber domain is changing, including its complexity (FIG 3), requires a new kind of networked approach that relies on strong coordination and common rules. The action must be able to combine the benefits of centralisation and decentralisation, i.e. strong coordination and quick reaction that emerges from local ownership.

Finland, generally speaking, has excellent chances of becoming a global forerunner of cyber security and the novel approach it entails. Our undisputed fortes include strong competence, a tradition of both intersectoral and public-private cooperation as well as well-defined processes and division of duties between different actors (see the Security Strategy for Society).

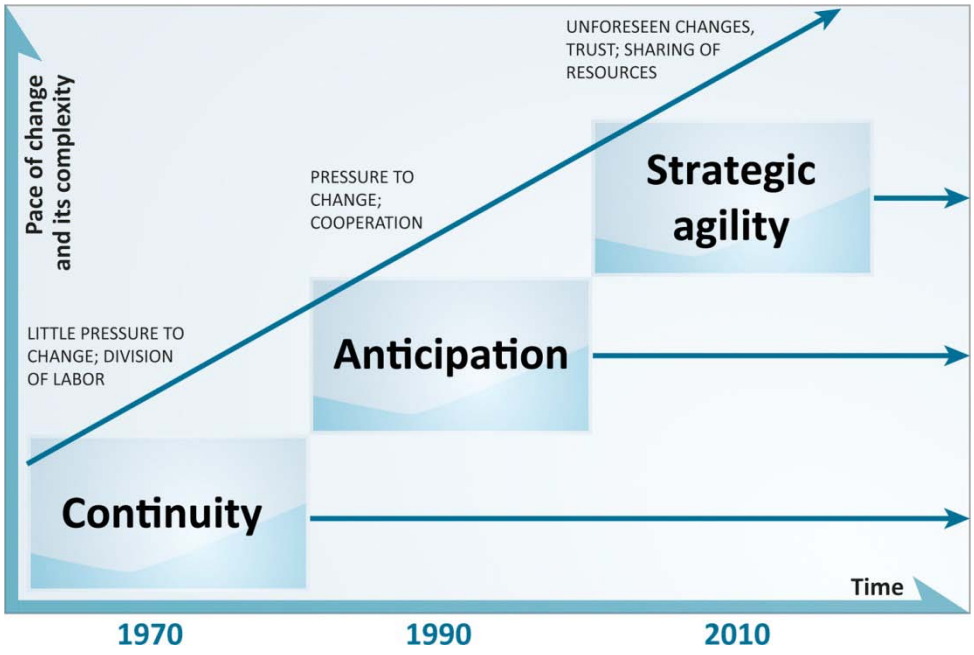

FIGURE 3. Strategic agility

3.2 Management of disturbances endangering society

As the vulnerability of society increases it is necessary to be able to rapidly start managing sudden disturbances in the cyber domain, aka cyber incidents. Cyber incidents typically have wide-ranging impacts. Therefore, it is necessary to provide the broadest possible intersectoral support to the competent authorities, when required. Concurrently, in spite of the disturbances, the viability of society must be secured in an appropriate manner.

Cyber incident management will follow the rule of law and the existing division of duties. The same cyber incident management principles that are used in normal conditions will be applied in emergency conditions. The authorities' division of duties and the *modi operandi* of the cooperation bodies will remain as they are in normal conditions. Situation management will be proactive and the needed resources will be brought online at once. The competent authority is in charge of operations, supported by intersectoral cooperation bodies. The competent authority is also responsible for communications. The other authorities, businesses and organisations will participate in the management of the situation as required. Along with operational activity in situation management, it is essential to ensure the flow of communication and provide sufficient information to the state leadership.

Disturbance management will be organised and implemented in accordance with the Security Strategy for Society. In line with the Strategy, the competent authority launches the action needed in managing the disturbance, informs the other authorities and actors as appropriate, and brings in the other actors needed for situation management. Cyber incident management encompasses four elements: contingency planning, compilation of a situation picture, countermeasures and recovery.

4. SECURING THE VITAL FUNCTIONS OF SOCIETY AGAINST CYBER THREATS

4.1 Cyber situation awareness and setting up the Cyber Security Centre

Improve comprehensive cyber security situation awareness among the key actors that participate in securing the vital functions of society. Establish a Cyber Security Centre, supported by a cooperative network of actors.

The decision-making process of the state leadership and the authorities requires sufficient situation awareness. The various actors need to have a reliable, real-time cyber security situation picture on the state of society's vital functions and the disturbances that are affecting them. The real-time cyber security situation picture does not only comprise information from technical monitoring and control, it also includes an analysis that amalgamates observations, intelligence, other information gathering and previous lessons-learned.

The national Cyber Security Centre will be set up to serve the authorities, the business community and other actors in maintaining and developing cyber security. The Centre's arrangements and services will be implemented as part of the integrated cyber security strategy action plan. The primary service of the Centre will entail the compilation, maintenance and dissemination of the situation picture in close cooperation with its support network. The Cyber Security Centre will be founded by merging the functions of the present CERT-FI and the planned GOV-CERT, and by earmarking the needed additional resources for its operation. The Centre will be supported by a functional network that encompasses all pertinent authorities, businesses and other separately designated actors tasked to prepare and respond to cyber security violations.

As the Cyber Security Centre is being established, other parallel projects will be taken into consideration in order to streamline and improve situation picture arrangements. The Government Resolution on Enhancing Information Security in Central Government provides guidelines for 24/7 ICT security arrangements in the central government. The planning and implementation of this function will be coordinated with the operations of the Cyber Security Centre. Furthermore, when it comes to the compilation of the situation picture, the central government's joint ICT projects, such as the security network (TUVE) venture, will be taken into consideration.

The Cyber Security Centre will:

1. Compile and disseminate the cyber security situation picture
2. Compile and maintain a cyber threat risk analysis, in conjunction with different administrative branches and actors
3. Support the competent authorities and actors in the private sector in the management of widespread cyber incidents
4. Intensify cooperation and support the development of expertise.

The most important service of the Cyber Security Centre is to compile, maintain and distribute the cyber security situation picture to those who need it. The compilation of the situation picture requires the ability to collect and analyse relevant information and to meet the information requirements of different actors. The integrated situation picture, compiled by the Cyber Security Centre and its support network, comprises a technical situation picture and an evaluation of the total consequences of the cyber security violations to the vital functions of society. The Cyber Security Centre and different actors will determine their respective information requirements. The information on vulnerabilities provided to network administrators will become more automatic; whereas, the content of the situation picture intended for the authorities and decision-makers will be developed more towards being an analysis of the consequences of the effects on society's vital functions.

Cyber incident damage control is the responsibility of the authorities and businesses that the disturbance concerns. The Cyber Security Centre can support the lead authority in managing widespread cyber incidents that concurrently impact many authorities or businesses. The

Cyber Security Centre generates an overall cyber security situation assessment built on its integrated cyber security situation picture. The purpose of such a briefing is to support the administrative branches in their cyber preparedness arrangements and contingency planning.

The Cyber Security Centre monitors and analyses cyber threats and, together with its international partners, generates forecasts on their consequences to Finland. In accordance with its monitoring activities, the threat scenarios of the Security Strategy for Society, the cyber threat scenario and real-time national intelligence information, the Cyber Security Centre alerts businesses and authorities critical to the vital functions of society concerning new cyber threats to Finland and increased cyber threat levels and, upon request, assists them in contingency planning.

The Government Situation Centre (GOVSITCEN) compiles the situation picture for the state leadership. Close cooperation between the GOVSITCEN and the Cyber Security Centre improves intersectoral monitoring and analysis capabilities, on which the integrated situation picture relies. Integrated situation awareness makes it possible to appropriately respond to threats at political and operational levels.

The Ministry of Transport and Communications is responsible for the performance guidance of the Cyber Security Centre. In order to guarantee the performance guidance a separate cyber security working group will be established. The participants of the group will include all service providers, users and facilitators of the Cyber Security Centre. The members of the working group must be experts in their respective fields, with extensive knowledge of their organisation's preparedness, and of the state and requirements of their cyber security situation.

4.2 Guaranteeing the preconditions of the business community; security of supply.

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 business community's continuity management.

The goal is to guarantee, also during ongoing cyber incidents, the continued operations of businesses that are vital to society. Continuity management planning in the business community will be supported when it can have impact on vital functions and the creation of a safe cyber domain. The security of supply organisation plays a central role in securing the conditions of the business community. Contingency planning will ensure the functioning of infrastructure crucial to the viability of society, and the continuation of critical production capabilities in all situations.

Society's critical production processes are increasingly dependent on automation. The development cycles of automation systems are long, and they are associated with rapidly

developing IT solutions. When it comes to continuity management in critical infrastructure, data protection arrangements in automation systems must also be addressed. The connections between equipment in the physical world and networks must be designed in such a manner that no simple cyber attack can bring a plant or unit down. Regarding society's vital functions it is imperative to minimise the vulnerabilities of automation systems, such as building automation, remote operations and remote reading.

Most of the modern critical infrastructure, including services, is owned and generated by the private sector. The prerequisites companies need to see to the continuation of their business operations during cyber threat situations is being improved, thereby increasing confidence in the continued supply of their products .

The security of supply organisation is a network which maintains and develops the security of supply in Finland as a public-private partnership. Security of supply is built on a well-functioning market and a competitive economy. Society's economic and technological basic functions are being prepared so that they can be sustained by various security of supply-measures that supplement free enterprise during different disturbances and emergency conditions.

Measures that support the continuity of businesses critical to Finland's security of supply will be outlined and carried out as part of the Government Decision on Safeguarding the Security of Supply, including its implementation. An individual organisation normally implements cyber preparedness through the traditional means, methods and structures of information security. Companies should be better prepared to evaluate the risks and consequences of cyber attacks as well as the required action. The capability for conducting analyses and assessments of various functional chains and networks will be improved, and awareness of network operations and security of supply will be increased. Cyber defence requires that actors operate under identical or compatible protection practices. The security of supply organisation provides instruments to critical businesses which make it easier for them to carry out risk assessments and develop their continuity management.

By virtue of its good cyber security situation Finland can also be a lucrative target for investment. Whereas the public sector is tasked with the creation of a safe and efficient operating environment, it is the responsibility of the private sector to develop business models, products and services. The aim is to establish an internationally renowned cyber security cluster. Close international contacts guarantee a sound knowledge base and facilitate internationally networked business operations.

Various national development projects run by Tekes (Finnish Funding Agency for Technology and Innovation) or Tivit (Strategic Centre for Science, Technology and Innovation in the Field of ICT), among others, must clearly shift their focus towards new business and research supporting cyber defence. For example, one focus area of the Cloud Software program laboratory, commencing its operation in 2013, must be aimed at the development of new cyber defence services.

Business security is implemented by countering illicit economic intelligence and cyber espionage and by reducing intellectual capital risks. In order to bolster the domestic information security sector the central government will increase investment in R&D and education, and intensify the internal development of its administrative agencies. The National Communications Security Authority will become a renowned authority in providing international information security certifications.

4.3 Cybercrime prevention

Make certain that the police have sufficient capabilities to prevent, expose and solve cybercrime.

The police must be able to identify and prevent the planning, financing and directing of terrorist crime and other crime in networks that endanger society, and be able to solve the suspected crimes.

IT crime has become an extremely noteworthy sector of crime with its consequences extending to states, individuals and businesses alike. IT networks provide an increasingly lucrative and, regarding the risk-benefit and damage ratio, ever more attractive environment for committing crimes that have financial or terrorist goals. Traditional organised crime, too, takes advantage of the vulnerabilities of networks and ICT systems. Cyber attacks can be employed to endanger society's critical infrastructure and carry out terrorist strikes. In addition to terrorism, traditional crime, such as fraud, sexual exploitation of children and industrial espionage, is increasing its presence in the cyber domain.

In general the police, being the competent authority in preventing and investigating crime and in taking cases to the prosecutors, cooperate with the other law enforcement authorities. Cybercrime is time and again transboundary in nature and its investigation often demands international police and judicial cooperation. Judicial cooperation is needed, among other things, to obtain evidence or for the extradition of suspects.

It must be ensured that the police have sufficient powers, competences and rights to information when it comes to exposing and preventing cybercrime as well as identifying criminals operating in cyberspace, and solving these crimes. Likewise, it must be ensured that the police have sufficient powers, competences and rights to information when it comes to identifying and preventing the planning, financing and directing of terrorist crime in networks and other crimes that endangers society, including associated propaganda and preparing the ground for criminal activity, and the capability to solve the suspected crimes.

The police will establish the competence, capacity and appropriate legal powers to exchange information and cooperate with other law enforcement authorities in preventing, identifying and solving crimes. As part of organised crime prevention the police shall invest in cybercrime prevention. The police will develop and bolster national IT crime prevention techniques by

increasing cooperation between different police forces, including their rapid response capabilities.

In accordance with the order of the National Police Board, the National Bureau of Investigation maintains a situation picture of international and organised crime. Moreover, the National Bureau of Investigation, together with the local police, maintains an integrated crime situation picture. The joint PCB (Police, Customs and the Border Guard) authorities' criminal intelligence and investigation centre is utilised in the compilation of the situation picture. The Finnish Security Intelligence Service maintains a situation picture of its field of activities.

It must be ensured that the police have sufficient and motivated personnel and that they are capable of tactical police investigations of demanding IT crime and for processing and analysing digital evidence in a legally certain manner. The competence of the authorities, prosecutors and judges involved in the prevention and investigation of cybercrime is improved by developing the pertinent education of the field.

4.4 Cyber defence capability

The Finnish Defence Forces will create a comprehensive cyber defence capability for their statutory tasks.

Cyber intelligence, cyber warfare and protection capabilities create the cyber defence capability. The goal is to customise the capability so that it will best support the Defence Forces' activities in protecting the territorial integrity and in national defence. Cyber defence will be implemented as an entity which comprises the capabilities of the Defence Forces, other authorities and the rest of society.

A credible capability is achieved by cooperating with the other authorities, businesses and universities. In normal conditions the capability will be improved by networking, exchanging information and participating in joint projects, national and international working groups and exercises. The basic approach will remain unchanged in emergency conditions and during disturbances. Cyber preparedness and threat management is achieved by maintaining and developing various defence and counterattack techniques. Furthermore, an appropriate recovery capability from cyber attacks will be established.

Cyber warfare can be used as an instrument of political and economic influence, and in a serious crisis it can be used along with traditional means of military force. The Defence Forces will protect their own systems and networks; they will also create and maintain cyber intelligence and cyber warfare capabilities. The development of these capabilities will be determined by the associated performance requirements and available resources.

Emerging cyber threats must be identified early on, and it must be possible to monitor the phenomena and events in cyberspace in real time. This requires the compilation of a cyber situation picture so as to enable early warning and allow for preparations and the

implementation of measures. The Defence Forces and the future Cyber Security Centre will cooperate with each other in the compilation of the cyber situation picture.

Intelligence capabilities yield information on networks, including their vulnerabilities, and cyberspace actors, and provide assessments of their ability to carry out cyber operations. The goal of cyber intelligence is to establish the kind of situation awareness and intelligence information that protection and cyber warfare require.

The national cyber defence capability will be developed by cooperating with the other authorities, the business community, the scientific community and other actors. National coordination, the compilation of an integrated situation picture and the provision of the requisites of cooperation demand regularly exchanged information between the different actors.

International cyber defence cooperation will be further intensified between the key actors. Such cooperation is built on bilateral agreements and multilateral collaboration. The purpose of international cooperation is to facilitate the regular exchange of information between different actors and, in particular, to develop domestic capacities and harmonise procedures.

The Defence Forces will provide executive assistance to the other authorities with regard to disturbances caused by cyber incidents. If required, the other authorities will support the Defence Forces in the implementation of cyber defence. The Defence Forces' capacity to support the other authorities during cyber incidents will be improved.

The options and powers related to cyber warfare capabilities require a thorough further review. This review must incorporate the applicability and adequacy of existing international law and national regulation, and the requirements of cyber defence capabilities, if any.

Sufficient powers, competence and the right to information will be given to the Defence Forces for the implementation of national defence, executive assistance, territorial surveillance and crisis management tasks.

4.5 International cooperation

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 national cyber security – integrated situation awareness, effective disturbance management and threat prevention – is nationally achieved through active cooperation between the different actors. Due to the wide-ranging nature of cyber security the importance of international cooperation is ever more emphasised. The goal of international cooperation is to exchange information and experiences, and to learn from best practices so as to raise the level of national cyber security.

International cyber security cooperation occurs at several levels and fora: in the Nordic context, the European Council, the European Union, and in international organisations such as NATO, the OSCE and the UN. Cyber threats are transboundary threats and, therefore, they require international cooperation in various international fora. Such cooperation provides an opportunity for exchanging information and learning from best practices. Furthermore, it provides benchmarks for the development of national cyber security as part of global cyber security and also increases the interoperability and compatibility of cyber defence.

Cooperation is implemented between different organisations and at the international level. When it comes to organisations, the EU and NATO are the key cyber security actors. Cooperation with them primarily entails the exchange of situational information, cooperation in the development of capabilities and in training and exercises.

Traditional Nordic cooperation also provides an opportunity for the advancement of cyber security. Closer Nordic cyber security cooperation was agreed on at the Nordic foreign ministers' meeting in 2009. As per the recommendations of the expert working group a Nordic authorities' cooperative network, which includes an associated secure network, is being planned.

The 2001 Convention on Cybercrime of the Council of Europe (aka the Budapest Convention) lays the groundwork for the prevention of all cybercrime. The European Union is also a very important venue as regards Finland's cyber security development. The EU is presently planning its very own cyber security strategy. At the moment the EU's guidelines and directives focus on cybercrime prevention, protection of critical IT infrastructure as well as legislative work on electronic communications, data security and data protection.

Finland continues its close cooperation with European cooperative organisations such as the European Network and Information Security Agency (ENISA); the European law enforcement agency Europol; the Body of European Regulators for Electronic Communications (BEREC); the European Forum for Member States (EFMS), which is an intergovernmental cooperative forum for the protection of Europe's critical infrastructure; and the European Public-Private Partnership for resilience (EP3R,) which deals with the robustness of ICT systems.

As cyber defence is being developed, cooperation with the EU Military Staff (EUMS), the European Defence Agency (EDA) and NATO will continue. NATO continues to cooperate with its partner countries in responding to new security challenges, supporting NATO-led operations and improving situation awareness.

The Organization for Security and Co-operation in Europe (OSCE) aims to improve confidence-building measures for the prevention of cyber conflicts by increasing transparency, cooperation and stability. The goal of this cooperation, built on the OSCE's comprehensive concept of security, is to complement the efforts of other international organisations.

UN Member States commit to increasing confidence and security in the use of ICTs in the outcome documents of the World Summit on the Information Society (WSIS). Finland participates in the cyber security debate which is being conducted in UN bodies and, in accordance with its WSIS obligations, supports the strengthening of cooperation between all actors as regards security-related topics. The International Telecommunication Union (ITU) also promotes this objective through its Global Cybersecurity Agenda initiative.

The work carried out within the Organisation for Economic Co-operation and Development (OECD) aims to develop or harmonise the policies of its Member States in various sectors of the economy or society. Finland participates in the OECD's data security and protection-of-privacy roundtables. The OECD is an expert organisation that supports its Member States' decision-making in economic and social policy. The OECD has issued recommendations on the security principles of IT systems and networks, and carried out comparative studies on its Member States' national cyber security strategies.

4.6 Improving research and competence; exercises

Improve cyber expertise and awareness of all societal actors.

Regarding the importance of cyber security to society, the goal is to improve understanding, competence and skills among the authorities, the business community and citizens and create a strong national cluster of cyber know-how. Cyber security research will be developed as part of national top-level research and a strategic cyber security centre of excellence will be established at already existing structures. The purpose of exercises is to improve the participants' ability to identify vulnerabilities in their activities and systems, and to improve their skills and train their personnel. Different sectors regularly test their preparedness when it comes to managing disturbances in vital functions.

The most cost-effective way to advance national cyber security is to improve competence. Increasing cyber risk awareness among the authorities, the business community and citizens will improve everybody's skills in the implementation of cyber security measures. Top-level research in this field will lay the foundation for developing competence and cyber security systems.

The Finnish education system will see to the preservation and development of such top-level competence which can be utilised in ensuring and improving the security of society's vital functions in the cyber domain. The study of basic cyber security skills must be included at all levels of education. The learning requirements of cyber security must be included on the curricula of basic education (comprehensive school), vocational upper secondary education, general upper secondary education and higher education.

Universities will bolster the requisites of basic research, applied research and innovation in cyber security, while universities of applied science will improve the preconditions of product development. The level of cyber security research will be raised and its research conditions will

be guaranteed so that basic and applied research can continually generate cutting-edge innovation and scientific breakthroughs. The development of cryptology skills, among other things, will be supported so that Finland can supply related products and services to national and international users.

An interdisciplinary, strategic cyber security centre of excellence will be established at the existing ICT-SHOK (TIVIT)[1]. It will provide an opportunity for top-level research teams and companies that utilise the results to engage in effective mutual cooperation over the long term. The centre of excellence will employ an application-oriented and interdisciplinary research strategy which companies, universities and research establishments have together defined. The results of that strategy will serve the implementation of the national Cyber Security Strategy, and the development of international-level top-expertise. These measures will support the creation of new and successful international cyber security business.

From the standpoint of continuous business growth it is imperative to retain top-level competence in Finland. This will make it possible for us to take advantage of the cyber domain. Judging by the needs of the business community, one to two educational establishments, together, should retrain at least 100 persons in this sector in 2013. Transition training will continue at the same level for several years ahead. Additional cyber/information security courses will be provided by universities and polytechnics as soon as possible. Educational establishments that provide training in the field will provide more IT security study places as well as secondary fields of study in cyber security. A professorship in cyber security will be established as soon as possible and, in the long run, the number of professors in cyber security will be increased.

Lessons-learned from cyber exercises provide concrete information on securing the vital functions of society, including required cooperation. In addition, they provide information on the development needs required by the strategic tasks of administrative branches and organisations, and the total situation of society's preparedness and crisis management capabilities. Exercises help test the basic principles and *modi operandi* of the Cyber Security Strategy; they also measure the implementation of the Strategy.

Preparedness for emergency conditions and serious disturbances in normal conditions must be exercised on a regular basis. This makes it possible to analyse how well cyber security is being achieved in Finland and to continually introduce improvements. Cyber threats have very short mutation cycles and, therefore, all national and international exercises must be frequent and well-organised so as to effectively support national cyber security.

Successful cyber exercises call for a systematic approach and clear lines of authority. The preparation and implementation of large national cyber exercises will be coordinated in accordance with the principles of the Security Strategy for Society. The implementation of

[1] The Strategic Centre for Science, Technology and Innovation in the Field of ICT

national cyber security entails close public-private cooperation. Businesses and NGOs that are important to society's vital functions will be included in exercises so as to improve society's comprehensive preparedness.

Public and private sector preparedness for cyber incident management will be trained in national cyber exercises which test the preparedness required by cyber incidents included in the Cyber Security Strategy' threat scenarios, and the functioning of management and cooperation arrangements. Exercise themes will incorporate topical challenges caused by changes in the cyber domain.

Participation in international multi-level exercises significantly supports the development of national cyber security, know-how in the field, practices, the creation of transnational inter-authority cooperation and a network of experts. Already during the planning stages Finland must actively try to influence the structures and running of exercises so that they advance the development of our national competence, and so that we can test the strengths and weaknesses of our national cyber domain.

5. CYBER SECURITY REGULATION

Secure the preconditions for the implementation of effective cyber security measures through national legislation.

Cyber security is a new legal phenomenon. Cyber threats are transboundary by nature. The actors behind cyber attacks may vary and are difficult to identify. Cyber attack techniques are versatile, rapidly changing and evolving. Cyber security concerns all walks of life, administrative branches and vital functions of society. Basic rights and human rights guarantee the right to privacy and confidentiality of communications. The origin and nature of the cyber threat determines the body of law that will govern the cyber incident.

5.1 International and national cyber security regulation

In the 1990s the United Nations (UN) recognised the criminal misuse of information technology as a cross-border crime. The UN has issued resolutions in the fight against the misuse of information technology and for the protection of critical IT infrastructure.

The European Union has drafted conventions, framework decisions, directives, proposals and communications on IT crime and its prevention, cooperation in the defence of attacks against information systems, and the protection of critical infrastructure and IT infrastructure.

No uniform international treaty exists which covers all cyber threat situations and is binding on all states. International law handles cyber incidents in a fragmented manner and approaches them from different viewpoints. Likewise, no consensus exists on terms such as cyber attack, cyber defence or cyber conflict/skirmish. There has been more international legal debate on

this complex topic in recent years. This will probably result in new legal interpretations on the assessment of cyber incidents at the state level or in international organisations. Presumably, these interpretations will not be legally binding on states, but, they will indicate the objectives which the states participating in the arrangements are prepared to adopt.

The UN Charter regulates the use of force in state relations. Apart from self-defence in the event of an armed attack or participation in Security Council-mandated military action, the use of force is forbidden. At present, the international community is debating whether cyber attacks in some situations can rise above the threshold of armed attack, as defined in the UN Charter, justifying a military response by the affected state. Sovereignty also includes responsibility. A state must see to it that its area will not be used in an attack against another state. It must, therefore, also try to prevent attacks beyond its national borders perpetrated by private entities. No rules of engagement exist for cyber operations.

No uniform cyber threat regulation exists in national legislation. Standards that address operations in IT networks are fragmented, and they approach cyber threats from different angles. Even though cyber operations by their very nature cross the boundaries of administrative branches, at the national level administrative branches define cyber threats from their own perspective. Moreover, powers also tend to be branch-specific. Depending on its origin and scope, a cyber threat can be considered to be an individual criminal act, a wider terrorist offence or an issue affecting state relations and military defence. This hampers the achievement of legal rulings and a consistent, national legal interpretation of the situation.

Pursuant to the Constitution of Finland the public authorities shall guarantee the observance of basic rights and liberties, and human rights. Basic rights must also be guaranteed in networks. Increased cyber security may improve, for instance, the protection of the privacy and property of network users. Well-functioning ICT networks can also be seen to promote the freedom of speech. More detailed cyber security-related regulation can be found in Chapter 34 of the Criminal Code, the Territorial Surveillance Act, the Readiness Act, the State of Defence Act and the Act on the Defence Forces, the Communications Market Act and the Act on the Protection of Privacy in Electronic Communications.

The obligation of the authorities to be prepared to discharge their duties well in all situations, as per the Readiness Act, also includes the development of cyber capabilities. The key requirement for invoking and using the powers of the Readiness Act is subject to the existence of emergency conditions, as provided by law. Pursuant to the justifications of the Act, an attack (according to the definition of emergency conditions) comparable to an armed attack may also mean an attack other than one implemented with traditional means of force. For instance, it can entail an attack against IT systems. An attack can also mean one executed by non-state actors, if it is so organised and wide-ranging that it can be likened to an attack carried out by a state.

5.2 Improving legislation

In its international action Finland supports and participates in interpretations of international law aimed at harmonising to the greatest possible extent the legal doctrines of different states. At the same time, this means that it is not sufficient to only adapt Finland's legislation to cover cyber threat situations. Finland actively participates in cooperation between different actors which aims for the transparent exchange of information, a common body of law and the division of duties between different actors. This can, among other things, limit situations in which discrepancies in national laws provide an opportunity for cybercriminals to carry out their activity in suitable states.

National law should be considered from the perspective of international cyber security-related legislation and EU legislation. This work must ascertain the different administrative branches' cyber security regulation, how modern and sufficient it is, and the need for legislative review, if any. The point of departure is that the powers required for managing cyber incidents which endanger and harm society must be included in the authorities' normal powers. The Constitution lays down that the exercise of public powers shall be based on an Act.

Legislation must be developed in such a manner that it adapts to rapidly changing phenomena in cyberspace, and makes it possible for the competent authorities in the different sectors to discharge their duties in protecting the sovereignty of the state and the livelihood of the population, and in defending society's vital functions against cyber threats. Cyber security must be regarded as an integral element of security. When it comes to the viability of society it is imperative to find a suitable balance between legislation and situation awareness, the responsibilities and practices of the authorities and the business community. This analysis must also take into account Finland's international competitiveness. A stable cyber security situation, for its part, creates a lucrative business environment.

In order to repel cyber threats that endanger the security of the state, possible legislative restrictions and hurdles, as well as those arising from international obligations, will be reviewed. Such restrictions and hurdles also include obligations related to data protection and those found to be useful for effective cyber defence purposes that impede the obtainability, disclosure and exchange of information between the different authorities and other actors. When it comes to assessing information-gathering and other data processing one should also estimate whether the competent authorities should be given better possibilities for gathering information, data processing or being informed of cyber threats and their sources, while simultaneously paying attention to the basic rights of privacy and confidentiality in electronic communications.

With regard to police activities, it is especially important to obtain the powers for intelligence gathering and investigation in order to prevent, identify and fend off cybercrime. The rules on jurisdiction related to cyber warfare and cyber intelligence should be clarified and improved in the review of legislation on the Defence Forces. Should the rules on jurisdiction be expanded,

special consideration must be paid to human and basic rights, and to their impact on the rules on jurisdiction, for instance, when intelligence-gathering powers are being expanded.

6. IMPLEMENTATION OF THE CYBER SECURITY STRATEGY

6.1 Principles of implementing the Strategy

Assign cyber security related tasks, service models and common cyber security management standards to the authorities and actors in the business community.

The cyber security of society and the securing of its vital functions rely on the strategic tasks of the ministries and a well-functioning security of supply in all situations. Each administrative branch is responsible for the preparation of its cyber risk analysis. The analysis process makes it possible to identify vulnerabilities and complete a maturity analysis. The process culminates in the completion of action plans for each administrative branch which meet their designated requirements.

The metrics and actions needed for improving cyber security will be determined through a more detailed analysis. Contingency plans and preparedness arrangements must regularly be reviewed, especially when major changes occur in society or in the security environment. The future Security Committee will monitor and coordinate the implementation and development of the Strategy.

In addition, each actor or sector in society has distinct cyber security tasks. These specific tasks expand the strategic tasks defined in the Security Strategy for Society, those related to security of supply and sector-specific tasks from the perspective of cyber security.

Maintaining society's cyber security demands accurate information on the preparedness and capacity of the administrative branches and the business community, as well as the crisis resilience and preparedness of society in general. The monitoring of the Strategy must enable timely and correct maintenance and development measures. Such monitoring provides the state leadership with up-to-date information regarding the correct allocation of resources in line with the goals of the Cyber Security Strategy.

The implementation of cyber security also requires the consistent application of the Strategy's principles at the regional and local levels. This calls for adequate cooperation between the different actors and the utilisation of best practices.

The future Security Committee will coordinate the joint monitoring and development of the implementation of the Strategy. The Committee will prepare annual reports on the state of the Strategy's implementation.

6.2 Required measures

Ministries will monitor the implementation and development of cyber security-related tasks and the security of supply-measures. The administrative branches will carry out the monitoring as part of their routine practices.

The Cyber Security Centre, together with its network, will regularly prepare cyber incident reports for the different authorities. The Centre and its support network will prepare annual reports on, at least, the following topics:

- How the cyber incidents were managed, including the lessons-learned, analyses and the economic impacts on society's vital functions,
- Estimates on the viability and further requirements of contingency arrangements,
- Lessons-learned from the administrative branches', the Government's and national cyber readiness exercises, and
- The improvement of action and competence-building and resource allocation.

When it comes to cyber incident management, it is important that all action launched for the purpose of situation management be carefully recorded and analysed. In addition, the analysis of 'close calls' must also be included in this tracking, especially for the purpose of preventing threats and risks. Lessons-learned and the measures they spawned will be discussed in different cooperative bodies so as to ensure the utilisation of best practices.

The observations and experiences from cyber exercises provide tangible information as regards securing the vital functions of society, including the necessary cooperation. Furthermore, they provide information on the development needs required by the strategic tasks of the administrative branches and organisations, and on the overall situation of society's preparedness and crisis management capabilities. Exercises test the principles and approaches of the Cyber Security Strategy, and help assess the implementation of the Strategy.

Monitoring the implementation of the Strategy also provides criteria and requirements for cyber security research, including national R&D cooperation. National and international security research will be implemented and its cooperative arrangements will be developed in line with the guidelines of the National Security Research Strategy (2009). Research that supports the Cyber Security Strategy is conducted at various research units and establishments, and through the research programmes of universities and other institutes of higher education.

The maintenance and development of the Cyber Security Strategy rely on a continuous improvement process. The Cyber Security Strategy will be annually reviewed by the future Security Committee. This will ensure the relevance and the continued progress of the Strategy. Any possible updates to the Strategy and the Action Plan will be carried out on the basis of an

analysis generated by the process. The salient points of the Cyber Security Strategy will be incorporated into the Security Strategy for Society the next time it is updated.

6.3 Resource allocation

Ministries, government agencies and establishments are to include the resources for the implementation of the Cyber Security Strategy in their operating and financial plans. Parliament will assign spending limits to the ministries, in which the resources required by cyber security measures will be included. Ministries will incorporate resource requirements in their normal operating plans. Businesses will take cyber security requirements into account as they make decisions on their budgets and resource allocation.

A separate supplementary appropriation will be earmarked for setting up the Cyber Security Centre, including its operation. The sum total of the appropriation will be determined in the joint implementation plan. The Centre will be able to operate on a 24/7 basis which, according to preliminary plans will require the additional resources of approximately ten person-years and at least one million Euros.

6.4 Action Plan and assessing effectiveness

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

Phase 1 of the Cyber Security Strategy will be put into practice during 2013-2015. Detailed contingency and development plans for cyber security will be prepared in that period so as to achieve by 2016 the Government Programme's target that Finland become a leading country in the development of cyber security. From 2016 on the Cyber Security Strategy will be implemented in line with the principles of continuous improvement. Administrative branches will implement the budgeting required by cyber security in accordance with existing guidelines.

The key features of the Action Plan include the establishment of the Cyber Security Centre, the ministries' measures for the purpose of achieving their strategic goals, and the required legislative review. A cyber security maturity model will be developed as part of the Action Plan with which the level and development of the actions can be benchmarked.

APPENDIX

THE CYBER SECURITY STRATEGY'S CONTINUOUS IMPROVEMENT PROCESS

The goal of the national cyber strategy process is to achieve a continuous improvement approach which will make it possible to more efficiently and effectively implement cyber security measures. The strategy process manifests itself at several levels and it includes different phases. The goal is to create a continuous strategy process with parts that regularly repeat and generate continuous improvement.

The cyber security process encompasses five phases:

Analysis
The Strategy's analysis phase defines our own position, i.e. our state in relation to the operating environment and its various elements. In the cyber strategy this translates into an analysis of the cyber threat environment and identification of vulnerabilities in society's vital functions, along with a risk assessment of the ensuing entirety. Moreover, one's own capabilities and shortcomings will be assessed.

The operating environment analysis will identify phenomena in cyberspace, assign the necessary definitions for the Strategy and catalogue the existing national cyber security projects, including related and ancillary projects.

Information from other countries' cyber security strategies and the best practices most suitable for us will be obtained through benchmarking.

The analysis will result in awareness of our standing in both the national and international cyber domain; it will also provide further grounds for definitions and reports.

Planning
The cyber security vision, national standards and the cyber security concept will be determined in the planning phase. This phase will take into account performance requirements, available economic resources and competence. Several options will be prepared as regards achieving the desired end state.

Decision
In the decision-making phase several options will be compared and the option leading to the desired end state will be selected as will be the national operating concept and the measures it requires. In addition, the desired cyber capabilities and the measures required to create them will be defined.

Production
The production phase will determine the structure of the Cyber Security Strategy, the manner in which things are presented, and the concrete goals and responsibilities of cyber security.

The production phase includes several iterations; mid-reviews will ensure that the strategic decisions appear in the text. The drafting of the Strategy is completed when it is presented to the commissioning body and is approved.

Implementation

The previous phases of the strategy process will have produced an approved strategy document which also includes an action plan as well as a plan for continuously keeping the strategy process relevant. In its implementation phase the strategy will be put into practice by delegating the proposed action of the strategy at the different levels of administration and organisations. A benchmarking and monitoring system for cyber security maturity will be created for the purpose of change management, which can then be used to monitor the success of the process. The future Security Committee will monitor the implementation of the Strategy. It will also prepare an annual report for the Government.

Developments in the cyber domain will be monitored in the implementation phase and, if necessary, administrative branches will be supported in putting the Strategy's principles into practice. The goal is to maintain a comprehensive cyber security situation picture, and to track the development of countermeasure capabilities.

Resource allocation is an important part of the implementation of the Strategy. Efficiency and effectiveness are directly attributable to the available economic and intellectual resources. The Government creates the framework for cyber security resource allocation through budget steering. Accountable departments, within the constraints of their budgetary power, will allocate resources for the practical implementation of cyber security, such as the compilation of a situation picture, contingency planning, research and development, and education.

The cyber security process is a process of continuous improvement and it is used to track changing conditions and the effectiveness of action. Consequently, the process will incorporate analyses and, when necessary, updates of the Strategy.

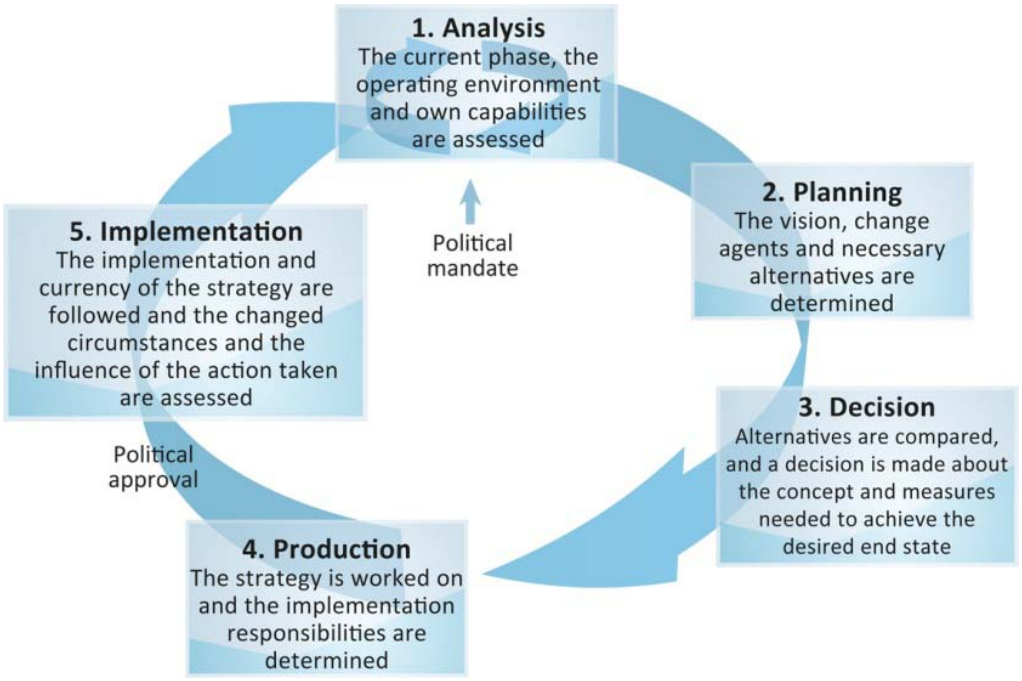

FIGURE 1 The continuous improvement process of cyber security.