Unofficial translation
Ministry of Defence, Finland
March 2015

GUIDELINES FOR DEVELOPING FINNISH INTELLIGENCE LEGISLATION

Working group report

MINISTRY OF DEFENCE

DESCRIPTION
14.1.2015

Authors	**Type of publication**	Working group report
Working group for developing legislation on intelligence Hanna Nordström (chair) Katriina Laitinen (vice-chair) Mika Lundelin (member of the working group) Jenni Herrala (secretary) Jan Sjöblom (secretary) Kosti Honkanen (secretary) Minnamaria Nurminen (secretary)	**Contracted by**	Ministry of Defence
	Working group nominated on	13.12.2013

Name of publication
Guidelines for developing Finnish intelligence legislation. Working group report.

The publication is available on the internet at **www.defmin.fi**

Summary
The report assesses the need to develop legislation governing intelligence work.

When the authorities responsible for national security collect information in the cyber domain to identify serious threats, their work is by its very nature intelligence work. However, existing Finnish legislation does not provide for intelligence work. The working group therefore proposes that the Government should initiate necessary measures to create a legal basis for intelligence work.

The purpose would be to collect vital information to protect national security against serious international threats, military or civilian in nature. Intelligence work would ensure that the senior government leadership is able to base its decision-making on timely and reliable information and that the competent authorities are able to take measures to combat threats.

The military and civilian authorities responsible for national security should be granted powers to conduct cross-border intelligence to respond to changes in the security environment. It would be practical to assign the technical execution of telecommunications intelligence to a single authority.

It is to be considered whether the Defence Forces and the Finnish Security Intelligence Service should be authorised to conduct foreign intelligence to gather information from individuals and on information systems. The policies of the government leadership should be taken into account when making decisions on conducting foreign intelligence, as this is related to sensitive foreign-policy elements. Responsibility and steering issues must be assessed if legislative drafting is begun.

An independent authorisation process should be part of telecommunications intelligence. An independent oversight system should also be created for the purposes of foreign intelligence and telecommunications intelligence.

The protection of confidential communications, provided for as a fundamental and human right, should be given special attention when the drafting of legislation on telecommunications is considered. With the possible exception of telecommunications intelligence conducted in a foreign country, it would appear that it will not be possible to draft legislation relating to telecommunications interception and access without amending the Constitution.

Key words:
legislation, intelligence, Finnish Security Intelligence Service, Defence Forces, police, telecommunications

Other information (HARE number, other reference):
HARE PLM004:00/2013

		ISSN	**ISBN**
Number of pages	**Language** Finnish		**Degree of confidentiality** public
Distributed by		**Published by** Ministry of Defence	

Unofficial translation
Ministry of Defence, Finland
March 2015

Unofficial translation
Ministry of Defence, Finland
March 2015

To the Ministry of Defence

On 13 December 2013, the Ministry of Defence appointed a working group to develop legislation to improve the capability of the security authorities to gather intelligence concerning threats in the cyber environment. The working group was required to report by 30 June 2014.

On 27 May 2014, the Ministry of Defence extended the reporting deadline of the working group to 31 December 2014.

The task of the working group was to assess needs for legislative development so as to ensure that Finnish national security can be safeguarded against threats in cyber networks.

The working group was also assigned to compile views on threats against Finland's national security through cyber networks and their impact on Finland's security and competitiveness; to assess the present state of the intelligence-gathering of the security authorities and development proposals in this regard; to examine to an appropriate extent the legislation that is in place concerning intelligence-gathering by the security authorities in other countries; to produce an impact assessment on the various development options; and, on the basis of their investigation, to submit proposals for legislation and a proposal for measures required for the implementation of that legislation.

According to the assignment, the working group report could be structured as a Government proposal, or it could contain proposals for launching separate legislative initiatives.

Ministerial Counsellor *Hanna Nordström*, Director of Legal Affairs, from the Ministry of Defence was appointed chair of the working group; Ministerial Counsellor *Katriina Laitinen*, later Director of Legal Affairs at the Police Department, from the Ministry of the Interior was appointed deputy chair.

The following were invited as members of the working group: Adviser *Minna Hulkkonen* from the Office of the President of the Republic; head of unit *Mikko Kinnunen* from the Ministry for Foreign Affairs; Director of Legal Affairs *Sami Manninen* from the Ministry of Justice; Superintendent *Jari Pajunen* from the Ministry of the Interior; head of unit *Timo Junttila* and Senior Officer *Pia Palojärvi* from the Ministry of Defence (until 4 June 2014); Budget Counsellor *Petri Syrjänen* from the Ministry of Finance; head of unit, Director of Legal Affairs *Kirsi Miettinen* from the Ministry of Transport and Communications (until 24 October 2014); Ministerial Adviser, later Director of HR and Administration *Kari Mäkinen* from the Ministry of Employment and the Economy; Assistant National Police Commissioner *Tomi Vuori* from the National Police Board; Sector Director *Mika Lundelin* from the Defence Command (from 4 June 2014); and Communication Counsellor, head of unit *Päivi Antikainen* from the Ministry of Transport and Communications (from 24 October 2014).

The following were invited as permanent experts of the working group: Director General *Päivi Kaukoranta* from the Ministry for Foreign Affairs; Senior Adviser, Legislative Affairs *Sami Kivi-*

vasara from the Ministry of Finance (until 4 June 2014); Senior Adviser, Legislative Affairs *Hannele Kerola* from the Ministry of Finance (from 4 June 2014); Director General *Antti Pelttari* and Deputy Director *Petri Knape* from the Finnish Security Intelligence Service; Chief of Defence Intelligence *Harri Ohra-aho* from the Defence Command; Colonel *Martti J. Kari* from the Defence Forces; and Ministerial Adviser *Laura Tarhonen* from the Ministry of Transport and Communications (from 10 September 2014).

Systems Analyst *Sari Kajantie* from the Finnish Security Intelligence Service and Engineering Captain *Jouni Flyktman* from the Defence Forces participated in the work of the working group as technical experts.

The secretaries of the working group were: Senior Officer *Jenni Herrala,* Senior Adviser *Minnamaria Nurminen* and Referendary *Kosti Honkanen* (from 4 June 2014) from the Ministry of Defence; Chief Inspector *Jan Sjöblom* from the Finnish Security Intelligence Service; and Sectoral Director *Mika Lundelin* from the Defence Command (until 4 June 2014).

The working group named itself the intelligence legislation working group. The working group held 45 meetings. The working group consulted the following persons:

situational awareness coordinator, head of unit *Jarkko Korhonen,* Prime Minister's Office
Director of Government Security *Timo Härkönen*, Prime Minister's Office
Director General, Information and Documentation *Ari Uusikartano,* Ministry for Foreign Affairs
Special Adviser *Kimmo Janhunen,* Ministry of Finance

Director of the EU Intelligence Analysis Centre *Ilkka Salmi*
Director, Intelligence Directorate, EU Military Staff *Georgij Alafuzoff*

Data Protection Ombudsman *Reijo Aarnio*
Professor of Law *Veli-Pekka Viljanen,* University of Turku

Manager ICT *Christian Fjäder,* National Emergency Supply Centre
Director *Kirsi Karlamaa,* Finnish Communications Regulatory Authority
Head of Security Regulation *Jarkko Saarimäki,* Cyber Security Centre
Information Security Expert *Tomi Hasu,* Cyber Security Centre
Director of the National Bureau of Investigation *Robin Lardot*
Detective Inspector *Timo Piiroinen,* National Bureau of Investigation
Systems Analyst *Pasi Paunu,* Finnish Security Intelligence Service

Nordic Policy Counsel *David Mothander,* Google
Administration and Security Manager *Vesa Vuoti*, DNA Oyj
Head of Special Network Security *Krister Kaipio*, TeliaSonera Finland Oyj
Security Manager *Jaakko Wallenius*, Elisa Oyj

Platform Strategy Manager *Pasi Mäkinen*, Microsoft Oy
Vice President *Kaisa Olkkonen*, Nokia Government Relations
Head of Security Technologies *Gabriel Waller*, Nokia Solutions and Networks
Chief Research Officer *Mikko Hyppönen*, F-Secure Oyj
Technology Director *Kimmo Kasslin*, F-Secure Oyj
SME Director *Jyrki Hollmén*, Confederation of Finnish Industries
Associate Partner *Vesa Weissmann*, Gearshift Group Oy

The working group has also consulted two foreign experts in confidence concerning the effectiveness and necessity of telecommunications intelligence.

The working group held a background briefing for the media on 12 March 2014 and public hearings for the business sector on 29 April 2014, and for NGOs and other interest groups on 6 May 2014.

The working group requested the Ministry of Defence to commission a study of foreign investments in the IT sector in Finland and Sweden between 2008 and 2013, and the potential impact of Swedish signals intelligence legislation on investments in Sweden.

In assessing the need for regulating intelligence gathering in cyber networks, it emerged that legislative development will need to be examined more broadly, addressing intelligence gathering by the security authorities in general. Improving the intelligence gathering capability of the security authorities is not principally about improving information security; rather, it is about improving the ability of the authorities to prevent actions that seriously threaten national security.

The working group did not structure the present report as a Government proposal. The report assesses the current state of intelligence gathering by the security authorities and presents development proposals for intelligence duties and powers.

One dissenting opinion and two comments were recorded; these are appended to the present report.

Having completed its work, the working group hereby respectfully submits the present report to the Ministry of Defence.

Helsinki, 14 January 2015

Unofficial translation
Ministry of Defence, Finland
March 2015

	Hanna Nordström	Katriina Laitinen
Päivi Antikainen	Minna Hulkkonen	Timo Junttila
Mikko Kinnunen	Mika Lundelin	Sami Manninen
Kari Mäkinen	Jari Pajunen	Petri Syrjänen
		Tomi Vuori
Martti J. Kari	Päivi Kaukoranta	Hannele Kerola
Petri Knape	Harri Ohra-aho	Antti Pelttari
		Laura Tarhonen
	Jenni Herrala	Kosti Honkanen
	Minnamaria Nurminen	Jan Sjöblom

CONTENTS

1. INTRODUCTION

1.1 Background

Global trends in internationalisation and technological development are important and necessary. These trends have resulted in Finland's security environment changing significantly and becoming more complex during recent years. Internal and external security threats are increasingly closely interlinked. The most serious threats to our national security are almost without exception of international origin or at least have contacts abroad. Finland's interests abroad – including crisis management operations in which Finland is taking part – also face more threats of a more serious nature than before. Identifying the governmental and non-governmental entities behind these threats and anticipating their actions has become more difficult. Advanced IT has provided even small governments and non-governmental operators with the capability for effective action. Technological advancements have enabled the execution of actions jeopardising national security with less preparation and with more serious consequences. Cyberattacks can be used as instruments of political and financial pressure and as a means of coercion in serious crises alongside traditional military force.

It follows from the international nature of these threats that the entities behind them are often networks based in various countries, whose members communicate across national borders. The rapid development of telecommunications technology has enhanced and simplified cross-border communications and networking among parties that constitute a threat to Finland and thereby fuelled the internationalisation of threats. Not only civilian operators but also modern military command is increasingly dependent on the public telecommunications infrastructure. The military is widely adopting command and communication systems designed for civilian use because of their rapid technological development and lower costs.

1.2 Object of the study

In the appointment letter dated 13 December 2013, the working group was assigned to develop Finland's legislation specifically with regard to the regulation of intelligence gathering by the security authorities. The goal stated in the appointment letter was the better management of national security, particularly with reference to combating threats in cybernetworks.

Cybersecurity had already been mentioned in the Security Strategy for Society 2010 (Government Resolution, 16 December 2010). Cyber threats were identified as a genre of potential threats, and it was observed that illegal access to information systems might, under certain circumstances, be comparable to the use of military force. Finland's Cyber Security Strategy 2013 (Government Resolution, 24 January 2013) outlined the vision that by 2016 Finland would be a global forerunner in cyber threat preparedness and in managing the disturbances caused by these threats.

For the purposes of the present report, improving the intelligence gathering capability of the security authorities is not primarily about improving information security, nor is it about the combating

of ordinary online crime; rather, it is about the detecting and identifying of serious threats to national security and enabling their combating. The aim is to improve the ability of the senior government leadership and the security authorities to obtain information on such threats and on developments in Finland's security environment. It must be possible to provide the senior government leadership with timely, impartial and reliable information as input for decision-making so that those decisions can influence and prepare for the threats, risks and opportunities that exist in the security environment. Ensuring national security through intelligence gathering is important for society at large and for the continued functioning of the economy. To this end, we must examine the present state of intelligence gathering by the security authorities and survey proposals for its development.

The authorities in the administrative branch of the Ministry of the Interior are responsible for the preventing of threats to national security in Finland that are civilian in nature. The Finnish Security Intelligence Service is a national police unit whose task is to prevent undertakings and offences that might compromise the government or public order, or internal or external national security, and to investigate such offences. The Finnish Security Intelligence Service is also required to maintain and improve general readiness for preventing actions compromising national security. The Finnish Security Intelligence Service engages in continuous intelligence work in its sector and maintains the resulting national and international situational awareness of national security, reporting regularly to the senior government leadership and the other security authorities.

The powers of the police to gather intelligence were recently revised in a reform of the Coercive Measures Act and the Police Act. By contrast, the Finnish Security Intelligence Service have no special statutory powers for intelligence gathering; its powers for intelligence gathering are derived from the legislation governing the police in general. The use of the powers for intelligence gathering is contingent on the prevention and discovery of offences. In the present report, as per the assignment, discussion of legislative development with particular reference to intelligence gathering by the Finnish Security Intelligence Service will occupy a central role.

Finland's military defence is the duty of the Defence Forces, which belongs to the administrative branch of the Ministry of Defence. The intelligence gathering needs of that administrative branch have to do with creating and maintaining situational awareness for military strategy and with security on international missions. The intelligence and monitoring system of the Defence Forces follows developments in Finland's security environments, identifies changes therein and produces information on the current situation. This system provides the senior government leadership with advance warning on the emergence of military threats, enabling the government to make timely decisions and to direct the vital functions of society as appropriate. There are no specific statutory provisions concerning intelligence gathering by the Defence Forces, i.e. military intelligence. According to the preparatory work for the Defence Forces Act (551/2007), intelligence gathering is one of the tasks of the Defence Forces, but no specific powers have been defined.

Finland has no legislation specifying what the purpose of intelligence work is or what kind of intelligence operations are permissible. The security authorities' powers for intelligence gathering are insufficient both in view of their importance to society at large and in comparison with other coun-

tries. This situation is unsatisfactory considering the major changes that have happened in Finland's international security operating environment in recent years.

The present report describes the changing security environment and the present state of intelligence gathering related to national security. We also discuss legislation in comparative countries, evaluate the need for Finnish intelligence legislation, evaluate the impact of development proposals and suggest an outline for legislative development.

1.3 Concepts

Because Finland has no legislation on intelligence, the concepts used to describe intelligence and its various areas are not well established and hence subject to interpretation. Understanding the connections and differences between intelligence and related operations requires a knowledge of key terminology.

General concepts in intelligence

Intelligence: Information acquisition from public and non-public sources, the purpose of which is to explore and increase understanding of a variety of threats, risks, opportunities and changes within a country and beyond its borders. Intelligence is intended to provide early information to allow for influencing and anticipating threats, risks, opportunities and changes. Intelligence includes information analysis for the purpose of understanding, reducing and in some cases leveraging various uncertainty factors in the security environment.

Intelligence cycle: The intelligence cycle illustrates the relationship between the client and the party acquiring the information, the processes of analysis and reporting, and the interaction between these. The figure below is an illustration of the cycle:

Military intelligence: Intelligence work carried out by the military authorities for the purpose of acquiring strategic and operational information and evaluations on the operating environment as input for decision-making by the senior government leadership and the Defence Forces command. Military intelligence is responsible for providing strategic, operational and tactical advance warnings, target support and the geographical and local conditions information required by the Defence Forces. Advance warnings enable countermeasures commensurate with the threat to be put into action.

Civilian intelligence: Intelligence work carried out by the civilian authorities for the purpose of acquiring information on matters other than military national defence as input for decision-making by the senior government leadership and for their own operations.

Security intelligence: Intelligence work whose purpose is to detect, identify, understand and prevent threats against internal or external national security. Information acquisition in security intelligence addresses the operating environment broadly and is not associated with individual offences as in the case of criminal intelligence.

Criminal intelligence: Intelligence work carried out by the law enforcement authorities for the purpose of acquiring information on offenders, offences and the circumstances of offences relevant for the prevention, detection or investigation of offences.

Principal genres of intelligence

Open Source Intelligence (OSINT): Acquiring information from public sources such as literature, maps, print media, public documents and websites.

Signals intelligence (SIGINT): Acquisition of information by military or civilian authorities from electronic signals. The internationally established sub-genres of signals intelligence are:

- *Communications Intelligence (COMINT),* meaning surveillance of electronic communications; and
- *Electronic Intelligence (ELINT),* meaning surveillance of sensor and navigation signals and other signals generated by technological devices; electronic intelligence does not concern person-to-person communications.

Human Intelligence (HUMINT): Acquiring information on the basis of personal interaction or by personally observing another person or other target. Human intelligence can also be conducted online.

Special concepts used in the present report

For the purposes of the present report, we define the concepts of ‘telecommunications intelligence’, ‘foreign information systems intelligence’ and ‘foreign human intelligence’.

Telecommunications intelligence is intelligence work focusing on traffic in telecommunications cables crossing Finland's borders. Telecommunications intelligence is a sub-genre of signals intelligence. It can include both communications intelligence and electronic intelligence.

Foreign information systems intelligence is intelligence work focusing with IT methods on information processed in information systems located abroad.

Foreign human intelligence is intelligence work based on personal interaction or the personal observation of another person or other target abroad.

The blanket term *foreign intelligence* may be used for foreign information systems intelligence and foreign human intelligence, as both are activities engaged in beyond Finland's borders. Telecommunications intelligence and foreign information systems intelligence have the common feature of being online activities and may thus be collectively referred to as *cybernetwork intelligence.*

2. THE CHANGING SECURITY ENVIRONMENT

2.1 Broad concept of security

On 20 December 2012, the Government submitted to Parliament its Report on Finnish Security and Defence Policy 2012 (hereinafter the **2012 Report**). The 2012 Report is based on a broad concept of security, as required in the Government Programme. The scope in time of the 2012 Report extends to the 2020s. The document forms the basis for governing Finland's policy-making to promote national interests and goals. The 2012 Report places particular emphasis on developments in the international operating environment and the significance of the globalisation of security issues for Finland's national security.

According to the 2012 Report, modern network-based structures of society are increasingly dependent on critical infrastructure such as transport, telecommunications and energy supply. Moreover, growing interdependence and the increasingly technical operating environment also bring a new kind of vulnerability of society to the forefront. Since nearly all critical functions and services of society depend on technical systems that use electricity and telecommunications, the risk of serious disruptions in society becomes all the more serious.

The 2012 Report stresses that Finland must be able to ensure the continuity of the vital functions of society under all conditions. According to the 2012 Report, the prevention of and the preparation for cross-border threats require the use of both civilian and military resources, the employment of a wide range of means and a more comprehensive national security policy.

From the perspective of the security authorities, the prerequisite for responding to this challenge is the capacity for sufficiently early detection and identification of cross-border threats to national security.

2.2 National security environment

The sovereignty of a country may be regarded as the most important interest of society to be protected. By 'sovereignty', we mean the independence of a country with regard to other countries and the exclusive right of its government to exercise supreme power within its borders. Other key interests include the management of government affairs, international activity, defence capability, internal security, functioning of the economy and infrastructure, and the population's income security and capability to function.[1] Threats against any of the above may be considered threats to national security. The authorities responsible for combating these threats are collectively referred to in the present report as 'national security authorities'.

With increasing internationalisation, the line between external and internal national intelligence has become blurred. It is also increasingly difficult to define threats and risks as specific to a particular region or location because of the transnational nature of economic, technological and social

[1] *Security Strategy for Society* p. 16.

systems and their interdependence. Indeed, the most serious potential threats to Finland's national security have to do with events beyond the borders of Finland. Thus, the consequences of a threat that is of foreign origin and that emerges abroad may be more likely to be realised in Finland than before. What is common for external threats to national security is that it is increasingly difficult to identify and distinguish between governmental and non-governmental operators behind these threats. Consequently, it is also more challenging than before to anticipate such threats.

Basically, threats may be divided into civilian and military threats. Key civilian security threats include international terrorism, espionage against Finland and Finnish interests by foreign governments, aims to distribute weapons of mass destruction and dual-use items, and types of international organised crime that aim to influence decision-making in society or to infiltrate government structures. In recent years, transnational espionage in information networks has emerged as a major threat. It is an activity that enables the acquiring of large amounts of information in a concentrated effort, which may cause irreparable damage to the security and interests of the target country.

Military threats have also changed in nature. In addition to traditional military action, modern military operations use various means of asymmetrical warfare. Modern military operations typically begin in peacetime with intimidation and disinformation operations and cyber attacks. Their purpose may be to deliberately influence decision-making in another country to achieve strategic aims to which the target country would not otherwise agree. Today, intimidation and disinformation operations are part of the continuum of governments' foreign and security policies. The potential for influence of non-governmental operators in military operations has also increased due to technological advancements and the increased vulnerability of societies.

The line between political influence and warfare is also blurred when it comes to political and economical pressure and disinformation operations. In the future, the use of force, even over a wide area, will not necessarily involve the capture and occupation of large areas of territory. Instead, the aim may be to achieve the desired goals by surprise deployments and the rapid takeover of limited areas.

2.3 Increasingly technological communications

Today, information is conveyed and personal communication undertaken mostly through cyber networks. Society has changed into an environment where almost all traditional services and functions are controlled by IT or are now online.

The operational logic of information networks differs from that of conventional telephone networks. Whereas the telephone network reserved a circuit connection exclusively to the caller and the respondent, the Internet carries the traffic of multiple connections interleaved. The sending device divides the message into packets that are reassembled into the message by the receiving device. Not all packets necessarily travel to the recipient by the same route, because the Internet routes each individual packet along whichever route happens to be the most efficient at that moment. Communications between parties in the same country may travel through a node abroad.

Cyber network development has enabled systems such as cloud services. Cloud services are storage systems where the data stored may be accessed by an authorised user from any online device. The servers actually storing the data in the cloud may be located in one or more countries. It may be impossible for users even to find out where the data are physically located.

Through globalisation, threats against national security increasingly involve connections between, and hence the need for communication between, persons in Finland and persons abroad. Electronic communications are used in communication between governmental and non-governmental bodies behind the threats; in assignments; in reporting on tasks carried out; in planning actions; in gathering intelligence about targets; in motivating and radicalising the participants; and in recruiting new members. In order to combat such threats successfully, the national security authorities must be able to become aware of such activities at an early stage and of the factors representing a threat to national security discussed in those contexts. Early intelligence will improve the response capability of Finnish society and broaden the range of means available for preventing or preparing for the realisation of such threats. Worldwide, intelligence gathering by national security authorities in information networks has played a crucial role for instance in preventing acts of terrorism.

Electronic networking among actors representing a threat to national security will continue to grow in importance. With the emergence of the social media, networking has diversified. Terrorist organisations and other radicals invest in developing their own media organisations and propaganda dissemination systems. They increasingly use the social media, such as instant messaging, and maintain both public and restricted chatrooms. These enable easy bilateral and multilateral communications and real-time planning and coordination of actions.

According to the 2012 Report, critical military capabilities will include intelligence and surveillance systems. Unmanned vehicles will be developed for intelligence and surveillance and, to a growing extent, as platforms for precision-guided munitions. The military operating environment has changed. Foreign military target systems have become increasingly complex, the volume of signal traffic has increased manyfold, and a growing portion of telecommunications is conducted via cable rather than by radio. Because of the changes in the operating environment, the potential of Finland's military intelligence to gather intelligence has declined.

Military intelligence targets are increasingly adopting communications systems designed for civilian use because of rapid technological advancements and lower costs. Military commands are increasingly relying on public cyber network infrastructure. With ubiquitous IT, the volume of data processed in information systems has grown exponentially, and the majority of data are now stored in digital form. Accordingly, intelligence work should focus on digital information in order to function effectively in an IT-based operating environment.

2.4 Cyber threats to national security

Parties constituting a threat to national security use information networks not only for communication but for carrying out their threats.

Threats to the viability of the state or the key security interests of the government discussed in Finland's Cyber Security Strategy include above all cyber espionage, cyber terrorism and cyber operations. The last of these includes pressure, low intensity conflict (LIC) in a cyber environment, and cyber operations in times of war.

Cyber espionage is the acquisition of classified or sensitive information – state or business secrets – from information systems.[2] Cyber espionage may go on for years without being detected. The security authorities estimate that several foreign powers are focusing extensive and technologically sophisticated cyber espionage against Finland's central government and enterprises of major importance for the national economy. The tools used for cyber espionage are not typical malicious software programs that can be detected using commercial anti-virus software; they are sophisticated and versatile cyber attack tools. The first task of such a tool is to take control of a specific part of the network, followed by the installation of advanced surveillance and malicious software programs. Espionage operations are carefully planned in advance and have specific operational goals such as to gather information on the foreign and security policy, national economy and industry of the target country. In addition to espionage programs, malicious software programs may be introduced into information systems to be activated in the event of a crisis. New technologies create new opportunities for warfare through cyber operations aimed at society as a whole, not just the armed forces.

Cyber espionage and cyber operations will continue to grow in importance in the near future. This is because in the cyber environment it is possible to undertake actions at low cost and minimal risk of detection, whereas protecting against such actions is difficult and expensive. All of the foreign powers that are of relevance for the development of Finland's security environment are making systematic and extensive investments in building their offensive cyber capacity. As examples of cyber operations against governments, we may mention the attacks against restricted official networks in Ukraine (2014), Georgia (2008) and Estonia (2007), which proved to be highly organised and well-planned operations that are suspected to have been conducted by another government or bodies closely related to a government.

The threat of cyber attacks against Finland for terrorist purposes remains marginal. However, this can change rapidly due to developments in the international operating environment. Certain international terrorist groups have sought to improve their cyber attack abilities; moreover, there are indications that several groups are making efforts both to improve their own expertise and to outsource (purchased services for targeted attacks). Possible means of conducting such attacks include denial-of-service attacks disrupting the availability of critical online services and cyber vandalism through the SCADA control room system, which in the worst case can cause substantial casualties and property damage.

[2] Examples of information gathering and influence through the cyber environment include the Stuxnet malicious software program aimed at the Iran's nuclear programme, the download files Red October and Agent.btz discovered in the defence administration networks of Ukraine, several European countries and the USA, and the spy programs Snake, Turla and Uroboros developed from the latter.

2.5 Cyber crime

The threat of cyber crime has been escalating rapidly in recent years. Such offences may be aimed at private individuals, businesses, organisations or society at large. This trend is apparent in the number of cyber offences reported to the police and in their increasing severity. According to the UNODC, a citizen is more likely to be a victim of cyber crime than traditional crime.

Cyber crime is latent crime to a very great extent, as most of it is never reported to the police because not even the injured parties themselves notice it. Even if they do notice it, this may take a long time, and they may then deal with it without notifying the authorities or even their potential customers.

Cyber crime is international in nature. Offenders often work in groups that come together as a pooling of expertise and resources. The members of such groups communicate online and do not know each other's identities. They each operate in their own country, using resources and services in various countries to commit their offences and may launch attacks against several countries at the same time. Their targets may include systems critical for the functioning of society, such as international banking or payment systems.

However, cases of a suspected serious crime do not always involve a deliberate offence but may be caused by a software glitch, a hardware malfunction, a misconfigured device or other human error; in other cases, it is not immediately possible to identify the party responsible for the offence or even their motive.

3. PRESENT STATE OF INTELLIGENCE GATHERING AND COMBATING INFORMATION SECURITY THREATS

3.1 Statutory duties of the national security authorities

3.1.1 Duties and powers of the police

The function of the police is to secure judicial and social order, to maintain public order and security, to prevent and investigate crimes, and to submit cases to prosecutors for consideration of charges. To maintain security, the police collaborate with other authorities, with organisations and with citizens and engage in international cooperation relevant to its duties. The police are also responsible for licence administration and other duties separately provided by law, and provide anyone with assistance if it falls within their purview. If there is reason to believe that a person has disappeared or been the victim of an accident, the police must take the necessary action to find that person.

The powers of the police to acquire information required for preventing and discovering offences are provided for in the Police Act. The powers of the police to acquire information required for in-

vestigating offences, on the other hand, are provided for in the Coercive Measures Act and the Criminal Investigation Act. In the overall reform of the Police Act and the Coercive Measures Act that entered into force in 2014, the provisions on powers concerning various kinds of information acquisition were harmonised; as a result the provisions on the means of information acquisition are now essentially the same in both Acts. The key difference is in the purpose for which information acquisition measures are used: preventing and discovering offences (Police Act) or investigating offences (Coercive Measures Act).

The rights of the police to acquire information are provided for in chapter 4 of the Police Act. Under section 2(1) of the chapter, the police have the right, notwithstanding the secrecy obligation, to obtain from an authority or a body assigned to perform a public function any information and documents necessary to carry out an official duty unless disclosing such information or documents to the police is prohibited or restricted by law. Under section 3(1) of the same chapter, the police have the right to obtain any information necessary to prevent or investigate an offence, notwithstanding business, banking or insurance secrecy. Subsection 2 of that section specifies that the police have the right to obtain from a telecommunications operator and a corporate or associate subscriber the contact information about a subscription that is not listed in a public directory or the data specifying a telecommunications subscriber connection if, in individual cases, the information is needed to carry out police duties.

3.1.1.1 Duties of the Finnish Security Intelligence Service

In the police organisation, the combating of threats to national security is the responsibility of the Finnish Security Intelligence Service, a nationwide unit. Under section 10 of the Police Administration Act, the Finnish Security Intelligence Service is a national police unit whose task is to prevent undertakings and offences that might compromise the government or public order, or internal or external national security, and to investigate such offences. The Finnish Security Intelligence Service is also required to maintain and improve general readiness for preventing actions compromising national security. The National Police Board specifies which categories of cases fall within the domain of the Finnish Security Intelligence Service.

According to the Government proposal for the Police Administration Act (HE 155/1991 vp), the provision was written in such a way as to allow for the increasing importance of preventive action in the domain of the Finnish Security Intelligence Service. It is noted in the preparatory work for the Act that the prevention of actions endangering national security is a key function of the Finnish Security Intelligence Service and that investigating an infringement of national security interests that has already happened is generally an indication that preventive action has failed in some way.

The means by which the preventive action assigned to the Finnish Security Intelligence Service should be executed are specified in more detail in the Police Administration Decree (158/1996). Under section 8 of the Decree, the Finnish Security Intelligence Service shall, in the discharging of its statutory duties, provide authorities and corporations with instructions, advice and information such as is needed for safeguarding national security or for preventing infringements of same.

Section 10 of the Police Administration Act outlines the domain of the Finnish Security Intelligence Service by listing the objects of legal protection whose protection falls within the duties of the Finnish Security Intelligence Service: internal security, external security and governmental and social order. The Act does not specify which concrete phenomena and security threats the Finnish Security Intelligence Service is required to combat. Apparently the motivation for defining the duties of the Finnish Security Intelligence Service on the basis of objects of legal protection was to ensure that the operations of the Finnish Security Intelligence Service protecting key national interests could be adapted to changing circumstances and to ensure the general applicability of its domain.

Actual concrete instructions concerning the domain of the Finnish Security Intelligence Service are given in the National Police Board directive on the duties of the Finnish Security Intelligence Service and cooperation with other police units, which is revised from time to time. According to the currently valid directive, the principal duties of the Finnish Security Intelligence Service are:

- the combating, prevention and detection of terrorism;
- the combating, prevention and detection of covert intelligence operations; and
- security enhancement.

The directive further specifies that the duties of the Finnish Security Intelligence Service include:

- prevention of the distribution of weapons of mass destruction, together with other authorities;
- analysing the country's security environment;
- maintaining national and international awareness in its domain;
- the combating, prevention and detection of illegal activism with internal national security implications;
- threat assessments in connection with state visits and significant conferences;
- security intelligence work in its domain; and
- investigating certain offences in its domain.

Managing the statutory duties of the Finnish Security Intelligence Service includes actively monitoring Finland's security environment, engaging in proactive information acquisition concerning security threats and analysing the information acquired. Analysed information is mainly produced for the needs of the senior government leadership. Section 4a of the Police Administration Act specifies that the Finnish Security Intelligence Service is obliged to report on matters of major significance to society within its domain directly to the Minister of the Interior and the National Police Commissioner. According to the preamble to the provision, the Finnish Security Intelligence Service is also obliged to inform the President of the Republic, the Prime Minister and the Minister for Foreign Affairs, in view of their foreign and security policy duties. The Finnish Security Intelligence Service also informs the Constitutional Law Committee, Administration Committee and Foreign Affairs Committee of Parliament of Finland's current security status.

As security threats become increasingly complex and international, more intelligence information of a higher quality is needed as input for political decision-making. The annual number of reports from the Finnish Security Intelligence Service to the senior government leadership describing Finland's security status has increased by a factor of 10 since 2008.

The Ministry of the Interior is currently preparing to alter the administrative status of the Finnish Security Intelligence Service to remove it from the supervision of the National Police Board and to have it report directly to the Ministry. According to the draft for the relevant Government proposal, this change would strengthen political strategic steering of the Finnish Security Intelligence Service and clarify the status of the Finnish Security Intelligence Service both vis-à-vis other government authorities in Finland and in the increasingly important international cooperation between national security and intelligence services. The change would bring the Finnish Security Intelligence Service closer to security policy decision-makers and simplify its collaboration and reporting relationships. The aim is to improve the ability of government leadership to control how the information acquisition efforts of the Finnish Security Intelligence Service are oriented, and thereby increase the ability of the Finnish Security Intelligence Service to provide relevant information that supports Finland's internal security and decision-making concerning foreign and security policy.

The goal of improving service capacity is closely connected with the issue of creating a permanent Ministry-level steering and coordination mechanism for directing information acquisition by the Finnish Security Intelligence Service. A working group appointed to explore the administrative status and performance management of the Finnish Security Intelligence Service and how to improve supervision submitted its final report to the Minister of the Interior on 24 September 2014 (Ministry of the Interior publications 28/2014), proposing the establishment of just such a mechanism. Under this proposal, information acquisition priorities would be set for the Finnish Security Intelligence Service on an annual basis under the leadership of the Ministry that directs the agency's operations. Before the adoption of these priorities, they should be subjected to preliminary discussion and coordination for instance in the Cabinet Committee on Foreign and Security Policy and reported to the relevant Committees of Parliament. Implementing the mechanism is not considered to require legislative amendments.

3.1.2 Duties of the Defence Forces

Under section 2 of the Act on the Defence Forces, the duties of the Defence Forces are the military defence of Finland, providing support for other authorities and participating in international military crisis management. Section 2(1)1(a) specifies that the military defence of Finland includes undertaking surveillance of Finland's land and sea areas and airspace, and securing the nation's territorial integrity. Section 2(1)1(b) specifies that the military defence of Finland further includes securing the livelihoods and basic rights of the Finnish people and the functioning of the government, and defending the lawful social order.

The sovereignty of a state includes territorial integrity. The Territorial Surveillance Act (755/2000) contains provisions on the surveillance and protection of Finland's territorial integrity. The purpose of territorial surveillance is to prevent, expose and investigate territorial offences and territorial

violations. More specific provisions have been adopted on territorial surveillance pursuant to the Act by Government Decree 971/2000.

The definition of 'hostile activity' in the Territorial Surveillance Act includes the following (section 34(2)4–5):

> "4) intelligence operations and electronic interference illegally targeted by a foreign state at objects in Finnish territory which are important for national security;
> 5) electronic jamming illegally targeted by a foreign state at a Finnish government vessel or government aircraft."

It is the duty of the national defence system to create and maintain the military strategic situational awareness required for decision-making. Military intelligence is mentioned as being part of the duties of the Defence Forces in the detailed preamble to section 2 of the Act (HE 264/2006 vp, pp. 17–18). The preamble for section 2(1)1(b) of the Act notes that "the Defence Forces, for its part, secures the livelihoods and basic rights of the Finnish people and the functioning of government, and defends the lawful social order. - - In order to safeguard these, sufficient defence capability must be maintained, and the Defence Forces must proactively prevent military threats and repel any attacks against the country." It is further noted in the preamble to section 2 that "in order to create and maintain military strategic situational awareness, the intelligence and monitoring system of the Defence Forces follows developments in Finland's security environments, identifies changes therein and produces information on the current situation. The system yields advance warnings on the emergence of military threats so that necessary counteraction may be taken." Military intelligence is mainly aimed at foreign states, particularly foreign military organisations.

However, there is no legislation providing for the powers of military intelligence, although there is a provision on the counter-intelligence duties of the Defence Forces, i.e. the prevention and detection of offences related to actions jeopardising national defence within Finland's borders, in the Act on Military Discipline and Criminal Investigation (255/2014).

3.2 Intelligence gathering by the Finnish Security Intelligence Service and the Defence Forces in Finland

3.2.1 Intelligence gathering by the Finnish Security Intelligence Service in Finland

3.2.1.1 General

The principal task of the Finnish Security Intelligence Service is to prevent and detect plans and offences connected with terrorism, illegal intelligence operations, the distribution of weapons of mass destruction, extremist movements and organised crime that jeopardises national security, and also, to a limited extent, undertake criminal investigation of offences related to the above.

Carrying out this task requires the Finnish Security Intelligence Service to be able to acquire information on such plans and offences.

Acquiring information that is publicly available usually does not require statutory powers. However, because the plans and offences which the Finnish Security Intelligence Service is meant to be combating are generally kept secret, action against them cannot in practice be based on publicly available information. For this reason, the operations of the Finnish Security Intelligence Service crucially rely on the acquisitions of non-public information. Also, in order to be efficient, such information must be acquired without the knowledge of the person or body that the information concerns.

The Finnish Security Intelligence Service has no specific statutory powers authorising the acquiring of information on threats to national security. The Finnish Security Intelligence Service, being a police authority, has the same powers and is subject to the same limitations as the police in general as far as information acquisition or any other operations are concerned.

The Finnish Security Intelligence Service routinely employs clandestine means for information acquisition provided for in the Police Act for preventing and detecting offences. Criminal investigation activities, however, are in practice restricted to offences connected to illegal intelligence work. The Finnish Security Intelligence Service rarely undertake criminal investigations.

3.2.1.2 The concepts of preventing and detecting an offence

According to chapter 5 section 1(2) of the Police Act, *preventing an offence* means action aimed at preventing an offence, attempted offence or the preparation of an offence when, due to observations of a person's actions or information otherwise obtained on the person's actions, there are reasonable grounds to believe that he or she would commit an offence, or action aimed at interrupting the commission of an offence already in progress or at limiting the injury, damage or danger directly caused by it. In the above, 'observation of a person's actions or information otherwise obtained' means observations made by the authorities themselves of a person's actions and information provided by a third party such as an information source – tip-offs and other indirect information. Information acquired through observation or otherwise also includes criminal intelligence, surveillance data, tip-offs and conclusions reached through criminal analysis. It is a requirement for a means of information acquisition that is provided for by law for crime prevention to be applicable that such information has led to reasonable grounds to believe that the person concerned has committed an offence (HE 224/2010 vp, p. 89).

Preventing an offence as referred to in the Police Act is an early awareness anticipatory action by the authorities. Under chapter 5, section 1(2) of the Police Act, preventing an offence includes taking action intended to stop the planning and preparation of an offence. 'Preventing the preparation of an offence' means stopping the preparation for a punishable offence even when the preparation itself is not a criminal action.

According to chapter 5 section 1(3) of the Police Act, *detecting an offence* means action aimed at establishing whether the grounds referred to in chapter 3 section 3(1) of the Criminal Investigation Act for starting a criminal investigation are met[3] when, due to observations made of or information otherwise obtained on a person's actions, it can be assumed that an offence has been committed. The concept of 'detecting an offence' refers to the grey area between preventing and investigating an offence. Actions falling under this concept do not belong to the investigation of an offence, because the grounds for starting a criminal investigation have not (yet) been met; nor to the preventing of an offence, because the offence is assumed to have already been committed. An offence is detected for instance in a situation where a tip-off has indicated that the offence has already been committed but there is as yet no concrete basis for suspecting an offence as required in the Criminal Investigation Act, i.e. the 'reason to believe' threshold has not been crossed (HE 224/2010 vp, p. 90).

3.2.1.3 Requirements for the use of secret methods of gathering intelligence

Chapter 5 of the Police Act provides for the methods of gathering intelligence that the police – including the Finnish Security Intelligence Service – are allowed to use for acquiring information without the knowledge of the targets. These means include:

- telecommunications interception (Police Act, chapter 5 section 5)
- obtaining data other than through telecommunications interception (Police Act, chapter 5 section 6)
- traffic data monitoring (Police Act, chapter 5 section 8)
- traffic data monitoring with the consent of the owner of the network address or terminal end device (Police Act, chapter 5 section 9)
- obtaining base station data (Police Act, chapter 5 section 11)
- surveillance (Police Act, chapter 5 section 13)
- covert intelligence gathering (Police Act, chapter 5 section 15)
- on-site interception (Police Act, chapter 5 section 17)
- technical observation (Police Act, chapter 5 section 19)
- technical tracking (Police Act, chapter 5 section 21)
- technical surveillance of a device (Police Act, chapter 5 section 23)
- gathering data identifying a network address or terminal end device (Police Act, chapter 5 section 25)
- undercover activities (Police Act, chapter 5 section 28)
- pseudo purchases (Police Act, chapter 5 section 35)

[3] Under chapter 3 section 3(1) of the Criminal Investigation Act, a criminal investigation authority shall conduct a criminal investigation when there is reason to suspect, whether on the basis of a report received or otherwise, that an offence has been committed.

- use of covert human intelligence sources and controlled use of covert human intelligence sources (Police Act, chapter 5 section 40)
- controlled delivery (Police Act, chapter 5 section 43)

Secret methods of gathering intelligence may be grouped in various ways, depending on their use and purpose. Some are technical methods aimed at the communications of the target, while others may be described as personal methods. Personal methods of gathering intelligence may be further sub-divided according to whether the methods require direct interaction between the person acquiring the information and the target, i.e. misleading the target. Covert intelligence gathering, undercover activities and pseudo purchases involve such a misleading direct interaction, while the use of covert human intelligence resources and the controlled use of covert human intelligence sources involve using a third party to obtain the information. Surveillance is based on sensory observation of the behaviour of the target.

According to chapter 5 section 2(1) of the Police Act, the general precondition for the use of secret methods of gathering intelligence is that *it can be assumed to result* in gaining information *necessary* for preventing, detecting or averting the threat of an offence. Section 2(2) states that telecommunications interception, obtaining data other than through telecommunications interception, extended surveillance, on-site interception, technical observation, technical tracking of a person, technical surveillance of a device, undercover activities, pseudo purchases, controlled use of human intelligence sources and controlled deliveries may be used only if *they can be assumed to be of very great significance* for the prevention or detection of an offence. Moreover, use of undercover activities or pseudo purchases also requires that this be *essential* for the purpose of preventing or detecting an offence.

The Police Act specifies general preconditions and special preconditions for the use of various methods of gathering intelligence. The special preconditions for secret methods of gathering intelligence are the specific offences for the prevention of which each of those methods may be used. Other special preconditions may also be found in the provisions concerning the various methods of gathering intelligence. In summary, we may note that the Finnish Security Intelligence Service may more or less comprehensively use the secret methods of gathering intelligence provided for in chapter 5 of the Police Act in order to prevent terrorism offences punishable under chapter 34a of the Criminal Code, and offences related to unlawful intelligence operations punishable under chapter 12 of the Criminal Code. With regard to preventing offences involving the distribution of weapons of mass destruction and dual-use items and offences compromising national security connected with the operations of organised crime groups, the situation is more complex and subject to interpretation.

The aforementioned secret methods of gathering intelligence may only be used for detecting the latter offences if the offence in question is specifically a treason offence or terrorism offence as defined in the Criminal Code. In detecting offences, the special preconditions listed in the provisions for each of the secret methods of gathering intelligence do not apply (HE 224/2010 vp, p. 92).

The selection and use of secret methods of gathering intelligence are governed by the general principles outlined in chapter 1 of the Police Act: respecting fundamental and human rights, the principle of proportionality, the principle of minimum intervention and the principle of intended purpose.

A common feature in the provisions on the secret methods of gathering intelligence is that they are defined on the basis of the target and offence involved. These methods may only be used against such persons or for acquiring information about the activities of such persons who can, with justification, be assumed to be intending to commit or preparing to commit or already have committed an offence of a particular level of seriousness. If no such crime prevention criterion associated with a specific person exists, using secret methods of gathering intelligence is not allowed under the Police Act. Therefore, the acquiring of all other intelligence must be based on monitoring public sources, general police surveillance and the information received by the Finnish Security Intelligence Service from other authorities and private corporations through its cooperation network.

3.2.1.4 Combating plans

Under section 10 of the Police Administration Act, the Finnish Security Intelligence Service combats offences compromising national security and plans to compromise national security. The concept of 'plan' is not specified in the Police Administration Act or in its preparatory materials. Because of the offence-based criteria for secret methods of gathering intelligence available to the Finnish Security Intelligence Service, these methods may not be used for acquiring information on plans to compromise national security that have not yet progressed at least to the stage of preparing for an offence.

The working group appointed to explore the administrative status and performance management of the Finnish Security Intelligence Service and how to improve supervision submitted its final report to the Minister of the Interior on 24 September 2014. This report addressed the issue of extending the powers of the Finnish Security Intelligence Service for gathering intelligence to combating plans. The final report stated that new powers for gathering intelligence should be considered for the Finnish Security Intelligence Service so that the agency would be able to respond to changes in the operating environment. This reform would involve acquiring information necessary for combating plans compromising national security from human intelligence sources and information networks even in cases where the plans have not yet progressed to the point where there is an actual offence to be prevented, detected or investigated. The working group noted that in considering this matter, the legal justification for extending intelligence-gathering powers should be studied *inter alia* from the perspective of fundamental and human rights.

3.2.2 Intelligence gathering by the Defence Forces in Finland

Military intelligence focuses on the operating environment outside Finland. Functionally, we must distinguish between military intelligence and counter-intelligence, the latter being a policing function carried out by the Defence Forces to prevent offences. Military counter-intelligence involves

preventing and detecting offences within Finland. Military counter-intelligence refers to the prevention and detection of offences involving unlawful intelligence operations against military national defence or compromising military national defence in Finland.

The purpose of military counter-intelligence is to prevent the acquiring of information within Finland by foreign powers that is punishable under the Criminal Code, for instance concerning the capability and formations of the Defence Forces. Typical titles of the offences prevented and detected in such operations are the treason offences defined in chapter 12 of the Criminal Code, such as treason, espionage and unlawful intelligence operations, and the high treason offences defined in chapter 13. However, more ordinary offences such as property crime may also be the focus of such prevention and detection if they are connected with intelligence operations against Finland in the area of military national defence or activities compromising military national security. Examples of the latter may include an information security offence or property offence involving confidential information of the Defence Forces. There is no exhaustive list of the offences against which these powers may be exercised.

In the defence administration, the military counter-intelligence duties of the Defence Forces are provided for in the Act on Military Discipline and Criminal Investigation. The Defence Forces is the special authority for counter-intelligence and, as such, is responsible, without restricting the statutory powers of the Finnish Security Intelligence Service, for the prevention and detection of offences involving intelligence operations against Finland in the area of military national defence and activities compromising military national defence. The powers of the Defence Forces for preventing and detecting offences is more limited than the general powers given to the Finnish Security Intelligence Service in section 10 of the Police Administration Act, and only applies to offences specifically involving intelligence operations against Finland in the area of military national defence and activities compromising military national defence. In this area, the powers of the Defence Forces are parallel to, but not mutually exclusive with, the general powers of the Finnish Security Intelligence Service. The police have a statutory takeover right, i.e. the right at its own initiative to take over the handling of the prevention or detection of an offence within the powers of the Defence Forces.

The Defence Forces follows the principles of the Police Act in the prevention and detection of offences, specifically the principles of respecting fundamental and human rights, the principle of proportionality, the principle of minimum intervention and the principle of intended purpose. The investigation of any offence detected by military counter-intelligence is the responsibility of the Finnish Security Intelligence Service.

Under the Act on Military Discipline and Criminal Investigation, the powers of the officials in the Defence Forces handling the prevention and detection of offences are equal to the powers defined for the prevention and detection of offences in the Police Act. However, regarding secret methods of gathering intelligence, only the following are allowable for the Defence Forces: 1) obtaining base station data, 2) extended surveillance, 3) covert intelligence gathering, 4) on-site interception, 5) technical observation, 6) technical tracking, 7) gathering data identifying a network address or terminal end device. Also, according to the additional limitation concerning the detection of of-

fences, these methods of gathering intelligence may only be used for the detection of the offences of compromising the sovereignty of Finland, incitement to war, treason or aggravated treason, espionage or aggravated espionage, disclosure of a national secret or unlawful intelligence operations. Any official charged with the prevention and detection of offences in the Defence Forces must notify the Finnish Security Intelligence Service whenever any of the secret methods of gathering intelligence listed above is used.

The Act on Military Discipline and Criminal Investigation provides for assistance given by the police in cases where the powers of the Defence Forces are inadequate for carrying out the actions required. In practice, this means acquiring information through methods that are available to the police but not to the Defence Forces. The officials in the Defence Forces responsible for the prevention and detection of offences are posted at Defence Command and the Defence Force Intelligence Agency under it.

3.3 Intelligence gathering by the Finnish Security Intelligence Service and the Defence Forces on foreign countries

3.3.1 Intelligence gathering by the Finnish Security Intelligence Service on foreign countries

Under section 10 of the Police Administration Act, the duties of the Finnish Security Intelligence Service include combating threats against external national security. Threats of foreign origin and thus threats against external national security include international terrorism, espionage against Finland and Finnish national interests by foreign powers, and the distribution of weapons of mass destruction. According to the mission assignment of the Finnish Security Intelligence Service, the agency's duties include analysing Finland's security environment and maintaining international situational awareness in its field. The Finnish Security Intelligence Service reports to Finland's senior government leadership on trends in the international security environment.

The report of the parliamentary police committee (committee report 1986:16) underlying the enactment of the Police Administration Act stresses that it follows from the value of national sovereignty that the government must maintain a continuous preparedness for protecting the external security of the country. The report notes that external security may be compromised by any efforts that would have a harmful impact on the rights and interests of the country or on relations between Finland and foreign powers. The parliamentary police committee concluded that the Finnish Security Intelligence Service in particular plays a key role in combating such hazards and harmful impacts.

Finland's security environment has become decidedly more international since the publication of the report of the parliamentary police committee. Information concerning foreign countries plays an increasingly important role in safeguarding the security interests that belong to the domain of the Finnish Security Intelligence Service.

There is no legislation concerning the gathering of intelligence by the Finnish Security Intelligence Service abroad. The Finnish Security Intelligence Service may only acquire information through the use of powers concerning the prevention and detection of offences as defined in the Police Act. These powers may only be used in Finnish territory.

In practice, the acquiring of information from abroad by the Finnish Security Intelligence Service depends on international intelligence cooperation, the monitoring of public sources and collaboration with liaison officers.

The Finnish Security Intelligence Service and its predecessors have engaged in extensive bilateral and multilateral cooperation with foreign intelligence and security services ever since Finland became independent. The purpose of this cooperation is to ensure that the competent Finnish authorities have access to the foreign intelligence necessary for upholding national security. Because of the general globalisation of security issues and the resulting increased importance of foreign intelligence, the Finnish Security Intelligence Service has in recent years systematically broadened its international network to include the intelligence and security services in all the countries that are relevant for Finland's national security.

International intelligence cooperation must be distinguished from international crime prevention mechanisms. The latter are of little importance in the domain of the Finnish Security Intelligence Service. One key reason for this is that the targets of crime prevention operations undertaken by the Finnish Security Intelligence Service are in the employ of a foreign power and often acting against Finland's interests even in their official capacity. A foreign government benefiting from illicit activities will in practice never give any assistance for the prevention, detection or investigation of such offences to the government (e.g. that of Finland) that is the target of those activities.

The Finnish Security Intelligence Service monitors public sources abroad across its entire domain. Information gained from public sources is combined with information from other sources to create an analysed situational awareness of Finland's international security environment.

In recent years, the Finnish Security Intelligence Service has employed liaison officers on short-term and long-term postings at Finnish embassies in certain countries outside Europe. They enjoy diplomatic status, including the related rights and privileges. The liaison officers of the Finnish Security Intelligence Service contribute to the combating of threats to external national security for instance by maintaining contacts between the country where they are stationed and the representatives of the authorities of other countries stationed there. The work of the liaison officers is based on the provisions on international exchange of information regarding personal data in the Police Act.

In its final report, the working group exploring the administrative status and performance management of the Finnish Security Intelligence Service and the development of supervision proposed that the augmentation of the intelligence-gathering powers of the Finnish Security Intelligence Service should be considered. The final report indicates that the changes prompting the need to update these intelligence-gathering powers stem above all from Finland's external security environment. The working group's proposal that the Finnish Security Intelligence Service be authorised to

acquire information from human intelligence sources for combating plans to compromise national security also applies to operations abroad.

3.3.2 Intelligence gathering by the Defence Forces on foreign countries

Military intelligence as part of national defence

Military intelligence work undertaken by the Defence Forces is traditionally considered to derive from the statutory mandate of the Defence Forces to defend Finland's sovereignty and territorial integrity. Military intelligence is considered to be subsumed in the provisions of section 2(1)1(a–b) of the Act on the Defence Forces and is not separately mentioned in the Act.

Military intelligence focuses on the operating environment outside Finland. The purpose of military intelligence is to create and maintain the military strategic situational awareness required for decision-making. In order to create and maintain military strategic situational awareness, military intelligence follows developments in Finland's security environments, identifies changes therein and produces information on the current situation. The Defence Forces maintains and develops its defence capability through military intelligence. Military intelligence is mainly aimed at foreign states. The purpose of military intelligence is to create and maintain awareness of the operating environment. A key function in this is the early-warning capability regarding the emergence of military threats which ensures that the decision-making of the senior government leadership concerning threats to Finland's sovereignty is based on up-to-date situational awareness and enables timely preparedness actions and countermeasures.

There is no legislation providing for the powers of military intelligence, which is governed by internal orders and guidelines of the Defence Forces.

The Defence Forces engages in cooperation with foreign intelligence authorities as required for executing its duties. The purpose of this cooperation is to acquire the necessary foreign intelligence.

Defence attachés at foreign missions

Under Article 3 of the Vienna Convention on Diplomatic Relations, the functions of a diplomatic mission consist, inter alia, in ascertaining by all lawful means conditions and developments in the receiving State, and reporting thereon to the Government of the sending State. Article 7 of the Convention makes specific reference to military, naval and air attachés among the members of staff of the mission.

Finland has about 20 accredited defence attachés posted to several countries. They report to Finnish military intelligence on the country where they are stationed. There are no provisions in the legislation on the Defence Forces on the powers of Defence Forces officials posted to diplomatic missions.

Military intelligence as part of crisis management operations

Under section 2(1)3 of the Act on the Defence Forces, the duties of the Defence Forces include participating in international military crisis management. Chapter 2 of the same Act contains provisions on the powers of the Defence Forces. Section 13 of the Act stipulates that the Defence Forces participate in international military crisis management as laid down in the Act on Military Crisis Management (211/2006).

Under section 5 of the Act on Military Crisis Management, the Ministry of Defence will assign the duties required for military crisis management to the Defence Forces and will guide and supervise the military crisis management undertaken. A Finnish crisis management organisation may include crisis management troops, separate units and individual persons. The crisis management organisation forms part of the Defence Forces and is subordinate to the Defence Command as provided in section 5 of the Act on Military Crisis Management. In operational terms, the crisis management organisation will be subordinated to the implementing party referred to in section 1(3) of the Act on Military Crisis Management, which may be the UN, the Organisation for Security and Cooperation in Europe (OSCE), the European Union, the North Atlantic Treaty Organisation (NATO) or some other international organisation or group of countries. Neither the Act on Military Crisis Management nor the legislation on the Defence Forces contain any specific provisions on military intelligence in connection with crisis management operations. An intelligence unit may be included in the operations.

A crisis management operation involves a military force operating in the territory of another country. The status of military forces present in the territory of another sovereign state (the host country of the operation) is provided for through agreements determining the legal status and immunity of the troops in that territory. These agreements are known as Status of Forces Agreements (SOFA). Principally, the negotiations concerning SOFAs are conducted by the authorising party or implementing party vis-à-vis the host country. The obligations enshrined in such contractual arrangements, which essentially involve the granting of special rights and privileges to the crisis management forces, unilaterally concern the host country, as a rule. It should be stressed that the SOFAs do not confer operational powers to the forces involved in the operation. Operational powers are derived from the international-law mandate for the operation, the national legislation of the countries sending troops and the military orders issued within the operation.

3.4 Combating information security threats

3.4.1 General

Being an information society and an economy reliant on international markets, Finland depends on the undisrupted functioning of the cyber infrastructure. The functioning and reliability of communications networks and services are important cornerstones for the growth and competitiveness of Finland's economy, for innovations and for wellbeing in areas of society.

The reliability of the cyber infrastructure is also vital for the overall security of society. The increasing reliance of society on IT, increasing foreign ownership of the telecommunications infrastructure

and the outsourcing of IT functions in central government create wholly new challenges for safeguarding the vital functions of society. By the 'vital functions of society', we mean cross-sectoral functional entities that are of crucial importance to the functioning of society as a whole and whose continuation must be safeguarded under all circumstances. The non-functioning of IT systems, the collapse of the cyber infrastructure and various information security threats would have a negative impact on public services, businesses, administration and society at large. As the majority of Finland's critical telecommunications infrastructure and its services is owned and provided by the private sector, it also plays an important role in safeguarding the vital functions of society.

The continued functioning of and absence of disruptions in telecommunications, cyber networks and IT systems is ensured through information security. By 'information security', we mean administrative and technological measures undertaken to ensure that any data are only accessible by those entitled to access them (confidentiality); that data cannot be altered except by those entitled to alter them (integrity); and that data and cyber systems are available to those entitled to use them (accessibility).

The parties who use electronic communications networks and services manage their information security in various ways. For instance, information security may be ensured by information administration means and by imposing technological limitations on the use of a communications network or service. Because of the coherent nature of central government, its information security can be controlled centrally and according to uniform principles. The Ministry of Finance steers and directs the overall development of information security in the public administration, information security in central government and ICT preparedness. The steering duties of the Ministry of Finance are derived *inter alia* from the Act on Information Management Governance in Public Administration (634/2011) and the Act on the Provision of Shared Government Information and Communications Technology Services (1226/2013).

In 2013, in order to safeguard the decision-making capability of the senior government leadership and the statutory duties of the security authorities, the Government adopted a proposal for an Act on the Security Network Operations of Public Administration (HE 54/2013).[4] The aim of this proposal is to enact a security network (TUVE) that would serve as a common telecommunications network for the government leadership, ministries, the Defence Forces, the Border Guard, the police and the rescue authorities. TUVE would ensure preparedness against telecommunications disruptions and the continuity of communications.

A public administration security network would offer all its users and their key service providers a stable ICT service environment. The telecommunications and information security solutions implemented in the security network would enable the use of various levels of protection and of IT environments either in joint use or separate for each user. This would cost-effectively create a robust, shared cyber network for all public authorities nationwide that would function reliably even under exceptional circumstances and in the case of natural disasters, power failures or cyber attacks that are constantly increasing. Under normal circumstances and related disruptions, the Ministry of Fi-

[4] The Government proposal is still being debated by Parliament at the time of writing.

nance would decide on the priority, urgency and other determinations of service production in and the use of the security network.

In 2013, the Ministry of Finance also launched the Central Government 24/7 Information Security Operations development project (SecICT). The purpose of this project is to plan and establish an official function for the prevention and coordination of extensive and serious information security incidents. The project is expanding and developing services in central government that improve information security. The project will also be launching incident troubleshooting groups (VIRT operations). Development efforts are being pursued jointly with information security and cyber security actors in government and in the private sector, and with pilot organisations. The project is scheduled to conclude at the end of 2015, with the new function starting up at the beginning of 2016.

Centralised information security steering is not possible in the private sector; each organisation chooses its level of information security and the means for ensuring it according to its respective needs and emphases. Detecting information security threats and protecting against them depends in practically all cases on commercially available information security software and services, both in government and in the private sector. Some units in central government and some enterprises critical for the security of supply also used the alert and detection system for serious information security breaches (HAVARO) developed by the Finnish Communications Regulatory Authority.

3.4.2 Section 272 of the Information Society Code

The Information Society Code (917/2014) was enacted by Parliament on 15 October 2014 (EV 106/2014 vp), and it will enter into force on 1 January 2015. Among other things, the Code repeals the Act on the Protection of Privacy in Electronic Communications. Section 272 of the Information Society Code contains a provision equivalent to section 20 of the aforementioned Act. The Information Society Code was enacted with input from the Constitutional Law Committee of Parliament.

Section 272 of the Information Society Code states that a telecommunications operator, an added value service provider or corporate or association subscriber, or any party acting on their behalf has the right to analyse messages transmitted or received in its network for ensuring information security in order to detect, prevent, investigate and commit to criminal investigation any disruptions in information security of communications networks or related services.

According to the original preparatory material for section 20 in the Act on the Protection of Privacy in Electronic Communications (HE 125/2003 vp, p. 71), “disruption” is understood to include the intentional distribution and use of malicious software programs. The detailed preamble for section 272 of the Information Society Code notes that this provision is not intended to change the current legal status (HE 221/2013 vp, p. 106).

The automatic analysis of communications content concerns all messages that are sent from or received in the cyber network or IT system of the body using automatic analysis. The principal pur-

pose of analysis is to detect attempts by malicious software to penetrate the system and any communications that malicious software already in the system is having with its hosts.

Malicious software and harmful commands are initially identified in automatic content analysis on the basis of predetermined criteria, and the content of the message is not passed on to a human individual. If, however, it becomes apparent that a message flagged in automatic analysis contains harmful software and information security cannot be ensured by automatic means, section 272 of the Information Society Code allows for an enterprise, an organisation or an authority to retrieve that message for manual processing.

3.4.3 National Cyber Security Centre at FICORA

The National Cyber Security Centre at the Finnish Communications Regulatory Authority (FICORA) is a national information security authority that prevents, gathers information on and investigates infringements of information security in public networks and perpetrated against Finnish parties through them. It also publicises information on significant information security threats. In accordance with the Cyber Security Strategy, the National Cyber Security Centre is also required to produce and maintain a combined cyber security situational awareness. The National Cyber Security Centre gathers information on cyber events and conveys it to various actors besides compiling and sharing the combined cyber security situational awareness. Customers of the National Cyber Security Centre may make use of the information in the situational awareness in their own preparedness and prioritisation measures.

The production of situational awareness draws not only on national sources but also on the international cooperation network of the National Cyber Security Centre, which operates on a voluntary basis and depends on mutual trust. The supervising organisations of the GovCERT groups that belong to this network occupy various functions in their respective central governments. For instance, CERT-SE in Sweden forms part of the Civil Contingencies Agency, while CERT-BUND in Germany is in the administrative branch of the Federal Ministry of the Interior. In some countries, the CERT groups are in the administrative branch of the Ministry of Defence, while in others the CERT groups are a division of an intelligence authority (as with the Government Communications Headquarters, GCHQ).

HAVARO is an early detection and alert system for information security infringements provided by the National Cyber Security Centre for enterprises critical for security of supply and for bodies in the central government administration. Its operations are grounded in section 272 of the Information Society Code (previously section 20 of the Act on the Protection of Privacy in Electronic Communications). HAVARO employs a variety of identifiers to detect harmful cyber traffic and advanced cyber attacks that threaten information security, known as Advanced Persistent Threats (APT). Another purpose of the system is to support the production of a more detailed situational awareness of the information security threats against Finnish information networks. The technical malicious software identifiers used in the system are mainly based on information gained from domestic and foreign partners of the National Cyber Security Centre.

4. INTERNATIONAL SURVEY

In this chapter, we discuss the legislation concerning intelligence on threats to national security in general and intelligence work in the cyber environment, in particular, that is in place in Sweden, Norway, Denmark, the Netherlands and Germany.

4.1 Sweden

4.1.1 General regulation of intelligence work

Intelligence operations conducted by the defence administration are regulated by the Signals Intelligence Act, a complementary decree and special acts.[5] Military intelligence is conducted by the Armed Forces (*Försvarsmakten*), the National Defence Radio Establishment (*Försvarets radioanstalt, FRA*), the Swedish Defence Materiel Administration (*Försvarets materielverk, FMV*) and the Swedish Defence Research Agency (*Totalförsvarets forskningsinstitut, FOI*), which are subordinate to the Ministry of Defence. The domain of intelligence work is limited to the support of Sweden's foreign, security and defence policy, and to the survey of external threats aimed at Sweden. Sweden also participates in international security cooperation. Intelligence work may only focus on circumstances abroad.

The general focus of intelligence work is determined by the Government. Authorities designated by the Government may, within this general framework, issue more detailed orders about where intelligence efforts should be aimed. The purpose of intelligence work is to acquire, process and analyse information. This information is acquired either technically or through personal inquiries, in public and other sources. The information is reported to the party issuing the assignment and to any other party on a need-to-know basis. The authorities engaged in intelligence work may, under specific orders from the Government and within the bounds determined by law, cooperate in intelligence work with other governments and international organisations.

The intelligence service may not undertake assignments that by law or according to other regulations fall within the powers of the police, the Security Service or other law enforcement authorities to combat or prevent crime.[6] According to the preparatory materials for the Signals Intelligence Act,[7] this means that it is not allowed in intelligence work to circumvent legislation and exercise powers of criminal investigation and coercive measures, the usage of and criteria for which are provided for in the Code of Judicial Procedure or the Police Act, for instance. On the other hand, the intelligence service may provide support to the criminal investigation authorities. Regarding

[5] *Lag om försvarsunderrättelseverksamhet* [Act on defence intelligence operations] (2000:130), *Förordning om försvarsunderrättelseverksamhet* [Decree on defence intelligence operations] (2000:131), *Lag om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst* [Act on the handling of personal data in the defence intelligence operations of the Armed Forces and the military intelligence service] (2007:258) and *Förordning* (2007:260) *om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst* [Decree on the handling of personal data in the defence intelligence operations of the Armed Forces and the military intelligence service].

6 The amendment entered into force on 1 January 2015. The earlier wording was "...the crime fighting and crime prevention activities of the police and other authorities".

7 Regeringens proposition [Government proposal] 1999/2000:25.

this, it is noted in the preparatory materials for the Act[8] that the Security Service largely functions like an intelligence agency these days and is involved in the acquiring of information on activities abroad that compromise Sweden's national security. In this function, the Security Service must be able to make use of the information gathering capability of other authorities with similar tasks.

Authorities engaged in intelligence work are required to report to the Ministry of Defence about the general orientation of their operations, international cooperation and the use of special methods of gathering intelligence. It has been considered that these special methods cannot be described in the Act; however, it is noted in the preparatory material that they mainly involve human and signals intelligence.[9] The intelligence authorities must also submit an annual public overview of intelligence work in the past year. A government-designated authority, the Defence Intelligence Commission (*Statens inspektion för försvarsunderrättelseverksamheten, SIUN*), oversees military intelligence operations. SIUN supervises *inter alia* compliance with the law, the direction of intelligence operations and the methods used in gathering intelligence.

4.1.2 Signals intelligence

There is a specific Signals Intelligence Act and decree.[10] Signals intelligence operations are conducted by the National Defence Radio Establishment (FRA), which is a civilian organisation in the administrative branch of the Ministry of Defence and thus not part of the Armed Forces. The duties of the FRA are to gather intelligence in accordance with assignments given and to deliver the information acquired to the parties issuing the assignments.

Under the Signals Intelligence Act, 'signal intelligence' is defined as the intercepting of signals in electronic form (*inhämta signaler i elektronisk form*). This is a technology-neutral definition and covers all methods of signals intelligence, such as cable and radio surveillance, and both manual and automatic gathering of intelligence. Signals intelligence is divided into four phases: direction, collection, processing and dissemination.

Signals intelligence must comply with both the general provisions in the Defence Intelligence Act and the special provisions in the Signals Intelligence Act. Under the general Act, the intelligence operation must be one that supports Sweden's foreign, security and defence policy, concerns circumstances abroad and is intended to survey external threats to Sweden. The Signals Intelligence Act exhaustively defines the threats and situations for the surveying of which signals intelligence may

8 Regeringens proposition [Government proposal] 2006/07:63: "En anpassad försvarsunderrättelseverksamhet" [Applied intelligence operations].
9 Regeringens proposition [Government proposal] 2006/07:63: "En anpassad försvarsunderrättelseverksamhet" [Applied intelligence operations].
10 *Lag* (2008:717) *om signalspaning i försvarsunderrättelseverksamhet* [Act on signal interception in defence intelligence operations], *Lag* (2007:259) *om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet* [Act on the handling of personal data in the defence intelligence and development operations of the National Defence Radio Establishment] and *Förordning* (2008:923) *om signalspaning i försvarsunderrättelseverksamhet* [Decree on signal interception in defence intelligence operations].

be used.[11] If essential for the operations, information may also be gathered for the purpose of monitoring changes in the signals environment, technological development and signals protection, and for the purpose of developing the technology and methods used for gathering information. As a general rule, if both the sender and the recipient of a signal are in Sweden, the signal may not be intercepted.

Undertaking a signals intelligence operation always requires an assignment, which may be given to the FRA by the Government, the Prime Minister's Office, the Armed Forces, the National Bureau of Investigation or the Security Service. The assignment may not designate a specific natural person.

Although the legislation is technology-neutral, it contains some special provisions on cable surveillance. Cable-borne telecommunications may only be intercepted when it crosses the Swedish border.

Signals intelligence always requires a permit from the Defence Intelligence Court, which is the special competent court. An application for a permit for cable surveillance must include a description of the intelligence assignment; a description of which fibres in the cable the surveillance will cover; the search criteria to be used; the duration of the permit; and other details that the signals intelligence authority wishes to point to. The Act contains specific provisions on the circumstances in which the court may issue a permit and on what the permit must indicate. The criteria for issuing a permit pertain to the legality and proportionality of the operation and the assignment, in particular. The permit must indicate the intelligence task being performed; the fibres in the cable that will be covered; the search criteria or categories that may be used; the duration of the permit; and any other terms and conditions needed to protect the privacy of private individuals. According to the preliminary work for the Act,[12] 'search criteria' refer to terms used to filter the flow of information (*informationsmängd*) to find records or clusters of data (*uppgiftskonstellationer*) where the term in question appears. Search criteria may also include variables that can filter larger quantities of data.

The use of criteria referring to a single private individual is excluded to ensure privacy. Such a criterion may only be used if it is especially important for the intelligence operation in question. Moreover, the FRA is obliged to report to the Defence Intelligence Commission on the use of any such search criteria. Any private individual so targeted must be informed as soon as possible – no later than one month after the concluding of the intelligence assignment – when and for what purpose the operation was carried out, unless precluded by confidentiality provisions.

Gathering information from a telecommunications cable requires working with the telecommunications operator. Because of this, telecommunications operators that own cables are required to route any traffic that crosses Sweden's borders to one or more specific connection points within

[11] Under section 1 of the Signals Intelligence Act, such situations are: a) a military threat against Sweden, b) Sweden's interests in international operations, c) international terrorism or organised crime threatening vital national interests, d) weapons of mass destruction, e) external threats against the infrastructure of society, f) conflicts abroad affecting international security, g) external intelligence operations targeting Swedish interests, and h) action or intention on the part of a foreign power with significant implications for Sweden's foreign, security and defence policy.
12 Regeringens proposition [Government proposal] 2006/07:63, pp. 76–77.

Sweden. The operators are also obliged to disclose to the authorities any information that will help in the intercepting of signals. The operators must perform these tasks so as not to compromise their own confidentiality.[13]

Only the Defence Intelligence Commission, as the supervisory authority, has access to the traffic routed by the operators to the designated connection points. Its duty is to distinguish and assign to the FRA access only to those fibres in the cables that are detailed in the court permit.[14] The FRA performs searches on these fibres and conveys any information acquired through signals intelligence operations to the party issuing the assignment and, insofar as the law so requires, to other authorities.

The FRA has a Privacy Protection Council (*Integritetsskyddsråd*) whose task is to oversee that privacy is not infringed. The Council reports to the FRA management and on an as-needed basis to the Defence Intelligence Commission. Signals intelligence is also supervised by the Data Protection Ombudsman, the Parliamentary Ombudsman and the Chancellor of Justice.

The Defence Intelligence Commission focuses particularly on the use of search terms in signals intelligence, the disposal of information and reporting. It may also order an intelligence operation to be discontinued and the information gathered to be destroyed if the operation has not complied with its permit. The Defence Intelligence Commission may, if so requested by a private individual, inspect whether that individual's messaging has been monitored and whether such surveillance was in compliance with the law. The Data Protection Ombudsman (*Datainspektion*) supervises privacy protection in the operations of the FRA as elsewhere.

The processing of personal details acquired through signals intelligence is provided for in a separate act.[15]

4.2 Norway

In Norway, intelligence work and the operations of the intelligence service are provided for in the Intelligence Service Act and a complementary decree.[16] The Ministry of Defence may issue orders further specifying the decree. Intelligence operations in Norway are undertaken by the Norwegian Intelligence Service (*Etterretningstjenesten, NIS*), which is part of the Norwegian Defence Estab-

[13] *Lag* (2003:389) *om elektronisk kommunikation* [Act on electronic communications], section 19a.
[14] *Lag om signalspaning* [Act on signal interception] section 12. This is an amendment enacted by Act 2009:967 pursuant to the Government proposal Prop 2008/09:21, *Förstärkt integritetsskydd vid signalspaning* [Enhanced protection of integrity in signal interception]. Previously, the gathering of information at the connection point according to the terms and conditions of the permit was executed by the FRA. The amendment was justified by the claim that increasing the credibility of signals intelligence required limiting access by the signals intelligence authority only to those fibres in a cable to which the permit applies.
[15] *Lag* (2007:259) *om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet* [Act on the handling of personal data in the defence intelligence and development operations of the National Defence Radio Establishment].
[16] *Lov om etterretningstjenesten* 1998-03-20 nr 11 [Act on the Norwegian Intelligence Service] and *Instruks om etterretningsstjenesten* FOR 2001-08-31 nr 1012 [Decree on the Norwegian Intelligence Service].

lishment. Pursuant to the Intelligence Service Act, it is responsible for detecting and analysing external threats and the motives, capabilities and methods of foreign operators. The purpose of intelligence work is to prevent threats and to lay a sound foundation for decision-making in foreign, security and defence policy. Steering and direction are undertaken by the Ministry of Defence, to which the NIS reports. Internal security is the responsibility of the Norwegian Police Security Service (*Politiets sikkerhetstjeneste, PST*).

The duties of the NIS are to acquire, process and analyse information concerning Norway's interests vis-à-vis foreign states, organisations and individuals, and on this basis to create threat analyses and intelligence assessments to such an extent as necessary for contributing to the safeguarding of key national interests.[17] However, the list of national interests given in the Act is not comprehensive. Assignments to the NIS are issued by the Ministry of Defence through the Chief of Defence. The NIS is required to prepare reports and to acquire information according to the needs of the Government and relevant ministries. The NIS has a statutory right to engage in international intelligence cooperation with other governments and international organisations; it also has a statutory obligation to collaborate with the defence alliances of which Norway is a member.

There are no provisions on the methods of gathering intelligence available to the NIS. However, intelligence-gathering is limited by law in that the NIS is not permitted to conduct surveillance on or gather information in secret on any Norwegian natural or legal persons within Norway; however, the NIS is permitted to gather information on Norwegian persons engaged in unlawful intelligence operations on behalf of a foreign power in Norway. In this case, the intelligence-gathering must be undertaken through or with the approval of the Police Security Service.

Cooperation between the NIS and the Police Security Service is provided for by decree.[18] Prioritised areas of cooperation include the combating of terrorism, the distribution of weapons of mass destruction and unlawful intelligence operations, and also other circumstances concerning important national interests. The agencies are required to provide mutual assistance in the execution of concrete intelligence-gathering operations, in the exchange of operational information and in the analysis and threat assessment of strategic information. It is a requirement for the cooperation that both parties comply with the provisions on their respective powers.

The monitoring of the NIS is provided for in the Act relating to the Monitoring of Intelligence, Surveillance and Security Services, which applies to all such bodies.[19] Under the Act, the NIS is monitored by a committee for the monitoring of intelligence, surveillance and security services elected

[17] Such key national interests include: a) the formulation of Norway's foreign, defence and security policy, b) readiness planning and crisis management, c) long-term planning and structural development of the Defence Establishment, d) capability of the operational units of the Defence Establishment, e) support for defence alliances of which Norway is a member, f) Norwegian troops involved in international military operations, g) Norway's participation in international disarmament and arms control agreements and their monitoring, h) international terrorism, i) transnational environmental problems and j) the dissemination of weapons of mass destruction and the equipment and materials required for manufacturing same.

[18] *Instruks om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste* 13. oktober 2006 nr. 1151 [Decree on cooperation between the Norwegian Intelligence Service and the Police Security Service].

[19] *Lov om kontroll med etterretnings-, overvåknings- og sikkerhetstjeneste* 1995-02-03 nr 07 [Act relating to the Monitoring of the Intelligence, Surveillance and Security Services].

by the Storting. The committee is independent of the Storting in its activities. The purpose of monitoring is to ascertain and prevent any exercise of injustice against any person, and to ensure that the means of intervention employed do not exceed those required under the circumstances, to ensure that the activities do not involve undue damage to civic life and to ensure that the activities are kept within the framework of statute law. Monitoring is undertaken both at the committee's own initiative and by processing complaints. The committee is guaranteed excessive access to the archives, registries and premises of the NIS in pursuit of its duties. The committee reports to the Storting on an annual basis.

4.3 Denmark

In Denmark, intelligence operations are undertaken by the Danish Defence Intelligence Service (*Forsvarets Efterretningstjeneste, FE*), a civilian agency under the Ministry of Defence. The duties, powers and the monitoring of intelligence operations are provided for in the Act on the Danish Defence Intelligence Service.

The FE is responsible for Denmark's foreign intelligence and military intelligence. It is also the national information security authority. The duties and operations of the FE are provided for in the Act on the Danish Defence Intelligence Service,[20] which was enacted in 2013 and replaced the earlier rather limited provisions incorporated in the Armed Forces Act.[21] The statutory duties of the FE are to create an intelligence basis for Denmark's foreign, security and defence policy, to help prevent and combat threats to Denmark and Danish interests, and for these purposes to gather, process and analyse information on foreign relations that is of relevance to Denmark and Danish interests abroad, and to report on the above. The FE is required to inform the Ministry of Defence of any emerging circumstances that are of relevance for Denmark and Danish interests, and of circumstances and matters affecting the domain of the FE. The FE may also undertake other duties related to the above if so decided by the Minster of Defence.

The provisions concerning the powers of the FE are general in nature. The FE is permitted to gather and acquire information that maybe of relevance to its intelligence operations. In the pursuit of its duties to gather information about foreign circumstances, it is also allowed to gather information on Danish citizens, Danish corporations and aliens resident in Denmark. More specific provisions than this on the powers of the FE are not given in legislation; there is no statutory distinction made between the various methods of gathering intelligence. According to public sources, information gathering is practised through human intelligence and signals intelligence (from satellites and terrestrial telecommunication lines); public sources are also used.[22] The processing of personal details is subject to the provisions of the Act on the Processing of Personal Data, regarding both natural persons and corporate bodies. The Act does not contain provisions on the information-gathering permit procedure.

[20] *Lov om Forsvarets Efterretningstjeneste* (602/2013) [Act on the Danish Defence Intelligence Service].
[21] *Lov om forsvarets formål, opgaver og organisation m.v.* (122/2011) [Act on the equipment, duties and organisation of the Armed Forces].
[22] http://fe-ddis.dk accessed 8 Dec 2014.

In addition to the FE, Denmark has the Danish Security and Intelligence Service (*Politiets Efterretningstjeneste, PET*), which is an arm of the police. There are no specific provisions governing operations abroad by the PET; however, according to the preparatory materials for the Act governing its operations,[23] it is considered to have the right to engage in joint human intelligence source operations with the FE and foreign intelligence services in Denmark and abroad. Human intelligence sources may also be sent abroad to gather information falling within the domain of the PET.

The FE and the PET may disclose to one another personal details and other information if such disclosure is of relevance to the carrying out of their duties. The aim is that the parties would not have to consider separately for each disclosure whether it is necessary or not. According to the state report proposing the enacting of Acts governing the FE and the PET, the functions of these two agencies are so closely connected that information exchange between them is largely tantamount to the disclosure of information within a government agency.[24]

The operations of the FE are monitored by the Ministry of Defence, the oversight committee, the Parliament's Committee on the Intelligence Services and, in budgetary terms, the National Audit Office.

The key task of the oversight committee is to monitor compliance with the law in the processing of personal details and registry administration in the operations of the intelligence and security services. It may investigate a matter involving the processing of personal details at its own initiative or at the request of a registered individual. It may also conduct inspections and reviews in the premises of the intelligence and security services, and it has a general right to obtain information from their person registries and their officials. The committee may issue statements and recommendations to the intelligence services.

The Parliament's Committee on the Intelligence Services is the parliamentary monitoring body for the intelligence and security services. The Government is required to inform the Committee of its policy outlines regarding the intelligence and security services as well as issues related to security or foreign policy that are of relevance to their operations. Any significant new duties assigned to the intelligence and security services must first be approved by the Committee.

4.4 Netherlands

4.4.1 Intelligence and security services

In the Netherlands, intelligence operations are conducted by the General Intelligence and Security Service of the Netherlands (*Algemene Inlichtingen- en Veiligheidsdienst, AIVD*) subordinate to the Ministry of the Interior, and the Military Intelligence and Security Service (*Militaire inlichtingen en veiligheid, MIVD*) subordinate to the Ministry of Defence. The duties and powers of both agencies

[23] *Lov om Politiets Efterretningstjeneste* [Act on the Danish Security and Intelligence Service].
[24] *Betaenkning om PET og FE* (1529/2012) [Committee report].

are provided for in the Intelligence and Security Services Act.[25] Each competent minister also has the authority to issue more detailed regulations concerning the organisation, working procedures and management of an agency in the ministry's administrative branch.

The AIVD and the MIVD are involved in both intelligence and counter-intelligence operations. The two agencies are required to provide mutual support in the execution of their duties. They have a joint coordinator for the harmonising of procedures. The directors of the intelligence and security services are obliged to support the coordinator in these duties.

The mandate of the AIVD is to uphold national security by acquiring information and evaluating groups, individuals and foreign powers that may jeopardise the democratic social order or vital national interests; by issuing security reports; by promoting action to secure vital national interests; and by compiling risk and threat analyses for protecting specific individuals, services and property.

The mandate of the MIVD is to uphold national security by acquiring information and evaluating the operational performance capability of the military forces of other countries; by conducting security screenings; by investigating and evaluating the status and organisation of the Dutch Armed Forces; by promoting the protection of the operational interests of the Dutch Armed Forces; and by compiling risk and threat analyses for protecting military targets and specific individuals, premises and services related thereto.

Legal provisions regarding powers are quite detailed in the Netherlands. The intelligence and security services are principally required to rely on information acquired from public sources or from partners. They are also allowed to exercise special powers defined by law, pursuant to which they may engage in human or signals intelligence operations, for instance.[26] Exercising the special powers is subject to a permit from the Minister of the Interior or the Minister of Defence. The exercising of special powers is subject for instance to the principle of least intervention and the principle of proportionality.

The intelligence and security services report to Parliament on their operations on an annual basis. Reports submitted by the competent ministers include a review of the past and future targets of the operations of the agencies.

The legality of the operations of the intelligence and security services is evaluated by an independent regulatory commission. This commission was set up to safeguard the right to respect for private life and the right to an effective remedy provided for in Articles 8 and 13, respectively, of the European Convention on Human Rights. The regulatory commission processes and investigates complaints filed against the intelligence and security services and submits its proposal regarding the resolution of a complaint to the competent minister. This proposal is not binding upon the minister. A complainant dissatisfied with the minister's decision may appeal to the National Ombudsman. In

[25] *Wet op de inlichtingen- en veiligheidsdiensten* 2002, *Intelligence and Security Services Act*, ISSA 2002 (English).
[26] The powers provided for in the Intelligence and Security Services Act concern *inter alia* surveillance, technical surveillance, covert operations, establishing covert organisations, guided use of informants, secret searches, secret opening of postal communications and infiltration of IT environments (e.g. decryption) and telesurveillance.

addition to the monitoring of legality, the regulatory commission issues advice and recommendations concerning the intelligence and security services to the ministers responsible for them.

The commission may conduct inspections and reviews in the premises of the intelligence and security services. It has a general right to obtain information relevant to its duties.

The Intelligence and Security Services Committee of the House of Representatives in the Dutch Parliament is the parliamentary special oversight body for the intelligence and security services. The Committee reports to Parliament.

4.4.2 Legislative development

Needs for reforming the Intelligence and Security Services Act were discussed in the report submitted by what was known as the Dessens committee on 2 December 2013.[27] According to this report, the Act is too technology-specific and has therefore become outdated because of advancements in telecommunications technology. The Act, as it now stands, prevents the intelligence services from effectively monitoring telecommunications over cable links.

The committee proposed that the intelligence and security services be given considerable broader powers for intelligence operations concerning telecommunications traffic over cable links. The Dessens report does not comment on how this monitoring would take place; however, it would presumably involve the sort of telecommunications traffic screening provided for in Swedish legislation. To balance the proposed extension to intelligence gathering powers, the committee proposed that the oversight of these powers should be further developed.

The Ministry of the Interior and the Ministry of Defence have taken action to put the recommendations of the Dessens report concerning telecommunications intelligence into practice.

4.5 Germany

Germany has three intelligence agencies at the federal level: the Federal Intelligence Service (*Bundesnachrichtendienst, BND*), the Military Counter-Intelligence Service (*Militärischer Abschirmdienst, MAD*) and the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz, BfV*). The BND is responsible for both civilian and military intelligence, while the MAD and the BfV are responsible for counter-intelligence in their respective fields. The mandate and powers of the BND and the MAD are provided for in the Acts governing them.[28] The operations of the BfV and the intelligence services of the Bundesländer are provided for in the Act Governing Cooperation between the Federal Government and the Federal States in Matters Concerning the Protection of the Constitution and the Federal Office for the Protection of the Constitution, which includes

[27] Evalutiecommissie Wet op de inlichtingen– en veiligheidsdiesten 2002.
[28] *Gesetz über den Bundesnachrichtendienst*, BNDG [BND Act] and *Gesetz über den militärischen Abschirmdienst*, MADG [MAD Act].

general provisions on intelligence operations that also apply to the operations of the BND and the MAD.[29]

The BND is subordinate to and reports to the Federal Chancellery. The duty of the BND is to collect and analyse information on foreign countries that may be of relevance to Germany's foreign and security policy. The BND is permitted to gather, process and use any information necessary for foreign intelligence work, including personal data, unless such processing would contravene the Federal Data Protection Act or other specific provisions. The BND may use methods of intelligence gathering at its disposal if the information required cannot be acquired by any other means and no other authority is responsible for gathering that information.

The BND may use secret methods, equipment and devices of intelligence gathering if essential to carry out its duties. The processing of personal data and the right of the persons concerned to obtain information is provided for in more detail in the Act on the Protection of the Constitution.

The Act limiting the privacy of correspondence, post and telecommunications (the 'G 10 Act')[30] provides for the right of the BND, the MAD and the BfV to monitor and record telecommunications and to open and inspect letters and other postal items. This Act contains provisions on when and how the fundamental rights guaranteed in Article 10 of the German Constitution[31] may be limited, on the protection of core privacy and on the disclosure of personal data. The Act also provides for oversight of intelligence work.

The G 10 Act also specifically provides for the right of the BND to acquire information from international telecommunications. Such acquiring of information must be operationally essential and is subject to a permit granted by a federal minister jointly with the G 10 Commission, which will be discussed below. The automatic search terms to be used in intelligence targeting international telecommunications must be specified in both the permit application and the permit itself. Search terms are only permitted if they are connected to the investigation of specific threats listed in the Act.[32] Pursuant to the Act, the intelligence and security services are allowed to screen no more than 20% of all international telecommunications using the specified search terms.

[29] *Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz*, *Bundesverfassungsschutzgesetz*, BVerfSchG [Act governing cooperation between the Federal Government and the Federal States in matters concerning the protection of the Constitution and the Federal Office for the Protection of the Constitution].

[30] *Gesetz zur Beschränkung des Brief-*, *Post- und Fernmeldegeheimnisses* [Act limiting the privacy of correspondence, post and telecommunications].

[31] Privacy of correspondence, post and telecommunications.

[32] Under section 5 of the G 10 Act, information searches constituting an infringement of fundamental rights are only permissible if necessary for identifying any of the following threats: a) an armed attack against Germany, b) an international terrorist attack with an immediate connection to Germany, c) international dissemination of military weapons or illegal foreign trade in armaments, computer software or technology of substantial significance, d) import of drugs into the EU by professional or organised criminals with substantial significance for Germany, e) undermining of the value of the euro undertaken from abroad, f) internationally organised money laundering of substantial significance, or g) smuggling of foreign nationals to the EU by professional or organised criminals.

In human intelligence, the intelligence and security services are permitted to acquire information from human intelligence sources and to direct them. They may also use false identification and misleading registry entries.

The key oversight bodies are the Parliamentary Control Commission[33] and the G 10 Commission, along with the Data Protection Ombudsman and the Federal Chancellery, which supervises the BND.

The Parliamentary Control Commission oversees all three intelligence agencies insofar as their operations are not subject to the G 10 Act. The Commission may conduct inspections and reviews in the premises of the intelligence and security services and has a general right to obtain information. The Commission reports to the Federal Parliament at regular intervals.

The G 10 Commission oversees exceptions to the privacy of communications. The Commission decides, at its own initiative or on the basis of complaints, whether infringements of Article 10 of the Constitution are permissible and necessary. Supervisory activities by the Commission concern the processing of personal data by the intelligence agencies and notifying the persons concerned thereof. The Commission has a general right to obtain information within the scope of its duties and the right to conduct inspections and reviews in the premises of the intelligence and security services.

The Data Protection Ombudsman oversees the application of data protection legislation.

5. EVALUATION OF THE CURRENT STATE

The duty of the national security authorities is to anticipate and prevent harmful actions and measures that may jeopardise national interests of particular importance. Serious security threats may be targeted at Finland from beyond its borders. The development of cyber networks has made physical distance less relevant in the implementation of threats.

The national security authorities engage in intelligence work required for the execution of their statutory duties. However, there are no statutory powers for intelligence work. Intelligence work is exclusively based on public sources and on information acquired through international cooperation and other voluntary cooperation.

5.1 Telecommunications technology and threats to national security

As shown in chapter 2 of the present report, ICT advancements are of significance for the emergence of threats to national security in two ways.

[33] *Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes* [Act on the parliamentary control of Federal intelligence operations].

Cyber networks are used as a tool for communicating about plans and intentions concerning actions to be taken in the real world. In other words, networks are not in this case used as a means of execution, but as a means of planning and preparation. The actions concerned may be military (armed attack) or aimed at national interests other than territorial integrity (e.g. espionage, terrorist attack, export of dual-use items).

Secondly, networks may be used as an actual means of execution of seriously harmful attacks against a specific target, such as the Finnish government. Such actions may include military cyber operations as specified in Finland's Cyber Security Strategy or actions that may be described as cyber espionage or cyber terrorism.

The detection of cyber threats and communication concerning them, the identification of the parties behind them and the investigation of the nature of the threat are cornerstones of the ability to prevent actions jeopardising national security from being realised. The party responsible for such prevention must be able to gain information about threats or communications concerning such threats at an early stage.

5.2 Capability of organisations to detect cyber threats against them

Enterprises, organisations and authorities who use cyber networks protect themselves against cyber threats with information security. The rights to take action to safeguard information security are provided for in section 272 of the Information Society Code. This provision gives enterprises, organisations and authorities tools for detecting and combating cyber actions against them. Detection measures are undertaken on a decentralised basis with their quality and level varying from one organisation to another. Section 272 of the Information Society Code and its predecessor, section 20 of the Act on the Protection of Privacy in Electronic Communications, have also enabled the development of a centralised detection system for information security threats (HAVARO) to protect bodies considered critical for the overall security of society.

The harmful programs that are the most difficult to detect, yet have the capacity to inflict the greatest damage on national security are spyware and other malicious software programs used by governmental actors. Identifiers for such programs are data at a high level of classification, and as such are typically exchanged in the context of international cooperation between intelligence and security services. Because the Finnish Communications Regulatory Authority (FICORA) is not and cannot be a party to this confidential cooperation, those identifiers whose importance for the protection of national security is the greatest cannot be disclosed to the HAVARO system.

The purpose of the information security measures enabled by section 272 of the Information Society Code, including HAVARO, is to implement information security by protecting individual target organisations from attacks. Information security measures are not intended to satisfy information needs related to the combating of actions jeopardising national security. From the perspective of the parties implementing information security measures, information essential for maintaining na-

tional security (such as the reasons, circumstances, perpetrators and background motives of the most serious information security infringements) is not crucially relevant.

5.3 Intelligence gathering powers

The powers of the police and the Defence Forces to use secret methods of intelligence gathering are linked to the concept of criminal activity in legislation. According to the Police Act, *preventing an offence* means action aimed at preventing an offence, attempted offence or the preparation of an offence when, due to observations of a person's actions or information otherwise obtained on the person's actions, there are reasonable grounds to believe that he or she would commit an offence; or action aimed at interrupting the commission of an offence already in progress; or at limiting the injury, damage or danger directly caused by it. Secret methods of intelligence gathering may be used to prevent the preparation of an offence even if the preparation of that particular offence is not in itself punishable.

Although secret methods of intelligence gathering may also be used for preventing the preparation of an offence and the scope of application of these methods is thus broad, it is obvious that today secret methods cannot be used just for gathering intelligence about plans threatening national security that have not yet progressed to the stage of preparing an offence or that are not in themselves punishable.

5.4 Notes on the international comparison

All the reference countries discussed in the present report have legislation on intelligence work. Intelligence legislation may include provisions on intelligence gathering in cyber networks. The precision of the provisions varies by country. It is therefore not possible to draw direct conclusions from the legislation of the reference countries on the individual methods of intelligence gathering in use. There are also differences in how specifically legislation defines the threats for the combating of which intelligence gathering is permissible.

In the reference countries, intelligence operations are either the responsibility of a single intelligence agency or divided into civilian and military intelligence services. The demarcation of intelligence gathering powers between the civilian and military authorities principally depends on whether the threat being investigated is civilian or military in nature. Intelligence services are generally subordinate to the Ministry of Defence and/or the Ministry of the Interior. Assignments for intelligence gathering may be given by the government leadership, the competent ministries or, for instance, from the command of the armed forces.

In the reference countries, it has been considered important to enact legislation on the oversight of intelligence work. Such oversight takes the form of both parliamentary and independent judicial oversight, in addition to internal supervision within the administrative branch. Judicial oversight is the responsibility of a party independent of the intelligence service in question such as a permanent independent control committee or inspection board. An oversight body typically monitors the

legality of intelligence work and the methods used, either at its own initiative or on the basis of complaints. The oversight bodies typically have unlimited access to the premises and documents of their respective intelligence services. The members of the oversight bodies are bound by secrecy. The oversight bodies usually report on their observations to the competent minister and to the object of inspection, both for individual cases and in their annual reports. Another purpose of judicial oversight is to safeguard the right to an effective remedy guaranteed by the European Human Rights Convention.

Legislation in the reference countries also includes provisions on the methods of intelligence gathering infringing on the right to privacy being a last-resort measure, on the permit procedures related to their use and on the processing of the personal data thus acquired, among others.

5.5 Relationship between the duties and the powers of the security authorities

Section 3.1 of the present report discusses the duties of the Finnish Security Intelligence Service and the Defence Forces. What these duties share is the concept of combating threats against national security. Combating threats requires an ability to detect them and to acquire information about them at a sufficiently early stage.

It is the duty of the Finnish Security Intelligence Service to prevent and detect plans and offences that might compromise the government or public order, or internal or external national security, and to a lesser extent to investigate such offences. The concept of 'plan' is not specified in the Police Administration Act or in its preparatory materials. A plan cannot be considered to be an offence, and thus in this respect the duties of the agency involve an intelligence assignment and not a crime prevention assignment. There are no provisions on intelligence gathering powers.

In the Defence Forces, crime fighting – i.e. the prevention and detection of offences – is the responsibility of military counter-intelligence. Military counter-intelligence is distinct from military intelligence, which generally follows developments in Finland's security environments, identifies changes therein and produces information on the current situation. Military intelligence is aimed particularly at military policy development and military development in Finland's neighbouring areas. The duties of military intelligence are not crime fighting. There is no legislation on military intelligence.

There are no provisions concerning the intelligence gathering powers of authorities combating threats against national security or on the division of these powers between civilian and military authorities. In current legislation, the intelligence gathering powers of the authorities are based almost exclusively on crime fighting rather than intelligence work.

Uncertainty factors in the changing security environment heighten the need to produce objective, confirmed and analysed information on security threats against Finland to support decision-making by political leaders and by the security authorities. Only accurate information acquired as early as possible concerning the intentions and plans of the parties behind the threats can guarantee suffi-

cient capacity for giving early warning of them. Early intelligence will improve the response capability of Finnish society and broaden the range of means available for preventing or preparing for the realisation of such threats. It is also vital from the perspective of preparedness for extraordinary circumstances that information on military threats against Finland be obtained under normal circumstances.

The current situation may be deemed unsatisfactory considering the changes that have occurred in the security environment. We should safeguard the continued functioning of Finnish society in the face of particularly serious external threats and attacks on our critical infrastructure. It is crucial for national security to obtain information at an early stage on the changes happening in Finland's security environment, not just through intelligence gathering aiming at a criminal investigation. What would be essential would be to acquire information on the current situation and analyse its meaning for Finland's national security.

6. DEVELOPMENT PROPOSALS

Finland's external security environment and the nature of warfare are changing at an accelerating pace. Accordingly, the intelligence gathering methods available to the authorities should be further developed. The current powers do not enable sufficiently early and effective detection of threats or allow for taking the required measures, including issuing military early warnings. The dissemination and use of disinformation heightens the need for the security authorities to produce objective, confirmed and analysed information to support decision-making by the senior government leadership and the military.

Intelligence is a broad field and involves a variety of methods of intelligence gathering. As the above international comparison indicates, governments typically do not legislate on a single method of intelligence gathering. No individual method can guarantee the acquisition of all necessary information concerning national security; instead, information must be gathered and confirmed using mutually complementary methods of intelligence gathering.

Below, we discuss three methods of intelligence gathering that in the working group's opinion would yield information that is particularly relevant for Finland's national security. These are *telecommunications intelligence, foreign human intelligence* and *foreign information systems intelligence.* They are not mutually exclusive since they differ in nature. The purpose of telecommunications intelligence is above all to detect international threats, while foreign human intelligence and foreign information systems intelligence mainly involve gathering information on threats already identified.

6.1 Telecommunications intelligence

6.1.1 General

Due to the changes described in chapter 2 of the present report, telecommunications intelligence plays a vital role in the detection of threats against national security. The majority of global communication between private individuals, enterprises and public entities is nowadays carried in cable telecommunications networks. The telecommunications equipment and cables located in Finnish territory carry not only domestic telecommunications traffic but also international traffic. International telecommunications traffic is defined as traffic that originates in Finland and terminates outside Finland's borders, and international through traffic that both originates and terminated outside Finland. Because of advancements in telecommunications technology, it is the information carried in telecommunications cables that is of crucial importance for detecting threats.

The importance of cable-borne telecommunications for combating threats against national security has been acknowledged in several Western countries comparable to Finland. The international comparison above shows that legislation in most reference countries allows the authorities to target cable networks in intelligence work, or such legislation is being planned.

Telecommunications intelligence involves an authority acquiring information relevant for national security from the content of telecommunications traffic. Telecommunications intelligence may target traffic within a country or cross-border traffic. Implementing such operations requires the intelligence authority to have access to the telecommunications cable connection points. Typically, intelligence operations are guided by using automatic search terms to screen the traffic. This means that telecommunications intelligence infringes on the confidentiality of correspondence. When considering development proposals, the international agreements binding upon Finland and the provisions of the Finnish Constitution must be taken into account.

6.1.2 Requirements of international human rights agreements and the Constitution

6.1.2.1 International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights was adopted by the General Assembly of the United Nations in 1966 and became binding upon Finland in 1976 (SopS 8/1976).

What is of particular importance for confidentiality of correspondence is Article 17, which states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Moreover, everyone has the right to the protection of the law against such interference or attacks. The provisions of the Article may only be derogated from in time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed.

The prohibition in Article 17 on interference with privacy and correspondence is not absolute; it only concerns "arbitrary" and "unlawful" interference. The States Parties may, in their national legislation, provide for situations in which such interference is allowed and for the means permissible in such cases. Indeed, all States Parties have legislation in place allowing such an infringement of rights for the purpose of crime fighting, and many also allow it for the purpose of upholding national security.

The implementation of the Convention is supervised by the UN Human Rights Committee, which is constantly updating the interpretation of its provisions. In General Comment no. 16 (A/43/20, 1988), the Human Rights Committee interprets the content of Article 17 from the perspective *inter alia* of electronic communications. According to the General Comment, it is not sufficient to enact legislation concerning the protection of privacy. Legislation authorising interference with that protection must not be arbitrary in content, nor may it be arbitrarily applied. Interference authorised by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant. Relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorised interference must be made only by the authority designated under the law, and on a case-by-case basis. The information thus gathered must be information the knowledge of which is essential in the interests of society. Information relating to an individual's private life must not be used for purposes inconsistent with the purpose of the Covenant.

Several complaints regarding infringements of Article 17 have been filed under the Optional Protocol to the Covenant, but so far the Human Rights Committee has not handled any matters related to cyber security or electronic communications. It may be considered likely that issues related to the confidentiality of electronic communications will become more important in the work of the Committee.[34]

6.1.2.2 Article 8 of the European Convention on Human Rights

In estimating the permissibility of enacting legislation on telecommunications intelligence, the aforementioned Covenant is of less practical importance than the European Convention of Human Rights, adopted by the Council of Europe in 1950, to which Finland acceded in 1989 (SopS 63/1999). Compliance with the Convention is monitored by the European Court of Human Rights (ECHR), which hears and rules on complaints concerning infringements of the Convention. The ECHR has in multiple decisions addressed the issue of how to interpret the right to confidential communications as defined in the Convention. Many of these decisions concern electronic communications; some involve telecommunications intelligence or comparable activities by the authorities.

[34] For instance, the fourth periodic report of the USA on the implementation of the Covenant (CCPR/C/USA/4) discusses electronic telecommunications surveillance in detail. In the list of issues submitted to the USA, the Committee requested further information on the legal supervision of electronic telecommunications surveillance undertaken by the National Security Agency in the USA and beyond its borders (CCPR/C/USA/Q/4).

Under Article 8(1) of the European Convention on Human Rights, everyone has the right to respect for his private and family life, his home and his correspondence. However, this right is not an illimitable one; Article 8(2) states that there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

According to the case-law of the ECHR, the concepts of "private life" and "correspondence" in Article 8(1) of the convention include telephone communications, e-mail communications and other electronic communications intended as confidential (e.g. *Klass and others v Germany; Kopp v Switzerland; Copland v United Kingdom; Liberty and others v United Kingdom*). The protection covers both the content and identification data of communications (e.g. *Malone v United Kingdom; Weber and Saravia v Germany; P.G. and J.H. v United Kingdom*). Regarding identification data, the Court has noted separately that information on the phone numbers that a person has called, for instance, constitute an integral part of the communications. Hence, the disclosure even of such data to the authorities without the consent of the person making the communication constitutes an infringement of that person's privacy (*Malone v United Kingdom*).

Infringement of privacy need not involve the actual processing of data by an authority; even the collecting of data and storing it for later use by an authority must be considered an infringement (*Marper v United Kingdom*). The mere existence of legislation that allows the secret monitoring of communications infringes upon the rights of the communicating parties and potential targets under Article 8 of the Convention (*Klass v Germany; Liberty and others v United Kingdom*). The potential targets of monitoring must in such a case have the right to an effective remedy before a national authority as provided for in Article 13 of the Convention. Article 13 states that everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

Even if the probability of secret monitoring being targeted at a person were low, that person must be able to have his or her allegation of rights infringement under Article 8 of the Convention heard at the ECHR if there are no effective domestic remedies available (*Kennedy v United Kingdom*).

Permitted infringement of the rights guaranteed by Article 8(1) of the European Convention on Human Rights

The fact that both the content and identification data of communications are covered by Article 8 of the European Convention on Human Rights does not mean that the authorities can never interfere with them. The authorities may interfere with the privacy of individuals to quite a large extent if it is justifiable under Article 8(2) of the Convention. Article 8(2) sets three conditions for the authorities being allowed to infringe upon the rights provided for in Article 8(1): 1) such interference must be *in accordance with the (national) law*; 2) it must be *in the specific interests listed in the provision*, and 3) it must be *necessary in a democratic society.* One of the items in the interests of

which the protection of privacy and hence the confidentiality of communications may be infringed upon is national security.

Requirement of being in accordance with the law

Infringements of the rights provided for in Article 8 of the Convention must be in accordance with national law. The importance of this requirement is particularly relevant when the infringement is kept secret from the target. The limits to and exercising of the discretion of the authorities must be defined clearly enough in law to avoid the potential for arbitrariness inherent in the secret use of executive powers (*Malone v United Kingdom; Amann v Switzerland; Telegraaf Media Nederland Landelijke Media B.V. and others v Netherlands; Rotaru v Romania*).

The ECHR has repeatedly stated in its decisions that any law allowing the authorities to take secret action infringing upon the protection of privacy must be consistent with the rule of law, available to citizens and of such quality that citizens are able to foresee what its application would mean in their particular case (e.g. *Kruslin v France; Huvig v France; Lambert v France*). It must be "sufficiently clear in its terms" to give "an adequate indication" of in what circumstances and by what criteria citizens may become the target of secret measures undertaken by the authorities (*Kopp v Germany; Kruslin v France, Huvig v France*). The law may not be such that it allows the secret surveillance of any random person (*Amann v Switzerland*).

In evaluating whether the requirement of foreseeability is fulfilled, the relevant decrees and official regulations must be taken into account in addition to the actual legislation (acts). An act may contain provisions that are very general in nature, being further specified by lower-level instruments. However, these must be published in order to qualify; internal directives not available to citizens do not fulfil the foreseeability requirement (e.g. *Silver and others v United Kingdom; Malone v United Kingdom*). A generally available law must define at least: the nature and scope of powers of secret surveillance; the categories of persons against whom the powers may be used; the nature of activities giving rise to the exercising of the powers; the procedures to be observed in inspecting, using, storing, forwarding and deleting data obtained through the powers; and provisions on how the powers are overseen and means of legal recourse (*Amann v Switzerland; Valenzuela Contreras v Spain; Prado Bugallo v Spain; Shimovolos v Russia*). The requirements for the foreseeability of legislation are the same regardless of whether the legislation concerns the surveillance of communications of individual persons because of a suspected offence or extensive general surveillance of communications because of a threat (*Weber and Saravia v Germany; Liberty and others v United Kingdom*).

The ECHR evaluated whether the surveillance of a volume of international communications is in compliance with the Convention in two important decisions. In *Liberty and others v United Kingdom,* the Court ruled that the national legislation allowing general programmes of surveillance was of such quality that it did not comply with the requirement of Article 8(2) of the Convention that secret surveillance must be in accordance with the law. In *Weber and Saravia v Germany*, the Court gave an opposite ruling: that the national legislation did fulfil the quality requirements and was thus in compliance with the Convention.

The case of *Liberty and others v United Kindgom* involved an extensive surveillance operation targeting international telephone traffic undertaken by a signals intelligence agency under the Ministry of Defence of the UK, where up to 10,000 phone channels could be intercepted at once. It was undisputed in the case that the operation was in accordance with national legislation.[35] Under this legislation, the Home Secretary could issue a warrant to various security authorities concerning surveillance of telecommunications between the UK and foreign countries. Warrants covered very broad classes of communications, for example "all commercial submarine cables having one terminal in the UK and carrying external commercial communications to Europe". At the time of issuing an interception warrant, the Home Secretary was required to issue a certificate containing a description of the intercepted material which he considered should be examined. However, the relevant Act allowed extremely broad discretion; it was sufficient that the intelligence to be gathered was necessary for "national security", "preventing or detecting serious crime" or "safeguarding the economic well-being of the United Kingdom". The Home Secretary, when issuing a warrant for the interception of external communications, was called upon to "make such arrangements as he consider[ed] necessary" to ensure that material not covered by the certificate was not examined and that material was [*sic*] certified as requiring examination was disclosed and reproduced only to the extent necessary. The Act contained no further specifications about the content or scope of these provisions. Having received a warrant from the Home Secretary, the security authorities would independently select the automatic search terms used to filter the intelligence pertaining to national security, or the other interests listed in the Act, out of the total volume of communications. The security authorities had their own internal regulations applying to the processes of selection for examination, dissemination, storage and deletion of the intercepted material, but details of these arrangements were not contained in legislation or otherwise made available to the public.

In its decision, the ECHR noted that pursuant to the Act, under a warrant from the Home Secretary any person who sent or received any form of telecommunication outside the British Islands could have had such a communication physically intercepted. Therefore the security services had in fact been granted unlimited discretion with regard to intercepting foreign communications. The Act also conferred a wide discretion on the authorities s regards which communications were listened to or read. It was sufficient that the Home Secretary considered the examination necessary for national security or other interests generally described in the Act. The Act contained no detailed provisions on the processing of non-relevant communications, and the instructions issued by the Home Secretary were not made public. In conclusion, the ECHR did not consider that the domestic law at the relevant time indicated with sufficient clarity the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. Therefore the signals intelligence legislation of the UK was not in compliance with the quality requirements of Article 8(2) of the European Convention on Human Rights and was found to be in violation of the Convention.

[35] *Interception of Communications Act* 1985.

The case *Weber and Saravia v Germany* involved extensive, "strategic monitoring" of mobile phone traffic between Germany and foreign countries conducted by the Federal Intelligence Service (BND) and provided for in a national Act.[36] The Act in question allows strategic monitoring of telecommunications in order to identify and avert serious dangers facing Germany, such as an armed attack on its territory or the commission of international terrorist attacks, international arms trafficking, the illegal importation of drugs in substantial quantities, the counterfeiting of money committed abroad, and the laundering of money in the context of the acts listed above. The order for executing each strategic monitoring measure was issued by the Federal Minister, having first consulted the Parliamentary Supervisory Board. The automatic search terms that were to be used for filtering the mobile phone traffic had to be given in both the BND's application and the order issued by the Minister. The Act contained provisions on how the filtered material was to be handled, and in which cases data on persons emerging through the filtering could be used for the prevention, detection and investigation of offences. The Act further contained provisions on cases in which the filtered data were to be considered irrelevant and how irrelevant data should be dealt with. The Act also provided for the duration of the monitoring, the retention period for filtered data, the destroying of the data and the limits and precautions concerning the transmission of data to other authorities.

The ECHR ruled that the German legislation satisfied the requirements of quality and foreseeability referred to in Article 8(2) of the European Convention on Human Rights. What was important in this respect was *inter alia* that the Act specified the threats for the combating of which monitoring was permissible. The Act was also considered to specify with sufficient accuracy which categories of persons could legally be targeted in the monitoring.[37] The automatic search terms used for screening must, according to the Act, be explicitly given in the orders concerning the monitoring measure, meaning that the authority executing the monitoring did not have unlimited discretion in determining them. It was also relevant for the fulfilment of the foreseeability requirement that the Act specified the maximum durations of the orders and included provisions on procedures that had to be followed when examining and using the data. The ECHR further ruled it relevant that the Act provided for limits and precautions concerning the transmission of data to other authorities and circumstances in which the data had to be destroyed. In its ruling on *Weber and Saravia*, the ECHR remarked separately that strategic monitoring of telecommunications on German soil essentially cannot interfere with the territorial sovereignty of other states even if the other party in a transmission is in another country.

National security as an interest allowing interference

National security is one of the interests that under Article 8(2) of the Convention may allow interference with the protection of privacy. In its case-law, the ECHR has only rarely questioned the claims of

[36] *Gesetz für Beschrenkung des Brief-, Post- und Fernmeldegeheiminisse* 1968 [Act on the limiting of the privacy of correspondence, post and telecommunications] and *Verbrechenbekämpfungsgesetz* 1994 [Act on crime fighting].
[37] "[T]he persons concerned had to have taken part in an international telephone conversation via satellite connections [...] [and] had to have used catchwords capable of triggering an investigation into the dangers listed [an armed attack on Germany, international terrorism, etc.]."

the respondent States that infringements have been undertaken because of national security.[38] It would seem that governments have considerable latitude of discretion in considering what activities threaten national security and thereby allow interference with the rights provided for by Article 8 of the Convention. Underlying this is the notion that national security traditionally belongs to the domain of sovereignty (*Bucur and Toma v Romania*). The decision history of the ECHR clearly demonstrates that at least military defence, combating terrorism and combating unlawful intelligence operations fall within the purview of national security (e.g. *Klass v Germany, Weber and Saravia v Germany*). However, national security may be subject to a variety of threats that are difficult to anticipate or to define in advance. It follows from this that further specification of the concept must principally be left to national practice (*Kennedy v United Kingdom*). The latitude of discretion that governments have may be partly augmented by the fact that the distinction between national security and the other interests allowing interference with the rights provided for in Article 8(1) of the Convention (such as public safety or the prevention of disorder or crime) may be vague in any given case.[39]

Necessity of interference in a democratic society

The third and final requirement for the authorities being allowed to interfere with the exercise of rights provided for in Article 8 of the Convention is for such interference to be necessary in a democratic society. The word "necessary" must be considered as somewhat non-specific, considering that the ECHR has noted: "the adjective 'necessary' is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable' " (*Handyside v United Kingdom*). It seems likely therefore that 'necessary', as referred to in Article 8, ranks somewhere between "indispensable" and "desirable".

The requirement of interference being necessary in a democratic society implies that such interference must "correspond to a pressing social need". It also implies that such interference must comply with the principle of proportionality: the interference must be in reasonable proportion to the interest referred to in Article 8(2) of the Convention that is claimed as justification (e.g. *Gillow v United Kingdom; Silver and others v United Kingdom; Handyside v United Kingdom*).

The responsibility of evaluating the necessity of interference as regards social need and proportionality is principally or at least initially the task of national legislators and national authorities (*Silver and others v United Kingdom; Handyside v United Kingdom*). National authorities have a certain margin of discretion in conducting such evaluation, depending for instance on which rights enshrined in the Convention the interference concerns, how far-reaching that interference is and which interest referred to in Article 8(2) of the Convention is claimed as justification. The margin of discretion is broader than usual when the interest claimed is national security (*Klass and others v Germany; Leander v Sweden*). The relatively broad discretion allowable to the government in issues of national security also applies to the concrete means and methods used by the government to protect that interest. In its decision in the case of *Weber and Saravia v Germany*, the ECHR ruled

[38] However, the ECHR has been sceptical on whether information on a person's political affiliation dating from 1937 could be relevant for national security 60 years later (*Rotaru v Romania*). The Court has also ruled that the smuggling of cigarettes cannot be a matter of national security even if a military airfield is used for the smuggling (*Dumitru Popescu v Romania*).
[39] The partial overlap of interests in this manner is referred to for instance in the judgment in *Silver and others v United Kingdom*.

that the government was within its rights to legislate on extensive telecommunications surveillance as a method for protecting national security. The case involved interference with the rights guaranteed to private persons in Article 8 of the Convention that was necessary in a democratic society.

In other contexts, the ECHR has stressed that secret surveillance and monitoring powers exercised by the authorities in the name of national security may constitute a danger to the democratic social order (e.g. *Antunes Rocha v Portugal*). For this reason, the government must provide for objective supervisory machinery and effective legal remedies. The decisions of the parties supervising the legality of the operations must be legally binding upon the agencies being supervised; it is not sufficient for protecting democracy that the supervisors can steer the agencies being supervised through recommendations (*Segerstedt-Wiberg and others v Sweden*). Legal regulation of secret powers must be public and specific enough for supervision of legality to be effectively conducted (*Liberty and others v United Kingdom*), though without compromising the purpose of the secret intelligence gathering (*Segerstedt-Wiberg and others v Sweden*). It is also relevant for the protection of democracy that the national parliament be involved in the oversight of secret powers of intelligence gathering (*Campbell v United Kingdom; Leander v Sweden*).

6.1.2.3 Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union, which entered into force in 2009, defines the fundamental rights that apply at the Union level. The Member States are obliged to comply with the Charter when they are implementing Union law. Under Article 7 of the Charter, everyone has the right to respect for his private and family life, home and communications. Article 8 of the Charter states that everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.

Article 52 of the Charter provides for the scope of the rights guaranteed in the Charter. According to paragraph 1, any limitation on the exercise of the rights and freedoms recognised in this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. Paragraph 3 of the same Article states that in so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

It follows from Article 52(3) of the Charter that Article 7 of the Charter is equivalent in content to Article 8 of the Convention. It is specifically stated in the preamble to the Charter that this Charter

reaffirms the rights as they result, in particular, from the European Convention for the Protection of Human Rights and Fundamental Freedoms and the case-law of the European Court of Human Rights. The extensive case-law of the ECHR concerning Article 8 of the Convention must therefore be considered to be of relevance for the application of Article 7 of the Charter.

Notwithstanding the above, oversight of compliance with the fundamental rights guaranteed in the Charter falls within the domain of the Court of Justice of the European Communities (CoJ) and national courts and not with the ECHR. What is of relevance for telecommunications intelligence is the decision issued by the CoJ in April 2014[40] invalidating the Data Retention Directive adopted in 2006. This Directive had imposed on the Member States the requirement to legislate on the comprehensive retention of telecommunications identification data for the purpose of combating and investigating serious crimes.

The CoJ ruled in its aforementioned decision that the Data Retention Directive violated the principle of proportionality referred to in Article 52(1) of the Charter. The principle of proportionality requires that an infringement of a fundamental right must be necessary in order to be permissible. In evaluating the necessity of infringement of rights undertaken pursuant to the Data Retention Directive, the CoJ noted that the requirement for retention of telecommunications identification data in the Directive covered, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime. The Directive applied even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Therefore the Directive entailed an interference with the fundamental rights of practically the entire European population.

According to the CoJ, the Directive should have included at least some[41] of the following elements in order to comply with the principle of proportionality:

- Objective restrictions related to the purpose of the Directive defining criteria according to which the telecommunications identification data for particular persons may be retained.
- More specific criteria by which to determine the offences for the prevention or investigation of which national authorities may be allowed access to and use of retained identification data. The Directive simply refers in a general manner to ‘serious crime’, as defined by each Member State in its national law.
- Substantive and procedural conditions relating to the access to the data and to their subsequent use. Access by the competent national authorities to the data was not made dependent on a prior review carried out by a court or by an independent administrative body; the Directive merely provided that each Member State is to define the procedures to be followed.

[40] Judgment on joined cases C-293/12 ja C-594/12.
[41] The Constitutional Law Committee considered that the judgment of the ECHR was based on an overall assessment of the Directive in question (PeVL 18/2014 vp, p. 6).

- Specific provisions on the retention periods for identification data. The Directive required that those data be retained for a period of at least six months, without any distinction being made between categories of data on the basis of their possible usefulness for fighting crime.
- Sufficient safeguards to ensure effective protection of the data retained against the risk of abuse. The Directive allowed providers of publicly available electronic communications services or of public communications networks to have regard to economic considerations when determining the level of security which they apply.
- A requirement for the data in question to be retained within the European Union.

The Constitutional Law Committee of the Finnish Parliament commented on the CoJ judgment in its statement PeVL 18/2014 vp. According to the Committee, an answer to the question of exactly what kind of national legislation would satisfy the requirements of proportionality in the protection of privacy and personal data cannot be directly obtained from the judgment. The Committee considers that at the very least it must be considered a violation of the requirement of proportionality to enact legislation specifying broad, non-differentiating, long-term and unlimited retention of data, combined with non-differentiating and unlimited access by the authorities to those data. The Committee further noted that it cannot be read from the judgment whether a requirement of retention enacted in view of the needs of the authorities covering data on practically all persons who use electronic communications in itself constitutes a violation of the principle of proportionality.[42]

The CoJ noted in its judgment that the Directive should have imposed objectively defined limits related to its purpose as to which identification data may be retained. The Directive should also have defined in more detail the offences for the combating of which the requirement of retention was imposed. What is important here is to realise that the CoJ judgment does not actually create new law. It is consistent with the established case-law of the European Court of Human Rights. The ECHR has issued a considerable number of decisions where it has, in line with the CoJ judgment but in more detail, addressed the elements that an Act sanctioning infringements of the protection of privacy must include in order to comply with the principle of proportionality and the requirement of foreseeability. The most important decisions of the ECHR in this respect, addressing telecommunications intelligence or related operations, are *Klass v Germany* (1978), *Weber and Saravia v Germany* (2006) and *Liberty and others v United Kingdom* (2008).

6.1.2.4 Requirements deriving from the Constitution of Finland on legislation restricting the protection of confidential correspondence

Rule of law

Under section 2(3) of the Constitution, the exercise of public powers shall be based on an Act, and in all public activity, the law shall be strictly observed. If any new duties are assigned to and new powers conferred on the authorities through intelligence legislation, both the duties and the pow-

[42] PeVL 18/2014 vp, p. 6.

ers must be defined in the legislation. Legal protection of the persons subjected to the exercise of these powers must also be enshrined in legislation.

Fundamental rights

Fundamental rights are generally not absolute in nature even if the provisions regarding them are formulated so as to afford protection, and even if such provisions do not reserve the right of restriction or refer to other legislation. In such cases, the issue of infringement of a fundamental right is resolved according to the general principles of infringement of fundamental rights.

The Constitutional Law Committee has outlined a number of general requirements concerning the infringement of fundamental rights, derived from the overall framework of fundamental rights and the nature of fundamental rights as rights protected by the Constitution (PeVM 25/1994 vp, pp. 4–5). These requirements are:

1. The infringement must be provided for by law.
2. The Act in question must be precise and delimited.
3. The infringement must be acceptable.
4. The infringement must be proportional.
5. The core of the fundamental right concerned must remain inviolable.
6. Sufficient legal protection must be provided.
7. Human rights requirements must be complied with.

Protection of confidential correspondence

Under section 10 of the Constitution, everyone's private life, honour and the sanctity of the home are guaranteed, and the secrecy of correspondence, telephony and other confidential communications is inviolable. The underlying principle is that an individual is entitled to live his or her life without the authorities or any other outside party arbitrarily or unnecessarily interfering with his or her private life. The section guarantees everyone the right to confidential communication without outside parties unlawfully gaining information on the content of confidential messages sent by or to him or her.[43]

Under section 10(3) of the Constitution, measures encroaching on the sanctity of the home, and which are necessary for the purpose of guaranteeing basic rights and liberties or for the investigation of crime, may be laid down by an Act. In addition, provisions concerning limitations of the secrecy of communications which are necessary in the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, as well as during the deprivation of liberty may be laid down by an Act. These criteria for infringing on the protection of confidential communications were intended as an exhaustive list when introduced in the fundamental rights reform (HE 309/1993 vp, p. 54). Unlike Article 8 of the European Convention on Human Rights, section 10(3) of the Constitution does not mention national security as an

[43] HE 309/1993 vp.

interest allowing for the enacting of legislation infringing on the protection of confidential communications.

The Constitutional Law Committee has considered that the "investigation of crime" as referred to in section 10(3) of the Constitution may include cases where there is a concrete and specific suspicion of an offence but the offence has not yet been actually committed.[44]

The provision in the Constitution concerning the privacy of confidential communications is deliberately device-neutral and technology-neutral. While correspondence and telephony are mentioned specifically, the provision covers all confidential communications of whatever kind.[45]

The principal purpose of the provision of the Constitution concerning the privacy of confidential communications is to protect the content of confidential messages from outside parties. The Constitution guarantees everyone the right to confidential communication without outside parties unlawfully gaining information on the content of confidential messages sent by or to him or her. This means a prohibition against the opening or destruction of letters or other sealed messages and against listening in to or recording phone conversations. The provision protects not only the sender but also the recipient of the message, privacy being a fundamental right of both parties.[46]

The provision does not protect the content of a conversation that is conducted within earshot of one or more other persons and can be heard without assistive means, but listening to a private conversation using technological means constitutes an infringement of the privacy of confidential communications.[47]

The provisions of the Constitution are not intended to define the relationships between the parties to communication or to regulate their behaviour. The issue of when and how a party to a confidential communication may publish the content of a message intended as confidential must be resolved pursuant to other criteria.[48]

Identification data of a confidential message

The Constitution protects not only the content of a message but also the identification data of its sender and recipient as well as any other data that may be of relevance to preserving the confidentiality of the message. In the established practice of the Constitutional Law Committee, the identification data of a message are considered not to be covered by the core area of the fundamental right protecting the privacy of confidential correspondence.[49] However, in a recent statement the Committee considered that in practice the nature of message identification data and the

[44] PeVL 19/2008 vp, pp. 3-4; PeVL 11/2005 vp, p. 3; PeVL 9/2004 vp, p. 3; PeVL 37/2002 vp, p. 3; PeVL 26/2001 vp, p. 3; PeVL 2/1996 vp.
[45] HE 309/1993 vp, p. 53.
[46] HE 309/1993 vp, pp. 53-54; PeVL 28/2000 vp, p. 3; PeVL 30/2001 vp, p. 2; PeVL 54/2001 vp, p. 4; PeVL 13/2003 vp, pp. 4-5; PeVL 9/2004 vp, pp. 3-4; PeVL 10/2004 vp, pp. 4-5; PeVL 16/2004 vp, p. 6; PeVL 59/2006 vp, p. 2; PeVL 19/2008 vp, p. 3.
[47] HE 309/1993 vp, p. 53; PeVL 11/2005 vp, p. 4; PeVL 36/2002 vp, p. 6; PeVL 2/1996 vp; PeVL 5/1999 vp, p. 4.
[48] HE 309/1993 vp, p. 54.
[49] PeVL 6/2012 vp, p. 3–4; PeVL 67/2010 vp, p. 4; PeVL 66/2010 vp, p. 7; PeVL 62/2010 vp, p. 4; PeVL 29/2008 vp, p. 2; PeVL 3/2008 vp, p. 2; PeVL 59/2006 vp, p. 2; PeVL 23/2006 vp, pp. 2-3; PeVL 11/2005 vp, p. 4; PeVL 10/2004 vp, p. 4; PeVL 9/2004 vp, p. 4; PeVL 37/2002 vp, p. 3; PeVL 26/2001 vp, p. 3; PeVL 5/1999 vp, p. 7; PeVL 26/1998 vp, pp. 2-3; PeVL 7/1997 vp; PeVL 47/1996 vp.

potential for compiling and combining them may become so problematic from the perspective of protection of privacy that it is not always justifiable to make a categorical distinction between which matters are covered by the core area and which are peripheral; the significance of the restrictions must be considered more generally.[50]

Any legislation interfering with the privacy of telecommunications identification data must satisfy the general requirements for an infringement of fundamental rights.[51] In the established practice of the Constitutional Law Committee, it is considered permissible not to associate access to identification data with specific offences as far as criminal investigation is concerned if the provisions in place otherwise satisfy the general requirements for an infringement of fundamental rights.[52] However, the infringement must in any case be restricted to matters involving offences of a type that endanger the safety of a private individual, the security of society at large or the sanctity of the home, or offences of a seriousness comparable to these.[53]

6.1.2.5 Measures to implement information security

Section 272 of the Information Society Code may be considered to address a situation technically very similar to telecommunications intelligence. The provision addresses measures to implement information safety, allowing a telecommunications operator, an added value service provider or corporate or association subscriber the right to undertake necessary measures, such as the automatic analysis of message content in all messages transmitted out of or into the network operated by the party in question. Section 272(3) states:

> "If it is evident due to the message type, form, or some other similar reason that the message contains malicious software or commands, and the measure referred to in subsection 2(1) [*automatic analysis of message content*] cannot ensure the attainment of the goals referred to in subsection 1, the content of a single message may be processed manually. - -"

The purposes for which the aforementioned measures may be undertaken are provided for in subsection 1. These purposes would seem to be only partly related to fighting crime, being:

> "1) in order to detect, prevent, investigate and commit to criminal investigation any disruptions in information security of communications networks or related services;
> 2) in order to safeguard the possibilities of the sender or recipient of the message for communications; or
> 3) in order to prevent preparations of means of payment fraud referred to in chapter 37 section 11 of the Criminal Code planned to be implemented on a wide scale via communications services."

These provisions were originally enacted in the Act on the Protection of Privacy in Electronic Communications (section 20) that preceded the Information Society Code in 2004. At that time,

[50] PeVL 18/2014 vp, p. 6.
[51] PeVL 62/2010 vp, pp. 4-5; PeVL 23/2006 vp, p. 3; PeVL 7/1997 vp.
[52] PeVL 29/2008 vp, p. 2; PeVL 11/2005 vp, p. 4; PeVL 9/2004 vp, p. 4; PeVL 26/2001 vp, p. 3; PeVL 37/2002 vp, p. 3; PeVL 7/1997 vp.
[53] PeVL 66/2010 vp, p. 7; PeVL 67/2010 vp, p. 4.

the provision only allowed interference with the content of a confidential message on the basis of suspicion of the specific offences referred to in the provision (endangering information processing or disrupting telecommunications).

According to a statement by the Constitutional Law Committee concerning that provision, its chief purpose was to safeguard the functioning and security of cyber networks in the interests of the various parties of communications, thereby ensuring the exercising of the freedom of speech and the confidentiality of communications in cyber networks. Matters pertaining to the exercising and enjoyment of fundamental rights in this matter were, in the opinion of the Committee, acceptable and weighty grounds for imposing restrictions on communications in cyber networks. Interference with the content of a confidential message was only permissible on the basis of suspicion of the specific offences referred to in the provision. The endangering of telecommunications and information security could be regarded as a risk to the security of the individual and of society at large in a broad sense. The Constitutional Law Committee considered that this legislation was not, in the context at hand, at odds with the confidentiality of correspondence guaranteed in section 10 of the Constitution.[54]

The provision was amended in 2008, following which interfering with the content of a message was no longer associated exclusively to the essential elements of offences. According to the preparatory materials for the provision (HE 48/2008 vp), if interfering with the content of a message was made conditional on the essential elements of offences, analysis could only be undertaken when an act is committed intentionally. In practice, harmful messages are not always sent intentionally. In order to maintain information security, it should also be permissible to analyse unintentionally sent messages that constitute a hazard to information security. It is further noted in the preparatory materials that there is a need to manually process the content of an individual message if it is evident that automatic processing cannot ensure the attainment of the goals referred to in the proposed subsection 1. Section 20 of the Act on the Protection of Privacy in Electronic Communication, which was subsequently superseded by the Information Society Code, was enacted with the input of the Constitutional Law Committee (PeVL 29/2008 vp), and so was the Information Society Code iteself (PeVL 18/2014).

6.1.3 Possible developments in national telecommunications intelligence

International human rights agreements binding upon Finland allow for both domestic and international telecommunications intelligence under certain conditions. It was noted above in the present report concerning the present situation that the most serious threats to Finland's national security are primarily external; consequently, Finland's needs in this sphere involve international telecommunications intelligence.

Telecommunications intelligence would involve intelligence-gathering powers the purpose of which would be to produce intelligence vital for national security on foreign operators and circumstances

[54] PeVL 9/2004 vp, p. 4

as input for decision-making by the senior government leadership. Another purpose would be to detect and identify serious external threats to national security and to gather intelligence on them that would allow the creation of situational awareness, the undertaking of preventive measures and, in the case of the military authorities, the issuing of early warnings. Intelligence work is not person-specific or offence-specific in the same way as crime fighting. The targets of telecommunications intelligence require more general criteria of operation than specific offences defined in the Criminal Code.

It may be regarded as a key requirement for the social acceptability of telecommunications intelligence that the threats concerning which intelligence gathering may be pursued are defined as clearly and concisely as possible. Under international human rights agreements, telecommunications intelligence may not be taken as a means for acquiring any information about any threat or risk. In the comparable countries, legislation usually specifies the threats and situations where intelligence operations are permissible.

The threats identified using telecommunications intelligence must be sufficiently serious and aimed at interests of vital importance for national security. The threats may be military or civilian in nature. Examples of sufficiently serious threats against national security might be a military threat against Finland, terrorism or actions with comparable effects, and espionage. It should be possible to use telecommunications intelligence for detecting and identifying espionage regardless of whether the espionage is aimed at the government or the private sector. It should also be possible to use telecommunications intelligence to chart sources of threats and the methods used by foreign powers for their espionage.

International organised crime might also be a target for telecommunications intelligence insofar as their activities threaten national security. Telecommunications intelligence should also be usable for the acquiring of information required to prevent the distribution of weapons of mass destruction.

International crisis management operations are becoming increasingly demanding, and there is no reason to assume that this trend will end in the future. The security of crisis management operations could be improved with information acquired through telecommunications intelligence.

It should be possible to use telecommunications intelligence for detecting serious threats against critical infrastructure. Such threats may originate in cyber networks.

The plans, intentions and actions of foreign governments may, under certain circumstances, damage or endanger Finland’s foreign and security policy interests. Telecommunications intelligence would ensure the availability of sufficient, reliable and timely information to the senior government leadership.

In certain situations, threats within the country might be of a seriousness and potential impact comparable to the external threats referred to above, and intelligence gathering aimed at interna-

tional telecommunications channels could help acquire information on them. An example of such a serious action might be the massacre in Norway in 2011.

In section 6.1.2 above, we discussed the concept of national security in the context of the European Convention on Human Rights. It is the considered opinion of the working group that threats such as those referred to above fall within the concept of national security as interpreted by the European Court of Human Rights, for instance.

The purpose of intelligence work is to detect, identify and acquire information on threats. Intelligence operations are not intended to prevent these threats from being realised. The line between intelligence work and preventive measures must be separately defined. The competent authorities must be able to act on information provided through intelligence work in order to combat the identified threat. It should be considered in further deliberations to what extent and in what way intelligence could be made available for instance for the prevention of offences.

The international human rights agreements do not seem to impose categorical bans on using telecommunications intelligence for criminal investigation. It must be assumed that telecommunications intelligence cannot be a method usable for the investigation of ordinary cyber crime or indeed any other kind of mass crime. Indeed, we might go so far as to say that basically telecommunications intelligence should not be used for criminal investigation at all. A case for this may be made on the basis of the legal protection of the individual and the secrecy of telecommunications intelligence methods.

The use of telecommunications intelligence for criminal investigation should be distinguished from a case where the intelligence authorities acquire information that indicates that an offence may have been committed. If the offence is a particularly serious one, it should be considered how this information might be passed on to the criminal investigation authorities. Even then, this process could not involve the use of that information in the judicial process, only as a guideline for orienting the criminal investigation.

If serious cyber attacks aimed at the private sector were to be detected in telecommunications intelligence, it should be considered how this information might be passed on to the target enterprise. The aim here would be to minimise the damage to the business sector and to the national economy.

The working group also noted that it would be necessary to analyse telecommunications traffic also for the purpose of ensuring the selectivity of telecommunications intelligence and of monitoring technological developments. This would be necessary for ensuring the functional capacity of the telecommunications intelligence system. Whether it would be possible to organise such activities and to what extent, considering the requirements of international human rights agreements and the Constitution, is a question for further study.

6.1.4 Executing telecommunications intelligence

Telecommunications intelligence should be executed so that traffic relevant to the intelligence assignment could be filtered from the overall volume of traffic as efficiently as possible while preventing irrelevant traffic from being subjected to analysis.

According to the ECHR, the relevant legislation must specify in sufficient detail under what circumstances and according to which criteria citizens may be subjected to secret surveillance by the authorities. Also, the Data Retention judgment of the CoJ requires that the processing of personal data must be delimited in advance. These parameters must be taken into account when considering how to execute telecommunications intelligence.

It must be possible to isolate from the telecommunications traffic flow the information that is relevant for national security. One way of fulfilling this requirement would be to use sufficiently well defined search terms or verbal descriptions of actions threatening national security that define the target of the intelligence-gathering activities as concretely as possible.

The description would need to cover communications models and other models that are known or may be assumed to have to do with activities that threaten national security. One way of organising these operations would be for the permit authority referred to in section 6.1.6 to approve such a description as the basis for a telecommunications intelligence assignment; this may be considered to fulfil the requirement of advance delimitation. On the basis of the description, the authority responsible for telecommunications intelligence would formulate the search terms necessary for directing the intelligence gathering as ordered. The use of the search terms formulated by the authority would have to be comprehensively documented in the interests of *ex post facto* monitoring.

The search terms used in the first phase of telecommunications intelligence could be identification data, such as identifiers of network devices and network addresses, and data on the date, time and location the of communications. It would also have to be possible to examine the content of the traffic screened using the search criteria to gain sufficient information on the threats on which intelligence is being gathered.

When the purpose of telecommunications intelligence is to detect cyber espionage undertaken using malicious software, it should be possible, exceptionally, to use content-related search terms from the outset. The search terms would then include technical identifiers for harmful software, and the operating model would be the same as for operations provided for in section 272 of the Information Society Code.

The infringement of the protection of privacy could be lessened by having the initial screening using the search terms performed automatically. The information relevant for the intelligence operation could be feasibly screened from the overall volume of telecommunications traffic using the search terms, and only after the automatic screening would it be possible to subject the screened content to manual processing. What would be essential for the protection of privacy would be that

no messages or identification data inconsistent with the search terms should end up in manual processing.

Telecommunications intelligence as described above would thus be a process consisting of consecutive stages where at each stage the volume of communications being processed is reduced. Only the information passing through every stage would be eligible for retention. All the other information processed would be destroyed and could then no longer be retrieved by the authorities. The international human rights agreements binding upon Finland require the establishment of unambiguous procedures for information processing.

Telecommunications intelligence would infringe on the confidentiality of correspondence to varying degrees at the various stages of the process. At the initial stage of an operation, all messages in the selected telecommunications channels would be compared to the search terms. The automatic screening would thus also cover the vast majority of telecommunications that is irrelevant for national security. At this stage, the screening could be based on identification data, except in the case of detecting malicious software. The screening would be an automatic process, and messages that do not match to the search terms would never be retrieved for manual processing. The risk of whether any 'false positives' would end up in manual processing depends on how precise the search terms used for the screening are. The more precise the search terms, the lower the risk of irrelevant information being passed on for further processing.

The next stage of the telecommunications intelligence process would involve a deeper infringement of the privacy of communications, but aimed at a substantially smaller number of persons. At this stage, the messages screened on the basis of the search terms defined would be brought to manual analysis. By default, communications brought to manual analysis are relevant to the intelligence assignment, and it must be possible if necessary to discover the content of any particular message.

Organising telecommunications intelligence as described above would not require a broad-based, non-differentiating, long-term or unrestricted retention of identification data; instead, the process would involve a screening of telecommunications traffic based on predetermined search terms and the retention only of information relevant for national security based on that screening.[55] The information being retained would only constitute a minor fraction of the overall volume of cross-border communications.

Organising telecommunications intelligence would require that telecommunications operators or the owners of cross-border telecommunications cables are ordered to notify the competent authorities of their connection points and to disclose to the authorities any information necessary for the carrying out of telecommunications intelligence. These operations must not impair the speed of telecommunications traffic. The connection required should be planned in cooperation with telecommunications operators so as to minimise the inconvenience to them. By default, any direct

[55] The Constitutional Law Committee, in its statement PeVL 18/2014 vp considered that this kind of retention, at least, violates the principle of proportionality.

costs incurred by the operators through the technical work required would be compensated by the clients of the telecommunications intelligence.

6.1.5 Guidelines for the administration of telecommunications intelligence

In section 6.1.3 above, we discussed the threats regarding which it would be necessary to acquire information with telecommunications intelligence in the interests of national security. Various authorities have the duty to monitor these threats, according to current legislation. Acquiring information about military threats is the responsibility of the Defence Forces, while monitoring civilian threats as referred to in the present report is mainly the task of the Finnish Security Intelligence Service. The National Bureau of Investigation combats international organised crime. It is the considered opinion of the working group that there is no reason to change the division of duties between these authorities.

It would not be feasible for the authorities requiring intelligence to undertake telecommunications intelligence each severally; activities should be undertaken centrally. In the centralised scheme, the technical execution of telecommunications intelligence would be entrusted to a single authority (*telecommunications intelligence authority*), which would receive assignments from the authorities entitled to receive telecommunications intelligence (*client authorities*) and gather the intelligence required. Factors in favour of the centralised scheme are the requirements on uniformity and secrecy of operations, the specialisation and technical expertise required, and aspects of monitoring the legality of the operations. The CoJ has required the establishing of unambiguous procedures for such operations and a comprehensive monitoring of legality. These could best be achieved in the centralised scheme.

The technical execution of telecommunications intelligence would have to be an official activity since such operations involve the handling of confidential information the public disclosure of which would seriously compromise national security.

It would be feasible to name as the telecommunications intelligence authority an official body that already has the technical expertise and international intelligence contacts required for the operations. The Cyber Security Centre, which participates in the combating of cyber threats, has the required technical expertise but does not have intelligence duties and therefore also does not have the contacts required for intelligence work. The National Bureau of Investigation has international partners and contacts. It is the authority responsible for investigating offences in its domain, and it is responsible for the technical implementation of coercive measures affecting telecommunications provided for in the Police Act and the Coercive Measures Act for the criminal investigation process. The Finnish Security Intelligence Service engages in international cooperation in intelligence gathering. The Defence Force Intelligence Agency has both the technical expertise and the international intelligence cooperation contacts required.

The authorities that would be giving assignments to the telecommunications intelligence authority would be known as the client authorities. These would be the authorities responsible for combat-

ing the threats that the intelligence operations would concern: the Defence Forces, the Finnish Security Intelligence Service and the National Bureau of Investigation.

If further deliberations lead to a solution where the technical execution of telecommunications intelligence is entrusted to a function within the Defence Forces, its duties in assisting civilian authorities and the powers of the civilian authorities to give assignments to it should be provided for by law.

It is the considered opinion of the working group that Finland's senior government leadership have a need for the information that could be acquired through telecommunications intelligence. Therefore, the senior government leadership should also be able to give assignments to the telecommunications intelligence authority. However, such assignments should be channelled to the party responsible for technical execution through those authorities who are responsible for combating the threats in question.

6.1.6 Points to consider vis-à-vis legal protection

If telecommunications intelligence is organised, they should be organised under the guiding principles of respecting fundamental and human rights, the principle of proportionality, the principle of least intervention and the principle of intended purpose.

Permit procedure

The ECHR considers it important that the authority responsible for acquiring information does not have unlimited discretion in directing its operations. One way of controlling the discretion of the relevant authority is to enact legislation specifying that a permit from an outside party must be obtained for every intelligence operation.

According to the ECHR, the scope of permit discretion should be described in legislation. What is essential here is that the permit application and the permit itself must demonstrate to a sufficient level of detail the groups of persons at which the intelligence operation is targeted. Permit discretion based on the approval of the search terms to be used for screening or on actions compromising national security or a detailed description of the persons concerned may be considered to satisfy the above requirements.

The ECHR has required that the duration of a permit also be provided for by law. In its judgment in the case of *Weber and Saravia v Germany*, the ECHR considered a three-month limit to be within the scope of the principle of proportionality.

As is evident from the international comparison, the party issuing the permit varies from one country to another. A permit may be granted by a court established specifically for that purpose or by a

party with political responsibility. It would be in keeping with Finland's judicial system to have a judicial permit process. The permit process should be set up with a view to secrecy, the requirement for special expertise and the ensuring of legal protection of the individual. In Sweden, for instance, the interests of private individuals in the permit process are safeguarded by a public ombudsman. The possibility of appeal in the permit process should be evaluated, along with the potential for an expedited permit procedure in urgent situations.

Information processing

The ECHR has ruled[56] that the procedures followed in telecommunications intelligence must be provided for in sufficient detail by law. The procedural provisions should cover at least the inspection, use, retention, disclosure and destruction of data.

By 'inspection', we mean the manual processing of data screened automatically on the basis of search terms. Guidelines concerning the situations in which screened data may be retrieved for manual processing were discussed above in section 6.1.4. The use of the data in combating threats and in informing the senior government leadership was discussed in section 6.1.3.

The information produced in telecommunications intelligence would partly consist of personal data. Pursuant to the Constitution, there should be legislative provisions in place concerning the handling of personal data by the client authority and by the telecommunications intelligence authority. Under section 10(1) of the Constitution, more detailed provisions on the protection of personal data are laid down by an Act.

The disclosure of data would basically involve the transfer of information acquired by the telecommunications intelligence authority to the client authority. It should also be considered under what circumstances data could be disclosed to third parties. Such third parties may include companies subject to a serious cyber attack detected through telecommunication intelligence operations. The limitations on the handling of personal data provided for in legislation must also be taken into account in the discretionary process.

There should be provisions on law concerning the circumstances in which intelligence may be disclosed to international partners. Basically, such disclosure should be allowed if it promotes national security and does not compromise Finland's interests, including the interests of the national economy.

Intelligence operations may also produce information not related to the assignment at hand. The ECHR has addressed the issue of the use of such "superfluous information" in various judgments. The conclusion to be drawn from the case-law is that sufficiently comprehensive and precise legislation is required concerning the handling of such information. Even if the relevant judgments concern criminal investigations, they allow for deducing how such handling of data should be organised in intelligence work. It should be possible for the authorities to use superfluous information at the very least in cases where the information concerns a threat against which it would have been permissible to use telecommunications intelligence. The disclosure of information to the criminal in-

[56] *Liberty and others v United Kingdom* and *Weber and Saravia v Germany*.

vestigation authorities for the purpose of directing a criminal investigation is discussed separately in section 6.1.3 of the present report.

The issue of data destruction must be considered separately for information consistent with the assignment, superfluous information with significance for national security and superfluous information irrelevant for national security. For information consistent with the assignment, retention times should be specified along with a determination of how they are specified and how the responsibility for retention is divided between the telecommunications intelligence authority and the client authority. The retention and destruction of superfluous information with significance for national security should be specified in the same way.

Superfluous information irrelevant for national security must be destroyed immediately once it is identified as such.

Telecommunications intelligence would not be intended for monitoring communications between parties within Finland. It would also not be intended for monitoring information stored by a user in Finland in a cloud service abroad if this activity does not involve communication, except for traffic generated by malicious software. In further deliberations, sufficient provisions should be put into place to ensure that such information is destroyed immediately once it is identified.

Effective remedies

In further deliberations, it should be considered what effective remedies should be adjoined to telecommunications intelligence. Such remedies might include a complaint, an indirect right of inspection where a person may request an inspection of the legality of the handling of his or her personal data, and the participation of a public ombudsman in the processing of a permit application. It should also be considered whether a permit decision could be appealed and how this appeal process should be established.

Oversight

Pursuant to the case-law of the ECHR, the oversight of secret surveillance powers of the authorities must be effectively provided for. Oversight may not be left to internal control by the authorities themselves. Even legality monitoring by an independent outside body cannot of itself be considered a sufficient guarantee of legal protection if that body cannot make legally binding decisions subject to appeal. The ECHR has recognised both oversight by an external court and parliamentary oversight.

Under the Constitution, the Chancellor of Justice and the Parliamentary Ombudsman have a universal right to receive the information needed for their supervision of legality. The Data Protection Ombudsman supervises the legality of the handling of personal data. The supervision of telecommunications intelligence may require such a degree of specialisation that setting up a dedicated supervisory body may have to be considered. Internal legality supervision of the telecommunications intelligence authority and the client authorities and the supervision by the controlling ministries should also be provided for.

Telecommunications intelligence would also require parliamentary oversight. The ECHR has noted that the participation of parliament in the supervision of secret surveillance powers is essential for the protection of democracy.

6.1.7 Telecommunications intelligence impact assessment

Weighing the advantages and disadvantages of telecommunications intelligence

In deliberating the acceptability of telecommunications intelligence, it should be considered whether the benefit to national security from the operations would be greater than the disadvantages caused to protection of privacy, the national economy and enterprises.

The threats to be identified through telecommunications intelligence is international, serious and aimed at Finland's key security interests. Telecommunications intelligence would produce intelligence vital for national security on foreign operators and circumstances as input for decision-making by the senior government leadership.

The international comparison contained in the present report and public sources[57] indicate that telecommunications intelligence is in use in several Western countries. It is obvious that the governments in those countries consider it an effective means for gathering intelligence. Foreign experts consulted by the working group in confidence also stressed that telecommunications intelligence is a means for acquiring information vital for combating threats against national security and for acquiring strategic information as input for decision-making by the senior government leadership. It was noted in the hearings that modern foreign and security policy decision-making can only be based on up-to-date intelligence, to which telecommunications intelligence make an essential contribution.

Telecommunications intelligence would also significantly complement Finland's actions against serious cyber threats. Current systems cannot detect governmental espionage software and other malicious software with a particularly high potential for compromising national security. Telecommunications intelligence would also help the business sector protect against serious cyber threats.

On the other hand, it is clear that this system would infringe upon the protection of confidential correspondence, which is a fundamental right. Section 6.1.4 of the present report addresses the issue of how telecommunications intelligence should be arranged so that its infringement of the protection of privacy would be as low as possible and acceptable from the perspective of international human rights agreements. Nevertheless, implementing telecommunications intelligence would seem to be problematic vis-à-vis the constitutional protection of confidential correspondence.

[57] See e.g. a study of the European Parliament entitled *National programmes for mass surveillance of personal data in EU member states and their compatibility with EU law* (http://www.europarl.europa.eu/studies).

Telecommunications intelligence would be functionally equivalent to the powers already exercised by information society operators for ensuring information security. Both involve the use of search terms for the automatic filtering of communications. A message can be retrieved for manual processing if an obvious match is found between the search term(s) used and the content of the message. An independent permit process and oversight procedure should be provided for telecommunications intelligence.

The hearings held have revealed that for technical reasons it is not always possible to distinguish between domestic and international telecommunications. Therefore any infringement of the protection of confidential correspondence could in theory also affect domestic telecommunications. In such situations, the protection of confidential correspondence could be upheld by imposing a prohibition on processing domestic telecommunications and requiring that the information acquired on same be immediately deleted.

It should be noted from the perspective of the protection of confidential correspondence that views on identification data and their specificity may be changing. In sections 6.1.2.3 and 6.1.2.4, we discussed the Data Retention judgment of the Court of Justice of the European Union and the comments of the Constitutional Law Committee. The extensive, non-differentiating, long-term and unrestricted retention of identification data in telecommunications intelligence must be prevented. It should be possible to retain such information concerning cross-border communications which matches the search terms used and which therefore can be estimated to be of significance in combating threats against national security. The information being retained would only constitute a minor fraction of the overall volume of cross-border communications.

The impacts of telecommunications intelligence on citizens, enterprises and on the economy as a whole must be assessed.

It was brought up in the hearings that telecommunications intelligence may have a negative impact on Finland's international competitiveness and on how attractive Finland is for foreign investors. Finland's attractiveness in this respect was considered in these statements to be based on clean information networks and Finland's reputation as a country with a high level of information security.

The notion of 'clean information networks' is questioned by a report from the Cyber Security Centre,[58] according to which the Western countries that systematically monitor cyber attacks detect dozens of cases of cyber espionage facilitated technically by a targeted malicious software program every year. According to that report, Finland is not exempt from this threat. Unlike the aforementioned countries, Finland does not currently have a system for monitoring especially serious targeted malicious software attacks. We may therefore conclude that our conception of Finland as having particularly clean information networks is due to shortcomings in detection ability at the national level; at least as far as the most serious cyber threats are concerned. It may be as-

[58] *Kohdistettujen haittaohjelmahyökkäyksien uhka on otettava vakavasti. Viestintäviraston Kyberturvallisuuskeskuksen raportti* [The threat of targeted attacks using malicious software must be taken seriously. Report of the Cyber Security Centre of FICORA]. Autumn 2014.

sumed that developing Finland's telecommunications intelligence capability would raise the threshold of cyber espionage being targeted at our country.

The claim that telecommunications intelligence would erode Finland's high level of information security should be assessed against the outline given for these operations above. Telecommunications intelligence would target communications across Finland's borders. The majority of the countries to which Finland's current and planned telecommunications connections go already have the capability under their respective legislations to monitor communications passing through their territory. Therefore, the communications carried over international network connections to and from Finland may already be subject to monitoring and intelligence operations by foreign authorities.

The working group aimed to explore the potential negative impact of telecommunications intelligence legislation on investments. It is difficult to assess the potential impact on Finland. The working group knows of no studies on this subject. We may point to Sweden as an example of a country that in recent years has enacted detailed and public legislation on telecommunications intelligence.

In order to investigate the possible investment impact of Sweden's new signals intelligence act (known as the 'FRA Act'), the Swedish Ministry of Defence commissioned a study from Gearshift Group Oy. This study focused on ICT investments in Sweden and Finland between 2008 and 2013. The study made use of reports by market research institutions and expert evaluations found through media reports in addition to the principal research sources. The complete study is appended to the present report as Appendix 1. A brief summary of the findings follows:

> *Impact on investments and the necessary preconditions for investments.* The study did not identify any deviations in foreign investments that could have been explained by the impact of the FRA Act. According to the study, the entry into force of the FRA Act did not have any clear impact on foreign investments in Sweden as compared to Finland and Denmark.
>
> *Impact on research and development.* While R&D expenditure relative to the GDP declined slightly in Sweden in 2009 and onwards, it is hard to see the fall in the level of R&D expenditure as a consequence of the FRA Act as it coincided with the onset of the global recession. The figures showing the sources of funding in Sweden indicate that foreign actors even increased their share of investments relative to the funding available within Sweden as well as relative to the investments made by the private and public sector. This strongly suggests that the FRA Act has not played any role in the allocation of foreign R&D investments.
>
> *Impact on international competitiveness.* In a comparison made by the World Economic Forum, Sweden ranks among the top ten countries both in terms of international competitiveness and innovation. Specifically in terms of ICT investments, an assessment of the competitiveness of the various countries can be made by evaluating the general preconditions for the establishment and operation of data centres. In the 2103 *Data Center Risk Index* comparison, Sweden was ranked the third best host country for data centres while Finland was placed ninth. The FRA Act is not deemed to have had any negative impact as far as the establishment of data centres is concerned. Sweden's competitiveness has translated into major new data centre projects such as Facebook in 2011 and capacity expansion in 2014; KnC Minter in 2014;

Hydro66 in 2014; and Bahnhof's major expansion project in Stockholm. According to the study, Sweden's clear intelligence legislation may, in fact, provide a competitive edge in the aftermath of the Snowden case. With large long-term investments, risk minimisation and the predictability of the operating environment are important considerations affecting the competitiveness of the individual countries.

Impact on the creation of new businesses. A comparative analysis of the rate at which new businesses have been founded in Sweden, Finland and Denmark during 2005–2008 shows Sweden taking the pole position by a wide margin. According to the report, the significance of the FRA Act in terms of the business environment is very low. It is not deemed to have impacted entrepreneurial activities or the creation of new businesses.

It is noted in the summary of the study that the entry of the FRA Act into force does not correlate clearly with trends in foreign investments in the ICT sector. No impact on similar investments in Finland that would be explained by the FRA Act was found. The study concluded that specific legislation, such as the FRA Act, creates a more predictable operating environment for all operators in the ICT sector.

The information received by the present working group at its hearings concurs with the findings of the aforementioned study. They indicate that the FRA Act did not have a negative impact on Sweden's competitiveness, nor did it reduce the volume of foreign investments in the country.

As a further note specifically concerning data centre investments, according to a study published by the Gartner research company in September 2014, Sweden and Norway are seen as attractive locations for data centres.[59] The intelligence legislation of Sweden and Norway was not brought up at all in the study.

Specific legislation creates predictability, which is important for operations planning and investment decisions for enterprises. In fact, specific legislation in this area could turn out to be an international competitive advantage for Finland.

The Finnish business sector has been worried about the potential eroding of the competitiveness of Finnish enterprises on international markets by requiring them to disclose encryption keys or to install backdoors in their software or equipment for the purposes of telecommunications intelligence. The working group proposes no such requirements for businesses.

Organising telecommunications intelligence would require that telecommunications operators or the owners of cross-border telecommunications cables are ordered to notify the competent authorities of their connection points.

At the interest group hearings held by the working group, it was pointed out that IT advancements might reduce the effectiveness of telecommunications intelligence in the future. Telecommunica-

[59] Gartner's report *Save up to 50% on European Colocation by Choosing the Right Location*, published 16 September 2014.

tions encryption and the increased volume of communications were considered to be the major factors in this development.

It was also brought up at the hearings that because of developments in encryption techniques, in the future it will not be possible to decrypt messages without encryption keys. This will have a decisive impact on whether telecommunications intelligence can yield the required real-time information. However, telecommunications intelligence may yield information useful for national security despite encryption, for instance in the form of identification data. They would also be used for detecting cyber attacks, in which encryption would be irrelevant. According to technical experts consulted by the working group, sufficient efficiency for the system could be ensured without demanding that enterprises should disclose their encryption keys or install backdoors.

The effectiveness of telecommunications intelligence was also called into question at the hearings on the basis that communications volumes will continue to increase. However, such growth cannot be considered to reduce the need for telecommunications intelligence, quite the opposite. The shifting of threats to information networks is discussed in chapter 2 of the present report. Sufficient resourcing for operations must be provided in order to respond to increasing traffic volumes, and the intelligence process must be selective enough to be effective.

A summary of the statements received from interest groups and experts is appended to the present report as Appendix 2.

Financial impacts and personnel impacts

Financial impacts will depend on whether a centralised or decentralised model is selected for implementing telecommunications intelligence. If the centralised solution proposed in the present report were selected and a unit of the Defence Forces were designated as the technical executor, the resource impacts would mainly concern the Defence Forces. Cost-sharing principles among the parties participating in these operations should be agreed upon in more detail in further deliberations.

The parliamentary assessment group exploring the long-term challenges of defence noted in its report (Office of Parliament 3/2014) that the current funding framework does not allow for sufficient resources for developing cybersecurity, whether in the defence administration or anywhere else in the public sector.

Implementing telecommunications intelligence would require further resources whose volume depends on how and on what scale the operations were organised. The resources would mostly be needed for system investments and human resources.

The client authorities would also incur costs, for instance for analysis and translation services.

The permit authorities and oversight authorities would also incur costs, but at this point they are difficult to estimate.

6.2 Foreign human intelligence and foreign information systems intelligence

6.2.1 General

As the most serious threats to Finland's national security are almost without exception of international origin or at least have contacts abroad, not all information pertaining to the security of Finnish society is available within Finland. In order to safeguard the security of Finnish society successfully, the Finnish security authorities must be able to acquire information from foreign operators.

Foreign intelligence as a blanket term refers to the acquiring of information relevant for national security on circumstances and targets in foreign countries. The purpose of foreign intelligence is to produce information that is vital for the decision-making of the senior government leadership and for the combating of serious external threats to national security.

Because of the nature of foreign intelligence work, it is a universal principle to aim to acquire the necessary information by the easiest possible means. In practice, much of intelligence work is based on operating models closely resembling liaison operations: voluntary exchange of information and views between the authorities of two countries for mutual benefit. Such exchange of information may concern phenomena of interest to both parties, individual events, observations or political moods on which one party may offer an interpretation to influence the other party's views. In addition to mutual information exchange, foreign intelligence work may be based on the unilateral efforts of the intelligence-gathering government. At its most basic, this involves personnel stationed abroad by the intelligence-gathering government making general observations about circumstances in the country where they are stationed and engaging in dialogue with representatives of that country's government or local citizens. Such activities are generally tacitly approved by the government of the country in question even though they are not equivalent to mutually agreed exchange of information. It is an accepted fact that all governments must tolerate a certain amount of intelligence activity in their territory.

In certain exceptional situations, intelligence gathering based on cooperation or tacit approval is not sufficient. In such cases, it should be possible to acquire information of critical importance for Finland's national security by using secret methods of intelligence gathering. Foreign intelligence work using secret methods may be divided into foreign human intelligence and foreign information systems intelligence.

Foreign human intelligence is intelligence work based on personal interaction or the personal observation of another person or other target abroad. Foreign human intelligence can be conducted over telecommunications connections by a party based in Finland.

Human intelligence is capable of acquiring detailed, deep-level information with high confidentiality classifications that is difficult or impossible to acquire with other intelligence methods. Human intelligence can also lay the groundwork for the efficient use of other kinds of intelligence.

Foreign information systems intelligence is acquiring information processed in an information system abroad with IT means. The key difference between foreign information systems intelligence and telecommunications intelligence is the geographical scope of the operations. Foreign information systems intelligence operations are generally based in Finland but are carried out in the target country of the intelligence-gathering and in some cases a third country, while telecommunications intelligence is carried out in Finland.

Many European countries have enacted legislation governing their foreign intelligence operations and the powers available. There are national differences in the precision with which individual powers are provided for in legislation. Generally worded provisions are in place for instance in Sweden. Legislation on intelligence powers in Sweden are limited to a provision stating that intelligence operations are undertaken by acquiring, processing and analysing information and that technical intelligence-gathering and human intelligence-gathering are used for this purpose. An example of more detailed provisions may be found in the Netherlands, where the relevant legislation contains detailed provisions on each of the powers available to the intelligence services.

Internationally, intelligence methods are undergoing rapid development, particularly in information systems intelligence. Intelligence services use information systems intelligence methods for acquiring a wide range of information concerning for instance operators, systems, cyber network structures and vulnerabilities in the target country. The purpose of foreign information systems intelligence may be not only to acquire information but also to disrupt the operations of the target systems or to damage them by altering or deleting data. Such operations may be interpreted by the government of the target country as the use of force or a violation of sovereignty tantamount to an armed attack.[60] Whether disrupting or damaging an information system may be interpreted as the use of force depends on both the target and the seriousness of damage caused. Causing a temporary inconvenience (as with denial-of-service attacks) does not constitute use of force; however, if the target is a significant one and if the operation is long-lasting and of a high intensity, it may be seen as use of force if not tantamount to an armed attack.

The foreign information systems intelligence proposed in the present report would not be on the level of cyber attacks and thus equivalent to the use of force; it would involve acquiring information as part of other intelligence-gathering. The basic purpose of information systems intelligence would be to collect information on information systems as covertly as possible, not to disrupt the target system or to alter or delete data contained therein. Although case-law and legal opinions concerning cyber operations are still only emerging and a threshold for what constitutes an attack in a cyber environment has not been defined in international law, it would seem that in-

[60] *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press 2013. This is a non-binding document written as a personal view by experts on international law concerning the application of international law to cyber warfare. Despite its informal nature, the Tallinn Manual is used widely as a reference.

formation systems intelligence equivalent to intelligence-gathering could not be considered a use of force violating international law, and certainly not an attack.[61] This view is supported by the fact that apparently so far, no government has undertaken military defence measures against a government targeting information systems intelligence against it. Also, action against cyber systems has so far not been undisputedly and publicly declared as equivalent to an armed attack in the international community.[62]

6.2.2 Development needs

In order to safeguard Finland's key security interests, it is necessary to enact a legislative foundation for intelligence-gathering abroad performed by the civilian and military authorities responsible for national security. The purpose of these operations should be to support foreign and security policy decision-making by the senior government leadership and to combat serious external threats against Finland's national security. In particular, such threats include: military threats against Finland; threats against international crisis management operations in which Finland is participating; international terrorism aimed at Finland; foreign intelligence operations targeted at Finland; international organised crime threatening national security; the development, dissemination and export of weapons of mass destruction, defence materiel and dual-use items that threatens national security; other serious threats, above all cyber threats, against vital functions of society; and plans, intentions and actions of foreign powers that may have a damaging or detrimental impact on or significance for Finland's foreign and security policy.

Legislation is needed to provide for both foreign human intelligence and foreign information systems intelligence.

The international comparison shows that it should be considered in further deliberations whether it should be possible to use human intelligence sources in foreign human intelligence and to acquire information by making systematic observations of persons, locations and other targets. It should also be considered whether it should be possible to protect intelligence-gathering so as to keep it secret to ensure the safety of the person acquiring the information or the person disclosing the information, to gain the trust necessary for acquiring the information, or to prevent the discovery of the intelligence-gathering.

Foreign human intelligence may be based on personal interaction between the official gathering intelligence and an outside person. It should be considered whether it should be allowed not only to ask human intelligence sources to disclose information in his or her possession, but also to instruct them to acquire information. It should be possible to keep the identity and organisation of the official gathering intelligence secret if necessary.

In addition to human intelligence being carried out abroad, it should be possible to carry it out over telecommunications connections while based in Finland. It should also be possible to carry out human intelligence as part of a crisis management operation.

[61] *Tallinn Manual*, pp. 50 and 52.
[62] *Tallinn Manual*, p. 57.

Foreign information systems intelligence means active measures undertaken by the security authorities to gather intelligence through cyber networks on individuals or government actors located abroad who might threaten Finland's national security or other vital interests of Finnish society. Information systems intelligence would enable preparations for and responses to threats against the protective structures and functions of Finland's critical information systems. Ultimately, information acquired through foreign information systems intelligence would enable the deployment of cyber warfare capabilities against enemy targets as part of military use of force in a crisis situation.

Information systems intelligence requires bypassing technical protections and operating in cyber networks beyond the borders of Finland.

National legislation should be enacted to legalise foreign intelligence operations. The eventual preparation of such legislation should also take into account needs for change for instance in criminal legislation and legislation governing the powers of government officials. International human rights agreements and other international obligations binding upon Finland should also be taken into account.

6.2.3 Point of view of the target country

It is a universal principle in international law that every sovereign state is guaranteed territorial integrity and political independence in respect to other countries. Each country may decide for itself whether and on what terms it allows foreign officials to operate in its territory. As noted above, most governments, up to a point, tolerate or even accept the activities of foreign intelligence officials in their territory. This may involve information exchange benefiting both parties, or it may simply be that the gathering of intelligence concerning general circumstances in the target country undertaken openly by a foreign power does not compromise the interests of the target country or any other party. Under other circumstances, a target country may take a negative view of activities by foreign officials in their territory. Such activities may, in some cases, be punishable under the criminal legislation of that country. Depending on the target country, whether an action is punishable may depend on who is acquiring the information, what the information being acquired is and what methods are used to acquire it.

The comparable countries have not enacted legislative provisions setting as a condition for foreign intelligence operations that the target country must accept the operations or that the operations do not violate the legislation of the target country. It would be natural for Finland to take a similar approach in considering the legislation governing intelligence operations. Foreign intelligence might be defined as actions necessary to achieve an acceptable goal (ensuring national security) that may in some situations involve risks. One of the potential risks is that the operations undertaken violate the legislation of the target country or would otherwise be unacceptable to its government. The attitudes of other governments and the contents of their legislation should be taken into account in foreign intelligence operations; for practical reasons, however, this could only be investigated when embarking on the actual operations and not when enacting legislation

concerning them. The deliberation here would involve considering whether the benefit to national security from any particular operation clearly outweighs the related risks.

6.2.4 Point of view of a third country

It is a universal principle in international law that every sovereign state is guaranteed territorial integrity and political independence in respect to other countries. This also applies when intelligence operations are undertaken by using the territory of a third country in some way.

It is also a universal principle in international law that a country may not allow its territory to be used for taking an action that has a damaging and illegal impact on other countries. In assessing such an action, it is not crucial whether the action actually causes damage to property or persons; what is crucial is whether the action may cause negative impacts of any kind.

Foreign human intelligence might involve meeting human intelligence sources in the territory of a third country or recruiting such sources in a third country.

The concept of a transit country cannot be directly applied to international telecommunications, because traffic is generally routed through the path of least resistance in unpredictable ways at any given time.

It may prove necessary to engage in intelligence-gathering in the territory of a third country, through a third country or in an information system physically located in a country other than the persons possessing the information sought through the intelligence-gathering. This scenario applies equally to human intelligence and information systems intelligence, although they may be seen to differ in their impact on the sovereignty of a third country. For instance, a group planning a terrorist attack in a Western country may communicate using a message service subscribed to in a third country that has no other connection to the members of the group except that the relevant server is located there. Although intelligence-gathering concerning such a service would technically take place in an information network in a third country, the impact of the operation would concern the country in which the persons engaged in the activity are located. The sovereignty impact would thus primarily concern the country where the persons engaged in the activity are located. Also, establishing in which country a particular server is located may also require operating in or through a third country.

Violating the sovereignty of a third country is also a consideration in a situation where a server in a third country is used to deceive a target in the target country, for instance by insinuating an intelligence program into a target information system. What is relevant in such a case is whether the authorities in the third country condone such actions.

6.2.5 Intelligence operations and international law

Under Article 38 of the Statute of the International Court of Justice, the key sources for international law are: international conventions, whether general or particular, establishing rules ex-

pressly recognized by the contesting states; international custom, as evidence of a general practice accepted as law; the general principles of law recognized by civilized nations.

There are no international agreements concerning intelligence work during peacetime. The protection extended to spies in wartime under Article 46 of the Protocol Additional to the Geneva Conventions of 1949 is not relevant for the matter at hand.

Although intelligence operations basically always involve violating the sovereignty of the target country, there is no agreement in jurisprudence as to whether international law accepts or condemns intelligence operations on the level of custom and general principles of law.[63] It may be assumed that intelligence operations are not universally acceptable under international law, because governments frequently indicate that they do not approve of such operations by declaring persons *persona non grata* or by other means. On the other hand, it cannot be assumed that intelligence operations should be considered prohibited under international law because nearly all governments engage in such operations. Intelligence operations are well established worldwide, and the attitude of any given country to such activities is determined according to whether it is an intelligence-gathering country or a target country, as the case may be.

Although there is no international regulation concerning intelligence work, there are numerous international cases demonstrating that the potential of the international agreement system has been leveraged in this context, specifically the guarantee of integrity and immunity from prosecution in criminal matters afforded to diplomatic representatives under the Vienna Convention (SopS 3–5/1970).

6.2.6 Decision-making concerning foreign intelligence operations

The international comparison shows that decision-making concerning intelligence-gathering varies by country. Decisions may be made by the intelligence authorities themselves or by a body with political responsibility. Decisions made by the intelligence authorities themselves must comply with the policies of the government leadership.

Because foreign intelligence operations involve matters sensitive for foreign policy, in Finland such decision-making should be governed by the foreign and security policy leadership. Important matters of foreign and security policy and matters otherwise concerning Finland's relationship with foreign countries are prepared at joint meetings of the Cabinet Committee on Foreign and Security Policy and the President of the Republic; these include important matters of internal security and important matters of national defence. Intelligence methods also affect the sovereignty of a foreign country in the target country itself when such operations are undertaken in cooperation with or through the territory of a third country. This heightens the political dimension of foreign intelligence operations. The potential impacts and risks of such operations would have an effect on the decision-making process. It would be important in further deliberations to ensure the

[63] See reviews on international legal literature for instance in: Baker Christopher D.: 'Tolerance of International Espionage: A Functional Approach'. *American University International Law Review*, vol. 19 (2003) issue 5; Radsan Afsheen John: 'The Unresolved Equation of Espionage and International Law'. *Michigan Journal of International Law*, vol. 28 (2007) issue 597.

functioning of the decision-making process for foreign intelligence and the prompt conveying of related information in urgent situations.

6.2.7 Oversight

In addition to providing for foreign intelligence operations by law and subjecting it to official liability, the operations should be provided with both legal and parliamentary oversight.

Legal oversight would concentrate on ensuring that foreign intelligence operations comply with Finnish law. Outside legal oversight would fall within the domain at least of the Chancellor of Justice, the Parliamentary Ombudsman and the Data Protection Ombudsman. A dedicated external oversight body might also be considered. Internal legality supervision of the organisations involved and supervision by the controlling ministries should also be provided for.

Because of its nature, foreign intelligence should be subject to parliamentary oversight. The international comparison shows that in some countries parliamentary oversight is conducted by a committee of parliament, whereas in other countries there is a body external to the parliament that has representatives from both the parliament and the judiciary.

6.2.8 Financial and personnel impacts

The extent of financial impacts depends on the scope and orientation of the operations. Initially, the work would be undertaken within the spending limits of the relevant authorities. The operations would then be gradually developed.

7. CONCLUSIONS

The purpose of both telecommunications intelligence and foreign intelligence would be to gather intelligence vital for national security concerning serious international threats. These operations would support decision-making by the senior government leadership and ensure that it is based on correct, reliable and timely information. The operations would also enable the competent authorities to take action to combat threats. Intelligence operations should be provided for by law

and provided with both legal and parliamentary oversight. It would be feasible to organise the oversight of the various methods of intelligence gathering as uniformly as possible.

7.1 Telecommunications intelligence

The Finnish government should consider introducing powers for intelligence work aimed at cross-border telecommunications so that the changes in the external security environment described in the present report could be addressed.

Telecommunications intelligence would be limited to acquiring information on threats against national security. These threats may be military or civilian in nature and may be implemented in the real world or through cyber networks.

Uniformity of procedures and legality oversight would favour the concentrating of the technical execution of telecommunications intelligence in the hands of a single authority. Financial reasons also favour centralisation. The Defence Force Intelligence Agency already has the technical capability and the international partnerships required. The client authorities could be the authorities responsible for combating threats and thereby the parties responsible for foreign, security and defence policy decision-making in Finland. In such an arrangement, the duties of the relevant unit in the Defence Forces in assisting civilian authorities and the powers of the civilian authorities to give assignments to it should be provided for by law.

It is the considered opinion of the working group that corporate bodies should not be required to disclose their encryption keys or to install backdoors in their software or equipment. Organising telecommunications intelligence would require that telecommunications operators or the owners of cross-border telecommunications cables are ordered to notify the competent authorities of their connection points and to disclose to the authorities any information necessary for the execution of telecommunications intelligence.

Fundamental and human rights must be appropriately taken into account in considering the preparation of legislation concerning telecommunications intelligence. In particular, the protection of confidential correspondence guaranteed to everyone in the Constitution must be taken into account, and also the fact that under the Constitution provisions concerning limitations of the secrecy of communications which are necessary in the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, as well as during the deprivation of liberty may be laid down by an Act. It would thus seem that it would not be possible to enact legislation on telecommunications intelligence for intelligence-gathering purposes without amending the Constitution, with the possible exception of intelligence operations aimed solely at telecommunications in a foreign country. Further deliberations might include considering whether it would be possible to implement effective telecommunications intelligence initially in a limited capacity, for instance by focusing only on identification data.

The permit procedure and implementation of telecommunications intelligence would have to be described with sufficient precision. Telecommunications intelligence must be subjected to clear guidance and comprehensive legal and parliamentary oversight.

In considering the impacts of telecommunications intelligence, its impacts on the digitalisation of society and the operating potential of businesses should be considered. Eventual preparation should consider not only the security policy angle but also factors affecting the development of economic policy and the digital ecosystem. Leveraging the potential offered by ICT for changing operating procedures and improving productivity is vital for achieving economic growth. Further deliberation should include a comprehensive survey of the technical means of conducting telecommunications intelligence and their financial impacts.

7.2 Foreign human intelligence and foreign information systems intelligence

Authorising the military and civilian authorities responsible for national security to gather intelligence supporting decision-making by the senior government leadership and concerning external security threats should be considered. This would involve acquiring the necessary information from human sources and information systems abroad.

International obligations binding upon Finland and the legislation of the country in which the information is to be acquired should be taken into account in considering the exercising of intelligence-gathering powers and in evaluating the risks involved.

Because of the nature of the operations, decision-making concerning foreign intelligence should take into account the guidelines of the senior government leadership in particular. Foreign intelligence is a sensitive area in terms of foreign policy. The steering and responsibility relationships should be carefully considered in any eventual further preparation. Foreign intelligence should be provided with both legal and parliamentary oversight.

7.3 Proposals for further action

In the interests of creating a legislative framework for intelligence work, the working group proposes that one or more legislative initiatives be launched on the grounds described above. This preparation could proceed stagewise if necessary, but the limitations deriving from the Constitution as it now stands to legislation concerning telecommunications intelligence must be taken into account. Parliamentary or other political preparation should also be considered.

Because the needs of the administrative branch of the Ministry of the Interior have to do with detecting serious civilian threats against national security, such as terrorism and espionage, and identifying the parties behind them, it might be considered that legislative preparation concerning civilian intelligence work be led by the Ministry of the Interior.

The needs of the administrative branch of the Ministry of Defence have to do with creating and maintaining the situational awareness related to the duties of the Defence Forces, with issuing early warnings and with targeting support; therefore, it might be considered that legislative preparation concerning military intelligence work be led by the Ministry of Defence.

Because both administrative branches need telecommunications intelligence, a separate Act on telecommunications intelligence should be considered. The needs of interest groups should be taken into account in the preparation, including representation from the business sector.

Any amendments that need to be enacted to the Constitution should be prepared under the leadership of the Ministry of Justice.

If intelligence legislation is prepared separately in the administrative branches, these efforts should be coordinated.

Appendices

gearshiftgroup

Foreign investments in the IT sector in Sweden and Finland during 2008–2013 and the potential impact of the Swedish 'FRA Act' on investments

Table of contents

1 Object of study

1.1 Background and objectives

The Finnish Ministry of Defence appointed a working group with a mission to develop Finland's legislation specifically with regard to the regulation of intelligence gathering by the security authorities. The objective was to improve the capabilities for ensuring national security, particularly in view of the threats posed by cyber networks.

The present study will assess this issue in terms of the foreign investments made in the IT sector in Sweden and Finland during 2008–2013. As a result of these efforts, a summary was prepared of the developments accompanied by an assessment of the potential impact of the 'FRA Act' on actual investments in Sweden.

Provisions regarding signals intelligence are set out in a number of laws and decrees: (Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet; Lag (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet; and Förordning (2008:923) om signalspaning i försvarsunderrättelseverksamhet). Signals intelligence operations are carried out by the National Defence Radio Establishment (FRA), a civilian organisation operating under the auspices of the Ministry of Defence. The FRA is tasked to gather intelligence in response to the assignments given and to make the information acquired available to the parties issuing such assignments.

1.2 Issues addressed in the report

The present report focuses on the foreign investments made in the IT sector in Sweden and Finland during 2008–2013, and provides an assessment of the potential impact of the Swedish 'FRA Act' on these investments from the following perspectives:

- impact on investments and the necessary preconditions for investments;
- impact on R&D activities in Sweden;
- impact on Sweden's international competitiveness;
- impact on the creation of new businesses in Sweden and Finland; and
- implications for various companies or groups of companies in Sweden.

1.3 Methodology

The approach used in the study is based on a desk study concerning the economic impact of 'Internet Surveillance' legislation. Aside from the effects of legislation, efforts were made to identify studies on the potential impact of such surveillance on investments. In addition to the actual research sources, use was made of reports issued by market research institutions and expert assessments underlying various media reports. The desk study identified the areas impacted by the legislation as well as the nature and extent of such an impact. Using the bibliography, the statistical sector and other analyses, an attempt is made to assess the extent of said impact in Sweden and compare this impact with the actual developments in Finland during 2008–2013.

2 Media reporting in Sweden and Finland before the adoption of the FRA Act

2.1 Google Sweden

”Google likens Sweden to dictatorship”, Published: 30 May 2007 11:49 GMT+02:00.

”Search engine giant Google has slammed Sweden's proposed wiretapping legislation as illiberal and incompatible with Western democracy. Speaking on a visit to Sweden on Tuesday, the company's global privacy counsel, Peter Fleischer, warned that Google would rule out making any major investments in Sweden should the controversial bill become law.

"We have contacted Swedish authorities to give our view of the proposal and we have made it clear that we will never place any servers inside Sweden's borders if the proposal goes through," Fleischer told Internet World.”

2.2 Afltonbladet daily, Sweden

19 June 2008, IT companies shun Sweden following adoption of the FRA Act: “Several major companies will not invest in Sweden.”

Sweden will miss out on major investments by multinational IT companies. “As a result of the FRA Act, companies will be reluctant to establish business in Sweden,” says Invest in Sweden Agency. “We’ve received clear indications from several major corporations that they will not invest in this country,” says Sales Manager Bengt-Åke Ljudén of Invest in Sweden Agency (ISA), a government agency that assists foreign companies to establish in Sweden. “Otherwise, Sweden is ideal for internet operators who need access to energy and cooling for their servers,” says Ljudén. “We receive a large number of inquiries from companies keen to build large data centres.”

Recently, Intel, a major IT corporation, invested a great deal of money in expanding the fourth-generation mobile telecommunications in Sweden. Unlike Invest in Sweden Agency, Carl-Daniel Norenberg, Business Development Manager at Intel, does not expect the FRA Act to have any impact on the willingness to invest in Sweden. “It won’t affect our operations in any way. We’re forging ahead normally,” he said to news agency TT.

2.3 Debate in Finland

Technology industry deeply concerned about the proposed ‘mass surveillance act’.
10 March 2014 13:00, It-viikko magazine.

“Finnish government officials are having pipe-dreams about massive data cable projects and Finland’s rise to the position of an ‘IT centre’ or ‘the Switzerland of Data’ in Europe. At the same time, the Government is preparing a bill for intelligence gathering dubbed as a ‘mass surveillance act’ by the critics. The Federation of Finnish Technology Industries fears that the foreseen law designed to improve the police’s capabilities in the cyber environment will ruin Finland’s reputation as a neutral country with a high standard of data security and kill the budding data business in its infancy.”

3 Perspectives

3.1 Impact on investments and the necessary preconditions for investments

Figure 1, depicting the overall trend in investment activities in Sweden, does not show any such deviation in investments since the entry into force of the FRA Act in 2009 that could be explained by the effects of the law. By contrast, the levelling off of the growth in investments that took place in 2009 is explained by the global banking crisis and subsequent overall decline in investments. While the figure does not provide specific data on investments in the IT sector, they tend to follow the overall trend according to experts.

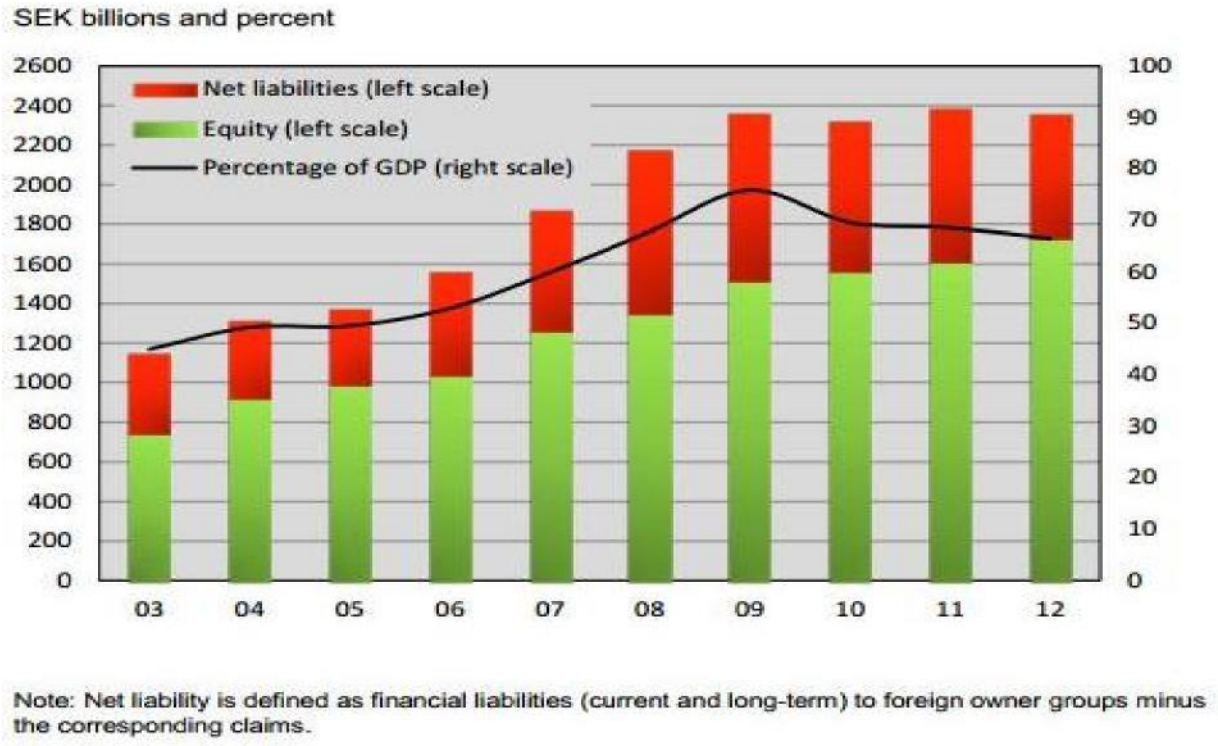


Figure 1. Foreign investments in Sweden.

A more comprehensive idea of the impact of the FRA Act in Sweden is obtained when we compare developments in Sweden, Finland and Denmark. Figure 2 shows that the entry into force of the FRA Act did not have any clear impact on foreign investments in Sweden as compared to Finland and Denmark. While the figure does not provide specific data on investments in the IT sector, they have followed the overall trends in all the countries included in the comparison.

gearshiftgroup

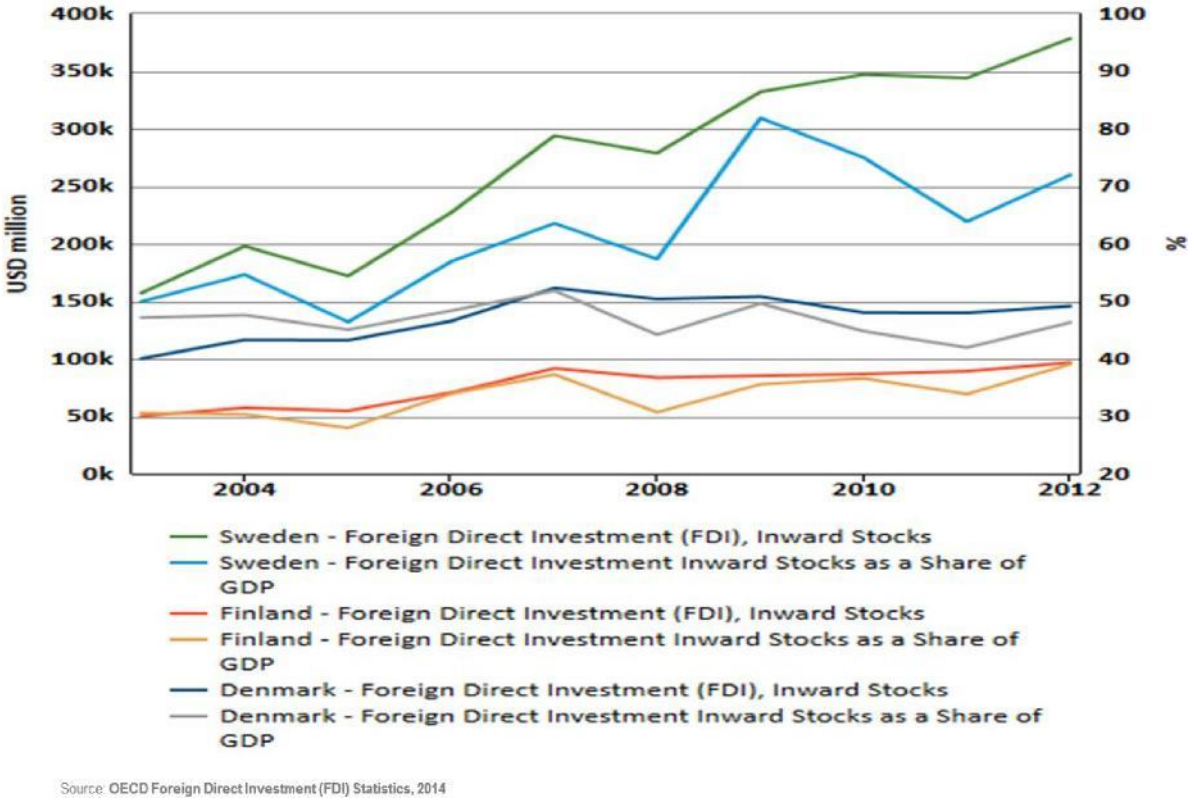


Figure 2. Foreign investments (USD million) as a percentage of GDP in Sweden, Finland and Denmark.

Generally, the foregoing figures suggest that there is no clear cause-and-effect relationship between the entry into force of the FRA Act and the level of foreign investments.

3.2 Impact on R&D activities in Sweden

When we examine the share of research and development costs relative to the GDP in Sweden and Finland as shown in Table 1, it is hard to discern any significant deviations in the overall trends. While the R&D expenditure relative to the GDP declined slightly in Sweden in 2009 and onwards, the same trend also set in in Finland in 2011. It should be noted, however, that even after this relative decline, Sweden and Finland still top the list of countries in terms of R&D expenditure relative to the GDP and clearly outperform, in this respect, the other EU countries included in the comparison. It is hard to see the fall in the level of R&D expenditure as a consequence of the FRA Act: after all, it was a period of time when the global economy was hit hard and businesses made cuts in their budgets. Moreover, the full impact of the recession was reflected on the figures for Finland with some delay.

Table 1. Research and development costs as a percentage of the GDP during 2002–2010.

	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
EU-28	*1.87*	1.86	1.82	1.82	1.84	1.84	*1.91*	*2.01*	*2.00*	*2.04*	*2.06*
Euro area (EA-17)	*1.88*	1.87	1.85	1.84	1.87	1.88	*1.96*	*2.06*	*2.07*	*2.12*	*2.14*
Belgium	1.94	1.87	1.86	1.83	1.86	1.89	1.97	2.03	2.10	2.21	*2.24*
Bulgaria	0.48	0.48	0.49	0.46	0.46	0.45	0.47	0.53	0.60	0.57	*0.64*
Czech Republic	1.15	1.20	1.20	1.22	1.29	1.37	1.30	1.35	1.40	1.64	*1.88*
Denmark (1)	2.51	2.58	2.48	2.46	2.48	2.58	2.85	3.16	3.00	2.98	*2.99*
Germany	2.50	2.54	2.50	2.51	2.54	2.53	2.69	2.82	2.80	2.89	*2.92*
Estonia	0.72	0.77	0.85	0.93	1.13	1.08	1.28	1.41	1.62	2.37	*2.18*
Ireland	1.10	1.16	1.23	1.25	1.25	1.28	1.45	1.69	*1.69*	*1.66*	*1.72*
Greece (2)	:	0.57	*0.55*	0.60	*0.59*	*0.60*	:	:	:	0.67	0.69
Spain	0.99	1.05	1.06	1.12	1.20	1.27	1.35	1.39	1.40	1.36	1.30
France (3)	2.24	2.18	2.16	2.11	2.11	2.08	2.12	2.27	2.24	2.25	*2.26*
Croatia	0.96	0.96	1.05	0.87	0.75	0.80	0.90	0.85	0.75	0.76	0.75
Italy	1.12	1.10	1.09	1.09	1.13	1.17	1.21	1.26	1.26	1.25	*1.27*
Cyprus	0.30	0.35	0.37	0.41	0.43	0.44	0.43	0.49	0.50	0.50	*0.47*
Latvia	0.42	0.38	0.42	0.56	0.70	0.60	0.62	0.46	0.60	0.70	*0.66*
Lithuania	0.66	0.67	0.75	0.75	0.79	0.81	0.80	0.84	0.79	0.91	*0.90*
Luxembourg	:	1.65	1.63	1.56	1.66	*1.58*	1.66	1.74	1.51	:	:
Hungary (4)(5)	1.00	0.94	0.88	0.94	1.01	0.98	1.00	1.17	1.17	1.22	1.30
Malta (4)	0.25	0.25	0.51	0.55	0.60	0.57	0.55	0.53	0.66	0.72	*0.84*
Netherlands (3)	1.88	1.92	1.93	1.90	1.88	1.81	1.77	1.82	1.86	2.03	*2.16*
Austria	2.12	*2.24*	2.24	*2.46*	2.44	2.51	*2.67*	2.71	*2.80*	2.77	*2.84*
Poland	0.56	0.54	0.56	0.57	0.56	0.57	0.60	0.67	0.74	0.76	0.90
Portugal (4)	*0.73*	0.71	*0.74*	0.78	*0.99*	1.17	1.50	1.64	1.59	1.52	*1.50*
Romania (2)(7)	0.38	0.39	0.39	0.41	0.45	0.52	0.58	0.47	0.46	0.50	*0.42*
Slovenia (4)(6)	1.47	1.27	1.39	1.44	1.56	1.45	1.66	1.85	2.10	2.47	*2.80*
Slovakia	0.57	0.57	0.51	0.51	0.49	0.46	0.47	0.48	0.63	0.68	0.82
Finland	3.36	3.44	3.45	3.48	3.48	3.47	3.70	3.94	3.90	3.80	3.55
Sweden (4)	:	3.80	3.58	3.56	*3.68*	3.43	*3.70*	3.62	*3.39*	3.39	*3.41*
United Kingdom	1.78	1.73	1.67	1.70	1.72	1.75	*1.75*	*1.82*	*1.77*	1.78	*1.72*
Iceland	2.95	2.82	:	2.77	2.99	2.68	2.65	3.11	:	2.40	:
Norway	1.66	1.71	1.57	1.51	1.48	1.59	1.58	1.76	1.68	1.65	1.66
Switzerland	:	:	2.82	:	:	:	2.87	:	:	:	:
Serbia	:	:	:	:	:	:	:	0.92	0.79	0.77	0.96
Turkey	0.53	0.48	0.52	0.59	0.58	0.72	0.73	0.85	0.84	0.86	:
China (except Hong Kong)	1.07	1.13	1.23	1.32	1.39	1.40	1.47	1.70	1.76	1.84	:
Japan (4)	3.12	3.14	3.13	3.31	3.41	3.46	3.47	3.36	3.25	:	:
United States (3)	2.52	2.52	2.45	2.49	2.55	2.62	2.76	2.81	2.73	2.67	:

(1) 2007: break in series. 2009: definition differs.
(2) 2011: break in series.
(3) 2004 and 2010: break in series.
(4) 2004: break in series.
(5) 2002 and 2003: definition differs.
(6) 2008: break in series.
(7) 2012: definition differs.
(8) 2005: break in series. 2003, 2004, 2006 and 2010: definition differs.
(9) 2006: break in series. Definition differs.
Note: when definitions differ, see http://epp.eurostat.ec.europa.eu/cache/ITY_SDDS/EN/rd_esms.htm.
Source: Eurostat (online data codes: t2020_20 and rd_e_gerdtot), OECD

Another perspective to the developments is offered by the sources of funding for R&D efforts. Table 2 provides a breakdown of the sources of funding available for covering research and development costs in 2007 and 2011. The figures showing the sources of funding in Sweden indicate that foreign actors have even increased their share of investments relative to the funding available within Sweden as well as relative to the investments made by the private and public sector during the period under review. This strongly suggests that the FRA Act has not played any role in the allocation of foreign R&D investments. Instead, the fall in the level of R&D spending is largely explained by a slow-down on the part of Swedish enterprises and the public sector.

Table 2. Sources of research and development funding in 2007 and 2011.

	Business enterprise sector		Government sector		Abroad	
	2007	2011	2007	2011	2007	2011
EU-28	*54.9*	*54.9*	*33.3*	*33.4*	*9.2*	*9.2*
Euro area (EA-17)	*56.7*	*56.8*	*34.0*	*33.9*	*7.4*	*7.4*
Belgium	61.4	60.2	22.2	23.4	13.0	13.0
Bulgaria	34.2	16.9	56.7	38.8	7.6	43.9
Czech Republic	47.2	37.7	44.7	41.7	7.3	19.7
Denmark (1)	61.0	60.3	25.9	28.9	9.5	7.2
Germany	68.1	65.0	27.5	29.8	4.0	4.2
Estonia	41.6	55.0	45.6	32.8	11.7	11.9
Ireland	49.5	*48.4*	32.4	*30.3*	15.8	*20.1*
Greece	:	32.7	:	49.2	:	14.8
Spain	45.5	44.3	43.7	44.5	7.0	6.7
France (2)	52.3	55.0	38.1	35.4	7.5	7.7
Croatia	35.5	38.2	50.4	48.2	10.9	11.6
Italy	42.0	45.1	44.3	41.9	9.5	9.1
Cyprus	16.4	11.0	64.6	70.6	14.5	14.1
Latvia	36.4	24.8	49.9	22.5	12.7	51.0
Lithuania	32.8	28.2	46.9	42.2	19.6	28.4
Luxembourg (3)	76.0	44.3	18.2	34.8	5.7	20.7
Hungary	43.9	47.5	44.4	38.1	11.1	13.5
Malta	51.9	51.9	25.7	29.0	22.4	16.8
Netherlands (2)	48.8	49.9	38.0	35.5	10.7	10.9
Austria	48.7	46.2	32.3	35.8	17.9	16.9
Poland	34.3	28.1	58.6	55.8	6.7	13.4
Portugal (2)	47.0	44.0	44.6	41.8	5.4	5.9
Romania (2)	26.9	37.4	67.1	49.1	4.5	12.1
Slovenia (2)	58.3	61.2	35.6	31.5	5.8	7.0
Slovakia (4)	35.6	33.9	53.9	49.8	10.2	14.2
Finland (5)	68.2	67.0	24.1	25.0	6.5	6.5
Sweden	62.8	57.3	24.6	27.7	9.6	11.1
United Kingdom	46.0	45.9	30.9	30.5	17.3	17.8
Iceland	50.4	47.5	38.8	42.3	10.0	8.4
Norway	45.0	44.2	44.9	46.5	8.5	7.8
Switzerland (6)	68.2	:	22.8	:	6.0	:
Serbia (7)	8.3	9.1	62.9	63.4	7.2	5.5
Turkey (8)	48.4	45.8	47.1	29.2	0.5	0.7
China (except Hong Kong) (3)	70.4	73.9	24.6	21.7	1.3	1.3
Japan (2)(3)(4)	77.7	75.9	15.6	17.2	0.3	0.4
United States (3)	64.9	*60.0*	29.1	33.4	:	:

(1) Government sector, 2007: definition differs.
(2) Break in series.
(3) 2010 instead of 2011.
(4) Government sector: definition differs.
(5) Government sector: break in series.
(6) 2008 instead of 2007.
(7) 2009 instead of 2007.
(8) Business enterprise and government sectors: break in series. Business enterprise and government sectors, 2007: definition differs.
(9) Definition differs.
Note: when definitions differ, see http://epp.eurostat.ec.europa.eu/cache/ITY_SDDS/EN/rd_esms.htm.
Source: Eurostat (online data code: tsc00031), OECD

To summarise the research and development spending, it is safe to say that the FRA Act has not had any practical impact on economic activity in this area. The biggest single factor explaining the changes is overall economic development and Sweden's continued investments in research and development relative to the GDP, which have remained at a high level despite the changes in the operating environment.

3.3 Impact on Sweden's international competitiveness

In a comparison made by the World Economic Forum, Sweden ranks among the top ten countries both in terms of international competitiveness and innovation. Figure 3 illustrates Sweden's competitiveness in the specific sectors of the economy. As shown in the figure, Sweden receives fairly high marks in many sectors. Based on these data, it is extremely difficult to determine the direct impact of the FRA Act on Sweden's competitiveness on a general level. At the same time, it should be noted that Sweden also has high marks for infrastructure and government action.

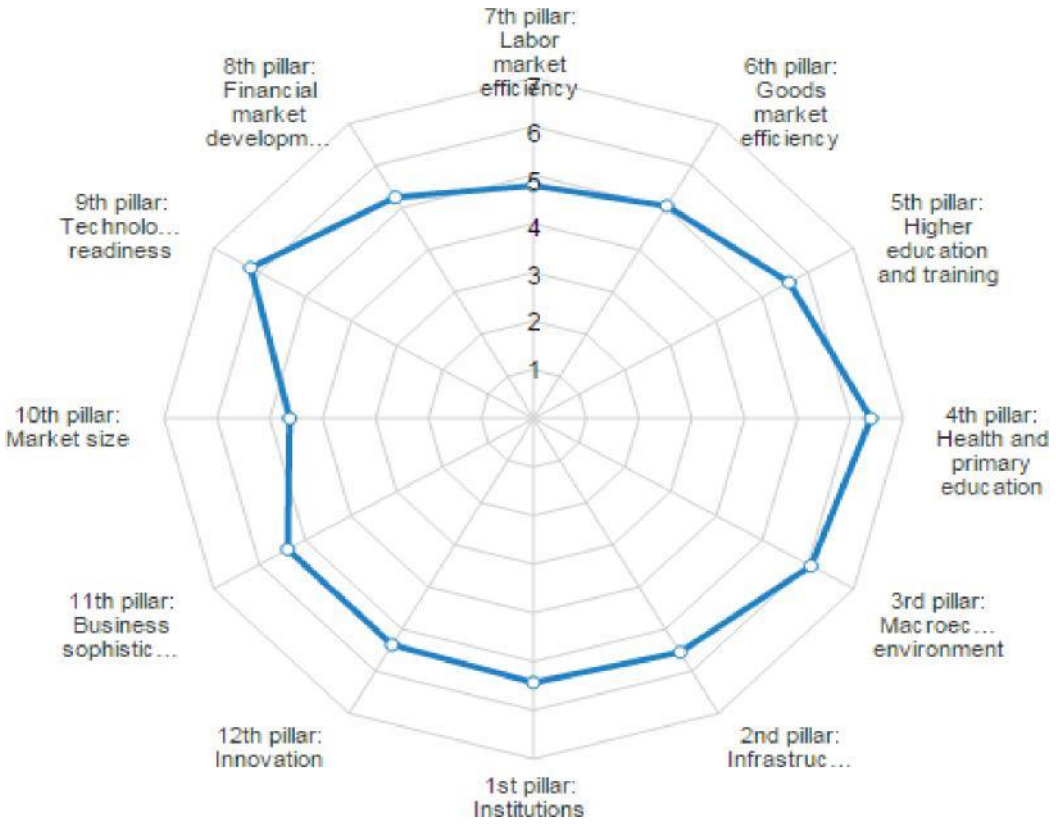
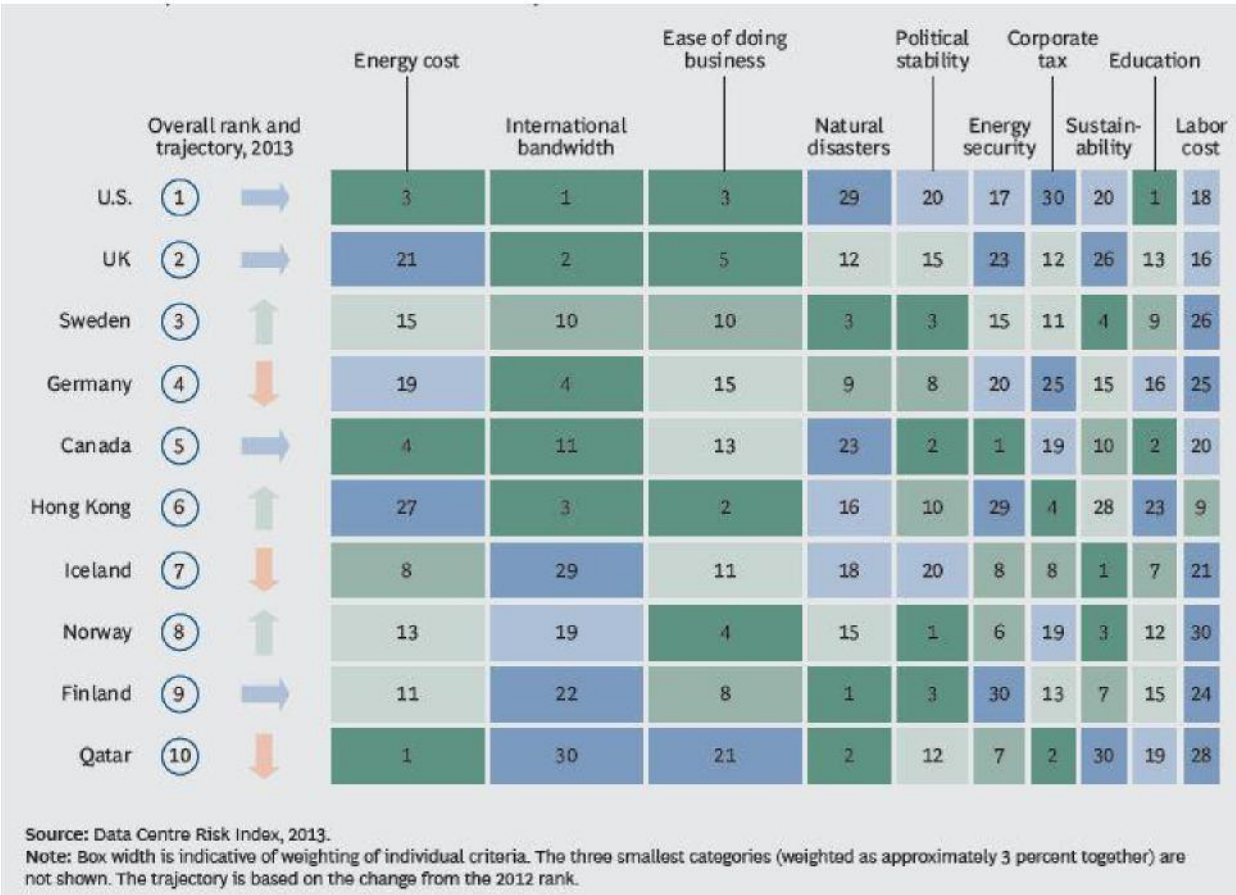


Figure 3. Sweden's competitiveness by sector. (www.weforum.org.)

A more illustrative assessment of the competitiveness of the various countries in terms of IT investments can be made by evaluating the general preconditions for the establishment and operation of data centres. The FRA Act is closely linked to the operating environment of data centres and the assessment of the locations of the facilities. Table 3 provides an annual risk comparison of the most important host countries for data centres. Sweden did extremely well in the 2013 comparison being ranked third, a great improvement from its eight place in 2012; Finland retained its ninth position in both years. Consequently, the polemic debate on the FRA Act at the time it was introduced is not reflected in the comparative risk analysis of the prospective host countries. In reality, Sweden's competitiveness in this respect has translated into major new data centre projects such as Facebook in 2011 and capacity expansion in 2014; KnC Minter in 2014; Hydro66 in 2014; and Bahnhof's major expansion project in Stockholm. Over the same period of time, investments in Finland were made by Google, which carried out several expansions, Telecity and Yandex.

Table 3. Comparison of risks associated with data centre host countries.



Source: Data Centre Risk Index, 2013.
Note: Box width is indicative of weighting of individual criteria. The three smallest categories (weighted as approximately 3 percent together) are not shown. The trajectory is based on the change from the 2012 rank.

An assessment of the impact of the FRA Act on Sweden's international competitiveness suggests that the law has not had any negative consequences, at least as far as the establishment of data centres is concerned. As data centres and their customer base cover a wide range of stakeholders, this approach provides a comprehensive idea of the situation. Moreover, said law did not figure in any way in the comparison of host countries.

In fact, it would even appear that due to the increased general awareness of the issues following the disclosures made by Snowden, the clear ground rules established by Sweden regarding intelligence gathering by the authorities may prove to give a competitive edge. With large long-term investments, risk minimisation and the predictability of the operating environment are important considerations affecting the competitiveness of the individual countries.

3.4 Impact on the creation of new businesses in Sweden and Finland

Over the past few years, Sweden's ICT sector has thrived compared to the rest of the economy. As a result, new ITC companies have been established and the overall significance of the entire sector has grown at a brisk pace. A comparative analysis of the rate at which new businesses have been founded in Sweden, Finland and Denmark during 2005–2008 (Figure 4) shows Sweden taking the pole position by a wide margin. The significance of the FRA Act in the general business environment is very low and thus cannot be deemed to have had any impact on the development of entrepreneurial activities or the establishment of new firms one way or another.

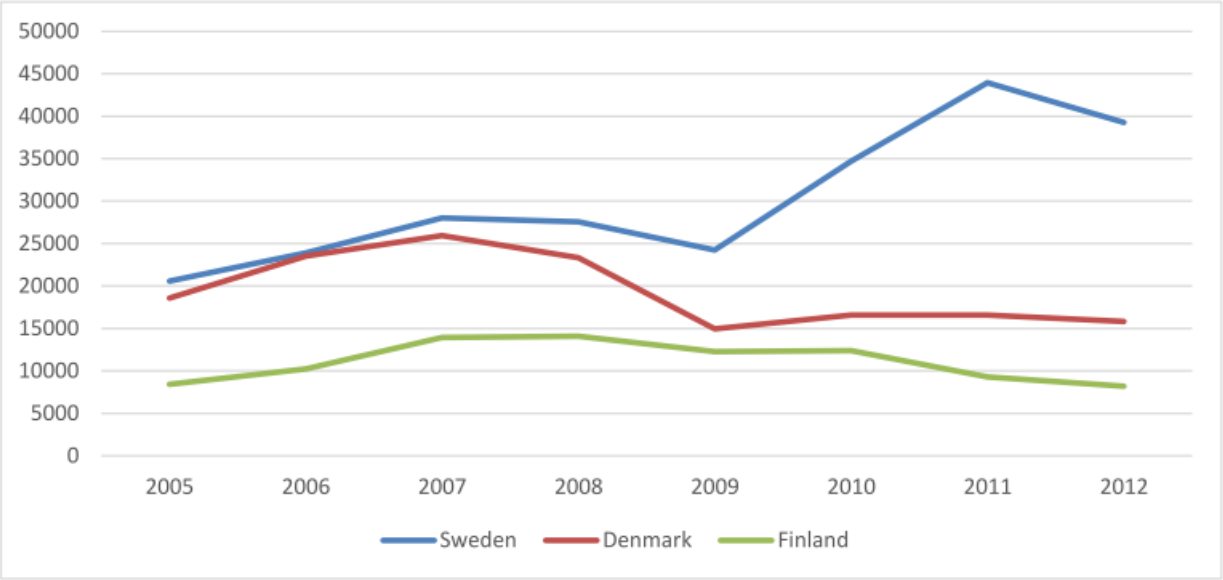


Figure 4. Number of companies established 2005–2012.

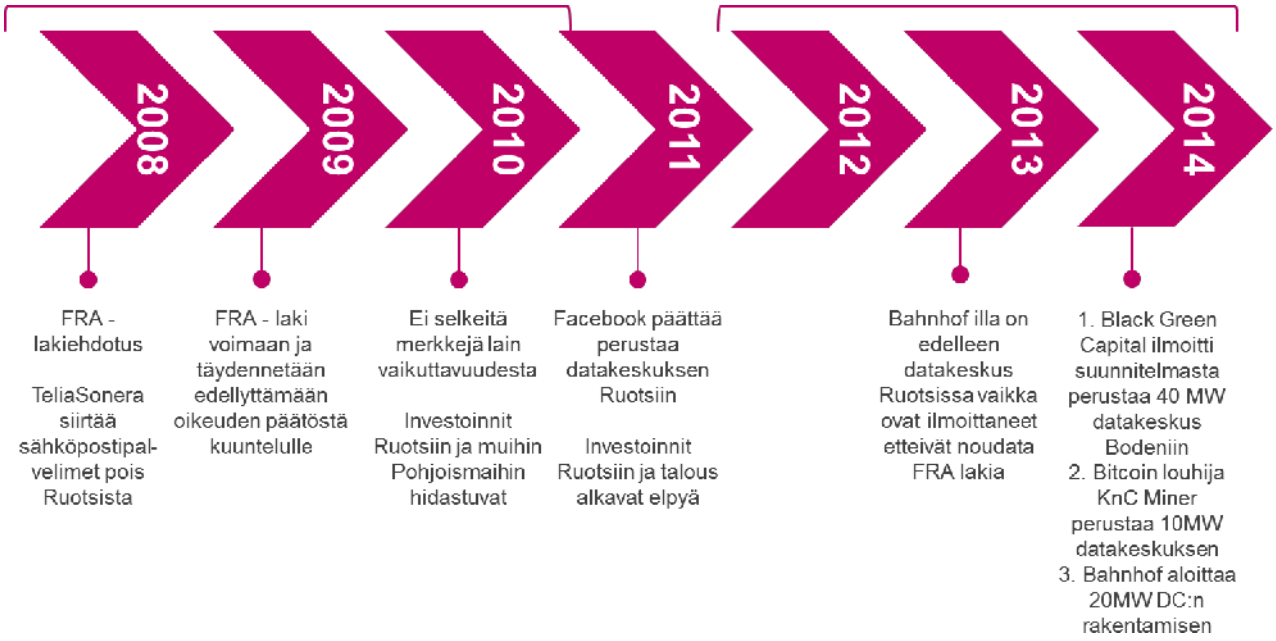
One indication of the strong showing of the ICT sector is the large data centre established by Facebook. When the original decision on the investment was made in 2010–2011, the FRA Act was already in force. Commenting on the FRA issue, Facebook announced that all states have their own ways of monitoring data communications and therefore, once clear-cut arrangements have been put in place, they were of no relevance to the investment decision.

3.5 Implications for various companies or groups of companies in Sweden

Following the enactment of the FRA Act, TeliaSonera relocated its e-mail server to Finland in 2008 because under Finnish law, the secrecy of correspondence applies equally to e-mail exchanges. At the same time, TeliaSonera relocated all its Swedish e-mail traffic to data centres in Finland; since then, however, no accurate information on the place of provision of the service or the location of the data containing e-mail traffic is available.

The FRA Act also inspired a lively debate in Sweden, particularly among ICT infrastructure players whose businesses could have been adversely affected by the new law. However, the real effects of the act have remained limited or practically non-existent. General awareness of intelligence gathering among companies has increased since the Snowden disclosures.

3.6 FRA timeline in Sweden



2008	2009	2010	2011	2013	2014
FRA bill TeliaSonera relo-cates e-mail serv-ers from Sweden	FRA Act enters into force and is amended by the inclusion of a requirement for a court order for wiretapping	No clear indica-tions of the Act having any impact Investments in Sweden and other Nordic countries slow down	Facebook decides to establish a data centre in Sweden Investments in Sweden and the economy pick up	Banhof continues to operate a data centre in Sweden despite their an-nouncement that they do not com-ply with FRA	1. Black Green Capital announces plan to establish 40MW data centre in Boliden 2. Bitcoin miner kNC Miner estab-lishes 10MW data centre 3. Banhof starts construction of 20MW data centre

Based on the timeline, it is safe to say after the initial confusion and uncertainty about the practical imple-mentation of the act that it has not had any impact on investments such as data centres. Similarly, the news of R&D investments announced in 20014 support the view that the act has not slowed down invest-ments. New companies also invest heavily:

17 June 2014 at 08:00 – CIO Sweden: ”IT investments growing faster than ever.”

4 Summary

Most of the strong positions and measures adopted by companies at the time when the FRA legislation was being prepared have mitigated. Current media reporting mainly focuses on civil rights, NSA disclosures and the political debate on the issue, and the general operation of the FRA law.

While Banhof, for one, says in public that it continues to object to the implementation of the act in its field of activity, the company does not clearly perceive the situation as detrimental to its own business or those of its customers. After all, they have greatly increased their presence in Sweden and have also launched an extensive new expansion project in Stockholm called 'Project Green'. The plan is to build a new 20MW data centre by the end of 2016, establish a major data communications node in the centre of Stockholm, and to harness energy production and cooling synergies in collaboration with Fortum. The facility of this size represents a EUR 200 million investment that cannot be made without binding agreements with customers.

In conclusion, it is safe to say that no clear connection between the potential impact of the FRA Act on foreign investments in the IT sector following the enactment of the law or differences relative to equivalent investments in Finland could be established on the basis of the present study.

At the same time, the findings suggest that a precise piece of legislation may actually provide a more predictable operating environment for the IT sector. Investments rest on a more solid foundation when the common ground rules are clear. Large international corporations are today more aware of cybersecurity, an area where regulations issued by the government to monitor content and defend against attacks are welcomed.

5 Links

Links related to Finland:

http://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-1.pdf
http://www.itviikko.fi/uutiset/2014/03/10/teknologia-ala-urkintalaki-saattaa-kostautua-kivuliaasti/20143451/7?pos=related

Links related to Sweden

http://www.thelocal.se/20070530/7452
http://www.aftonbladet.se/nyheter/article11442895.ab

Links related to Germany:

http://www.sueddeutsche.de/digital/bundesnachrichtendienst-aufruesten-fuer-den-cyberkampf-1.2211761

Other links:

http://www.itworld.com/article/2845603/german-spy-agency-seeks-millions-to-monitor-social-networks-outside-germany.html#tk.rss news

Contact details:
Vesa Weissmann
Gearshift Group Ltd.
Mannerheimintie 16, 4th Floor
FI-00100 Helsinki, Finland
Mobile +358 50 500 2120
Email vesa.weissmann@gearshiftgroup.com
Web www.gearshiftgroup.com

CONSULTATIONS WITH INTEREST GROUPS AND EXPERTS SUMMARY

1. Comments on the appointment of the working group

In a bid for support for its efforts, the working group requested statements on the decision to appoint the working group from the following seven parties:

- The Confederation of Finnish Industries
- Electronic Frontier Finland (EFFI)
- The Finnish Federation for Communications and Teleinformatics (Ficom)
- The Finnish Communication and Internet Exchange (FiCix)
- The National Emergency Supply Centre
- The Finnish Information Security Cluster (FiSC) and the Federation of Finnish Technology Industries (joint statement).

Additionally, FiCom made a background memorandum available to the working group ('Views of the business and industry regarding the legislative project to improve the intelligence-gathering capabilities of security authorities', version 0.3D, 16 Jan 2014).

Comments were specifically requested on the objectives and duties of the working group and the legal and socio-political considerations that it should take into account.

The round of comments was held early on in the project to enable the working group to give due considerations to the proposals during the course of its work.

A summary of the requests for statements, statements, other position papers and written information submitted to the working party has been posted on the Ministry of Defence's website.

2. Consultations with business and industry and organisations

The working group held two hearings, one for business and industry (29 April 2014) and one for organisations (6 May 2014). These hearings focused primarily on the monitoring of telecommunications for intelligence-gathering purposes. The participants were also provided with an opportunity for submitting statements in writing.
Written statements were submitted by:

- F-Secure Corporation
- Nokia Plc and Nokia Solutions and Networks (joint statement)
- TDC Oy
- Microsoft Corporation
- Finland Chamber of Commerce
- Internet-käyttäjät ikuisesti – IKI ry (Internet Users Forever)
- The Finnish Communication and Internet Exchange (FiCix)

The invitations, lists of participants, event programmes and the statements submitted to the working group are posted on the Ministry of Defence's website.

3. Provision of background information for the media

The working group held an information meeting for the media on 12 March 2014 to discuss the working group's remit and objectives as well as other issues to be considered during the course of its work.

4. Experts consulted by the working group

In the course of its mandate, the working group heard a total of 26 experts representing the key authorities and interest groups in the context of the project.

Jaakko Korhonen, Situational Awareness Coordinator, Head of Unit, Prime Minister's Office
Timo Härkönen, Director of Government Security, Prime Minister's Office
Ari Uusikartano, Director General, Information and Documentation Division, Ministry for Foreign Affairs
Kimmo Janhunen, Special Adviser, Ministry of Finance

Ilkka Salmi, Director of the EU Intelligence Analysis Centre
Georgij Alafuzoff, Director, Intelligence Directorate, EU Military Staff

Reijo Aarnio, Data Protection Ombudsman
Veli-Pekka Viljanen, Professor of Law, University of Turku

Christian Fjäder, Manager ICT, National Emergency Supply Centre
Kirsi Karlamaa, Director, Finnish Communications Regulatory Authority
Jarkko Saarimäki, Head of Security Regulation , Cyber Security Centre
Tomi Hasu, Information Security Expert, Cyber Security Centre
Robin Lardot, Director of the National Bureau of Investigation
Timo Piiroinen, Detective Inspector, National Bureau of Investigation
Pasi Paunu, Systems Analyst, Finnish Security Intelligence Service

David Mothander, Nordic Policy Counsel, Google
Vesa Vuoti, Administration and Security Manager, DNA Oyj
Krister Kaipio, Head of Special Network Security, TeliaSonera Finland Plc
Jaakko Wallenius, Security Manager, Elisa Corporation
Pasi Mäkinen, Platform Strategy Manager, Microsoft Oy
Kaisa Olkkonen, Vice President, Nokia Government Relations
Gabriel Waller, Head of Security Technologies, Nokia Solutions and Networks
Mikko Hyppönen, Chief Research Officer, F-Secure Plc
Kimmo Kasslin, Technology Director, F-Secure Plc
Jyrki Hollmén, SME Director, Confederation of Finnish Industries
Vesa Weissmann, Associate Partner, Gearshift Group Oy

5. Summary of the statements received from interest groups and experts

5.1. Project organisation, objectives and tasks

At the hearings, special attention was paid to the work to be carried out by the working party on intelligence gathering by the authorities as a process. In particular, the representatives of business and industry emphasised that companies should be more closely involved in issues unrelated to the division of powers between the authorities or similar considerations.

Targeted intelligence gathering across telecommunications networks is a sensitive issue. It should be prepared in close collaboration with business and industry. Concerns were raised about economic interests not holding centre stage in the efforts. Business and industry need to be able to depend on the authorities, just like the authorities need to be able to depend on business and industry.

Very little information was available on the working group's remit, especially in the early stages. The preparations were expected to be transparent, broad-based and thorough.

The six-month time limit established for the completion of of such an extensive project with wide-ranging social, political and long-term implications was felt to be too short.

The decision to establish the working group inspired a debate, including the fact that the decision may be interpreted as not necessarily giving a mandate to investigate intelligence-gathering needs beyond the cyber intelligence context. When the objectives of the working group are determined, the role of the private sector in identifying cyber threats should also be considered.

An assessment of the existing legislation was felt to be an important objective. Some of the parties argued that the current legislation already provides a great deal of latitude for action to the authorities. Further, no overlapping or mutually contradictory operational and surveillance mechanisms should be created.

Some experts held that the outcomes of the working group's efforts should not be drafted in the form of a government proposal. The memorandum to be drawn up to serve as a basis for the working group's further efforts should address the special regulation of specific sectors and assess the impacts of the regulation of intelligence gathering and any limitations of the scope of application sector by sector, for example in fields of activity such as healthcare and banking.

5.2. Nature of the Internet and communications

The experts highlighted the cross-border nature of the Internet and communications in general. Many of the services used by people in Finland are actually produced abroad. National borders do not count according to the experts. At the same time, cloud services are expanding and so the physical location of data no longer matters much.

The amount of data passing through the Internet is enormous and continues to grow. As a result, the organisation of all-encompassing surveillance is highly challenging, both technically and financially. Another issue raised at the hearing was that although the Internet has been around for 20 years, steps to investigate the problems associated with it have not been taken until now.

5.3. Level and further development of data security

It was pointed out at the hearing that Finland's reputation as a country with a high standard of data security was debatable. For example, businesses are not that well protected – there is a huge number of systems where no precautions have been taken with a view to potential cyber attacks. We tend to think that Finland is one of the most honest countries in the world; however, it is clear that there have been infractions but they have not come to light.

In the view of the interest groups, surveillance of the information received by the government organisations constitutes acceptable cyber security action. For example, this would apply to a given agency with clearly identified sites and offices. Examples cited in this connection included firewalls, the acquisition of secure software and in-house data security procedures complied with in daily activities. All this can be accomplished under the existing legislation.

A further point raised at the hearings was that it is up to the companies themselves to ensure a proper standard of data security as the government resources are simply not enough. All parties need to be prepared for cyber threats. Individual actors may be best placed to detect irregularities in their network traffic.

According to the experts, the government should be capable of defending against cyber attacks in order to ensure security of supply and to safeguard other core functions. However, whenever cyber defences are designed, it should be understood that a cyber security policy underlining the importance of the reactive detection and limitation of attacks is more risky in terms of the protection of fundamental rights than a preventive strategy emphasising the systems' capacity to resist attack.

The reactive detection of attacks and cyber intelligence call for real-time monitoring and profiling of data communications. In contrast, the efforts to increase the attack resistance of proactive systems focus on improving the systems in the course of development, with the result that the enhanced data security also shores up data protection.

Reactive detection and active counter-measures do not necessarily help in the face of a real conflict because the attacker may make use of zero-day vulnerabilities, which are either overlooked or the impacts of which are too quick to be addressed even through automatic adaptive measures. However, the provision of various surveillance and defence systems is the very essence of the business of companies offering data security products. Therefore, lobbying for these products is more intense than the efforts to promote the development of secure software, which would not require massive investments in systems but more so in training and processes.

Proactive security work, for example in compliance with the latest Information Security Instructions for Application Development (VAHTI1/2013), would improve the passive defence capability of the systems and lower the risk of zero-day attacks. Consequently, giving a greater strategic role to the efforts to improve the security of software and application development would most likely contribute both to the protection of fundamental rights and cyber security.

Also, there is a need to improve the exchange of information between the authorities in the event of data security infringements. Additionally, the authorities should be able to inform companies and private individuals of ongoing attacks to allow them to take defensive action. At the same time, it would be advisable to obligate the victims, depending of the degree of severity, to report the attacks and technology employed in order to make it possible for others to defend against them.

Comments were made on the centralised detection system for information security threats (HAVARO) saying that it was operational and has proved itself in practice. According to the expert, the system could probably be developed further to make it more suitable for intelligence gathering purposes. Steps should be taken to promote its adoption across central and local government administration. With HAVARA, or a commercially available monitoring system, it would be possible to target the intelligence-gathering efforts so as not to include communications that are of no intrinsic value or at variance with the general sense of justice. At the same time, the accurate targeting of intelligence activities permits precise and optimised cost control.

According to the National Emergency Supply Agency, HAVARA services will continue to be provided and reinforced as part of the operations of the National Cyber Security Centre. The CERT-FI and HAVARO services will be extended to include the shared government ICT services.

5.4. Finland as a safe haven of data

It was stressed at the hearings that Finland can serve as the guarantor of cyber security in the digital world. A key national vision is to stand out as a node for future data communications, a sort of 'Switzerland of Data' capable of handling international communications reliably and providing a secure storage location for data. Finland possesses a great deal of technology that could be harnessed in realising this vision.

The lack of confidence across the world has created a vacuum in the market, in which Finland will have unlimited opportunities for growth. This potential is underpinned by the planned subsea cables designed, among other things, to facilitate the establishment of knowledge-intensive industry in Finland.

Recent global developments give Finland the opportunity to serve as the country of rule of law in the cyber world. By acting fairly and defending the rights and independence of private individuals and companies, Finland can project itself as an intelligent digital society and the world's leading centre of secure technology and entrepreneurship.

The working group should seek to avoid a situation where Finland is first marketed as a secure, stable and predictable environment and then, once the investment decisions have been taken, adopts procedures that make hay of the previous efforts.

Another point raised at the hearings was whether 'Finland as a safe haven' could be taken to mean that in Finland you are safe from the authorities who lack the necessary powers to act. A closely regulated surveillance and monitoring system could actually give an edge in competition.

5.5. Impacts on business

The experts stressed that the new intelligence-gathering powers given to the authorities would affect individual companies differently. Companies should not be treated as one. Costs will be incurred by telecom operators in particular.

Costs play a crucial role and determine which country a company chooses to invest in. Today, the market covers the whole world. Costs should be analysed in advance as accurately as possible and a decision made as to who is to bear them.

It should noted that intelligence-gathering activities would target private property. The companies' consent should be secured for the activities. For telecom companies, data gathering is not part of their regular business. Therefore, they should not be called upon to bear either the costs, or the legal or moral responsibility.

The customer promise 'we will protect you' is based on the belief that these companies seek to ensure the confidentiality of communications. Conceivably, the authorities' intelligence-gathering powers may erode this trust.

Aside from direct consequences, we need to consider the perceptions that consumers and companies rely on when selecting services. The risk to Finland's reputation needs to be recognised. Caution should be taken so as not to give the impression that everything will be controlled and monitored when no such thing is even proposed.

On the other hand, it was highlighted that predictability is important to investors. Finland is a safe and secure country with an image value worth protecting.

The representatives of the telecom companies operating both in Finland and Sweden stated that as far as their respective companies were concerned, the FRA Act had not had any impact on their operations at the practical level.

5.6.Powers needed by the authorities

According to the comments received, monitoring network traffic related to criminal activities committed using Finland as the base should be intensified. It was concluded that under the current legislation, combing this traffic is not possible; instead, all cases are treated as isolated events. For example, the use of mal-

ware and other technologies by cyber criminals and government actors is often based on active data communications connections beyond Finland's borders. Technically, the network traffic related to such activities could be detected and identified without any need to monitor the content of such traffic or all the internal traffic in Finland.

The transparency of government actions was felt to be important; after all, it is very much part of the Finnish political culture. All that the authorities are up to should openly disclosed. It was also noted that the actions of Finnish authorities abroad would mostly likely not create any problems from the service providers' point of view.

Although Finland already has extensive coercive powers and legislation with regard to telecommunications in place, they are not exercised to the full.
If new regulations on intelligence gathering by the authorities are introduced, the related tasks and powers must be closely identified and defined in sufficient detail. A clear legal basis must be created for intelligence gathering.

The laws should also provide a definition of malicious traffic, and any legislation addressing this area should be precise and accurate. It was thought that Finland could stand out from the crowd in this respect. The law should clearly stipulate what the authorities may and may not do, as this will inspire confidence in government action. Similarly, the distribution and intended use of the information should be closely regulated.

Sufficiently precise regulation also calls for a definition of the cyber environment and the establishment of objectives. The objectives must be based on a perception of the type of decision making and operations that intelligence gathering is supposed to support, what other parties are involved beside the security authorities and what obligations and burdens this will impose.

The resources available to the authorities were also brought up. For example, the Swedish FRA has a EUR 100 million budget and 300 employees. Before any project can be launched, its efficiency must be ascertained. At present, surveillance is also being carried in Finland's neighbouring countries.

Yet another option that may have to be considered is that the actual services would not be provided by the authorities at all; instead, they would be called upon to create the framework for cooperation and exchange of information between the various parties.

5.7. Mass surveillance

Mass surveillance was perceived in various ways. It emerged in the course of the hearings that intelligence gathering from all telecommunications using precise search criteria was also considered as mass surveillance. Even if no data beyond the search criteria were accessed, it constitutes mass surveillance because monitoring is not targeted. It was also argued that mass surveillance would no longer be possible in any EU Member State after the data retention judgement handed down by the EU Court of Justice.

Mass surveillance cannot be defined by any administrative decision. 'Combing' is taken to mean mass surveillance. The authorities would be tasked to control every aspect of where the data is sourced.

A sense of proportion was felt to be important. It would be necessary to strike a balance as to how extensively monitoring is carried out. All-embracing surveillance is not generally accepted.

According to the experts, mass surveillance does not really help in combating cyber threats. This is because it is a reactive response where problems are not detected until the threat is realised and an intrusion to a consumer device or government network has already taken place.

5.8.Back doors and decryption keys

Back doors – the ability of the authorities to access a computer, software or similar without the user being aware of it – were felt to present problems, and it was proposed that such a possibility should be excluded from the authorities' toolkit. Similarly, it was felt to be important that no obligation will be imposed on companies to create back doors or release keys to the authorities for decrypting purposes. In the view of the experts, both would have a highly detrimental impact on business as the consumers' trust in the products would be eroded.

5.9. Protection of privacy, confidential communications and sources

The protection of privacy is a fundamental right in any consideration of the intelligence-gathering powers of the authorities. Despite this, it is notable that people disclose very much information about themselves to companies over the Internet, for example in the social media.

On the matter of the protection of privacy, the organisations stated that right to privacy is a fundamental value: the state may not gather information on citizens if they are irreproachable and their conduct impeccable. Data may not be gathered even if they are not analysed or evaluated. The mere act of gathering data is a violation of privacy.

The experts pointed out that significant in this respect are Article 7 (Respect for private and family life) and Article 8 (Protection of personal data) of the Charter of Fundamental Rights of the European Union.

It was agreed at the hearing that public trust in the confidentiality of communications services must not be shaken, except for substantial reasons. Any cyber intelligence gathering (presumably meaning telecommunications intelligence) would represent a major change to the Finnish legal system and could erode user confidence in the communications and other services provided by Finnish actors.

Views were expressed at the hearings to the effect that no intelligence-gathering activities should include the option of compelling journalists to reveal their sources. Source protection is based on trust that may not be compromised.

Application of the established interpretation of the confidentiality of communications as defined by the Constitution Law Committee to intelligence gathering is complicated. Due consideration must be given to the doctrine of avoidance of any emergency powers acts. If the objective is to create permanent arrangements, emergency powers legislative procedures would not be enough; instead, the wording of section 10(3) of the Constitution would have to be reassessed. The existing wording cannot be extended to intelligence gathering by any extension of the interpretation.
Any restriction on any fundamental right needs to be duly justified. For example, section 10(3) of the Constitution presupposes a substantiated suspicion of the commission of a crime.

From a legal point of view, equating intelligence gathering to measures permitted to achieve data security was not considered tenable.

5.10. Impact on foreign policy and foreign relations

It emerged at the expert hearing that the storage and confidentiality of sensitive information on foreign states acquired through intelligence work in the national context involves a political risk. Recent international developments show that national cyber intelligence schemes have wide-ranging foreign policy implications.

Any conflicts between states need to be settled. To avoid conflicts in legislation, states need to establish a sustainable framework conducive to transparency for the management of cross-border requests for information, for example by strengthening the existing agreements on executive assistance.

States need to agree on procedures for resolving problems arising from potential conflicts between the laws of individual countries.

5.11. Permission for intelligence gathering by the authorities and regulatory oversight

The experts consulted by the working group argued that intelligence gathering must have a mandate laid down by law, and its implementation must be subject to permission.

Intelligence gathering should be based on acceptable criteria to be assessed by the whole of society (parliamentary control).

Additionally, the experts pointed out that the activities of the authorities should be subject to control. The greater the powers granted, the more efficient control. Such control must be independent. The system should be transparent, closely controlled and inspire public confidence. Sufficient advice must also be provided.

Any errors in enforcement must be sanctionable. A system establishing liability for damages must also be created. Since the activities are covert, the affected parties must be provided with an opportunity to de-

fend themselves if they feel that they have been subject to improper probing. The burden of proof must rest with the authority gathering the information.

It was also noted that if the working group decides to propose an extension of the rights of access to information, it should also examine the issue in terms of introducing controls regarding the procedures employed in gathering intelligence. An efficient and comprehensive system of controls, including media control, should be put in place.

Parties assisting the authorities must have the right to publish general information (e.g. statistics) on how they have provided such assistance. This is important especially in terms of the legal protection of the companies. Similarly, the citizens have a right to know the extent to which cyber monitoring is carried out in Finland and what results have been achieved through such monitoring.

Additionally, Finland must establish an operations model where proof is left of all the actions taken by the authorities in their efforts to combat and investigate crimes. Such proof can be used to demonstrate that no excesses have taken place and that all actions have been in compliance with joint decisions. By doing so, Finland will be able to gain broad international trust as a cyber-secure country in which it pays to invest and store data. It is important to be able to show to those subjected to surveillance what information had been gathered and to what parties it had been forwarded. This will prevent the risk of any ongoing misuse and offer the exceptional opportunity to establish Finland as a true 'Switzerland of Data'.

Due to the nature of intelligence, the organs overseeing the activities need to be independent and impartial. Those subjected to surveillance and receiving requests for information must have the opportunity to appeal.

To enable citizen control, all significant decisions of the authorities and control organs must be announced promptly.

It was established that reporting on the activities was of great importance. For example, Google publishes the official requests for information it receives. It is essential that companies will be able to release reports in the future as well. Similarly, the authorities need to provide accurate reports on their operations and publish statistics. To enable a genuine public discourse, the authorities should be obligated to disclose the total number of requests made.

5.12. Summary

On the whole, the experts consulted by the working group found it positive that Finland's cyber security is being developed by assessing the current regulations and identifying the needs of the security authorities while giving due consideration to the fundamental rights of the citizens. Almost all the feedback received underlined the importance of a careful analysis of the effects of the proposals for further development.
Much attention in the feedback was attached to data security and its enhancement. As far as the prevention of cyber threats is concerned, it is important for both public and private actors to ensure data security

in their own respective networks through technical measures, among others. Efforts should be made to improve the exchange of information between the key actors.

The comments at the hearings primarily addressed the monitoring and surveillance of data networks. Mass surveillance and back doors to software were generally opposed. However, to ensure security, it was considered justified to carry out well-founded, accurately targeted measures in the cyber environment in response to the situation at hand.
The interest groups stressed that public trust in the confidentiality of communications services must not be eroded except for substantial reasons. Cyber intelligence gathering could erode user confidence in the communications and other services provided by Finnish actors. However, it was recognised that, in the interest of national security, the authorities should have the capabilities to combat crime and the threat of terrorism with due regard to the rights of the individual and secrecy of communications.

A number of issues related to fundamental rights were raised such as the protection of privacy and access to information, confidentiality of communications, freedom of trades, protection of private property and freedom of speech.

Special concerns were raised about competitiveness and Finland's reputation as a safe haven of data, the impacts of the working group's proposals on business and foreign investments in Finland.
Finland's reputation as a country that respects the right to privacy is one of the competitive edges enjoyed by the Finnish IT industry that should be retained. No steps should be taken that could diminish the attractiveness of Finnish companies as investment objects.

Special attention in the comments was drawn to the supervision of the operations of the security authorities and maximum transparency. An efficient and comprehensive system of controls should be put in place.

Citizens should have a right to know the extent to which cyber monitoring is carried out in Finland and what results have been achieved. Similarly, companies should be able to report on the requests for information they have received.

The representatives of the interest groups pointed out that improvements to data security call for cooperation between the authorities and private sector actors. Efforts are needed from all the parties involved.

Unofficial translation
Ministry of Defence, Finland
March 2015

MEE/2491/00.05.01/2013

16 December 2014

Ministry of Defence

Statement on the report by the Working Group on Intelligence Legislation

According to the Government Resolution on cyber security strategy issued 24 January 2013, the cyber security duties of the ministry consist of the duties defined in the Security Strategy for Society. As part of the Government, the Ministry of Employment and the Economy (MEE) is responsible for the operating environment of businesses and innovation activities. In this context, the Ministry of Employment and the Economy is called upon (3) to support incident and continuity management in business and industry through its decision-making and governance systems; and to take action to create and maintain an investment-responsive and secure operating environment for entrepreneurial activity, foreign data centres included.

At a joint meeting on 7 November 2013, the President of the Republic and the Cabinet Committee on Foreign and Security Policy addressed, among other things, the need to enhance national cyber security. As part of the implementation of the Finnish cyber security strategy, the Cabinet Committee on Foreign and Security Policy concluded that prompt action was to be taken to develop Finnish legislation in this area (measure no. 42 of the implementation programme and a proposal for the entity in charge and partners). As a result, the Ministry of Defence, in its capacity as the entity in charge, appointed on 13 December 2013 a civil service working group – Working Group on Intelligence Legislation – in which the Ministry of Employment and the Economy also participated. In its report, the Working Group on Intelligence Legislation proposes new powers for intelligence-gathering purposes that would apply to telecommunications intelligence and extraterritorial intelligence (extraterritorial personal intelligence and information system intelligence).

The Ministry of Employment and the Economy understands and accepts the background, objectives and mandate of the decision to appoint the Working Group on Intelligence Legislation, including the need to develop the performance capabilities of both the Defence Forces and the police on a broad front.

From the perspective of the MEE's area of responsibility, industrial and economic policy considerations, such as the general operating conditions of business and industry, the promotion of competitiveness, the elimination of excessive administrative burdens, circumstances related to the evolution of a digital ecosystem, and the promotion of foreign investments are valid considerations that merit careful scrutiny along with the security policy and civic society issues in the context of the efforts of the working group.

The statement issued by the Ministry of Employment and the Economy relates to the conclusions and proposals for further development regarding electronic intelligence gathering. In this respect, the Ministry of Employment and the Economy agrees with point 4 (*Online surveillance can have significant implications for business and industry*) of the dissenting opinion issued by the Ministry of Transport and Communications. Said section goes on to say that online surveillance and related powers may have negative consequences for the competitiveness of both business and industry and for investment decisions. For example, one of the objectives established in Prime Minister Stubb's government programme was to make Finland into an international hub for data communications. Whether this goal can be achieved depends on Finland's ability to succeed in the competition for foreign investments. Additionally, the Prime Minister has stated that cyber intelligence legislation will be reassessed in the programme and during the term of the next government.

Based on these premises, the Ministry of Employment and the Economy holds that, considering the major economic policy and other social implications of the issue, it is necessary to appoint a more broad-based working group in which business and industry is also fully represented in order to be able to credibly examine, assess and express an opinion of the pros and cons of communications-related intelligence gathering, draw conclusions and put forward proposals for legislative reforms.

MEE-appointed Member of the Working Group on Intelligence Legislation

Kari Mäkinen
Director of Human Resources and Administration, Head of Preparedness

POLIISI
POLIISIHALLITUS

Statement ID-1555035541 109 (120)

16 December 2014 POL-2014-16707

Ministry of Defence

Statement by Assistant National Police Commissioner Tomi Vuori on the report by the Working Group on Intelligence Legislation

On 13 December 2013, the Finnish Ministry of Defence appointed a working group with a mission to develop Finland's legislation, specifically with regard to the regulation of intelligence gathering by the security authorities. The objective was to improve national security management, particularly in terms of combating threats in cyber networks. The members of the working group included representatives from the key government agencies responsible for internal and external security as well as from the ministries responsible for issues related to the remit of the working group as defined in the division of duties in government.

Over the past few years, security issues have been characterised by a blurring of the distinction between military and civilian threats. Among other things, this has been reflected in that a more broad-based concept of security has been adopted in Finland. With regard to the threats to data networks in particular, it is difficult tell, at least initially, what types of threat are involved. It is extremely important that the situation picture formed by the security authorities is sufficient, even if it relates to a grey area outside the conventional classification of threat scenarios.

More specifically, the working group was to address threats to data networks, also referred to as cyber threats. At the same time, the administrative position and powers of the Finnish Security Intelligence Service were being assessed by a committee established by Minister of the Interior Päivi Räsänen with a partly overlapping remit. To the extent the working group came to address the powers related to extraterritorial intelligence activities in contexts beyond just data networks, I feel bound by the outcome of the Ministry of the Interior project because the police representative on said committee was my superior National Police Commissioner Mikko Paatero and also because the issue was not included in the original remit of this working group.

Digitalisation is a trend that permeates all functions of society. At the same time as services migrate to electronic networks, the threats unfortunately migrate as well. However, this trend is irreversible. Consultations with experts underlined the need to protect

the online environment of people, businesses and society at large from cyber threats while at the same time stressing the importance of freedom of communications. Consequently, the task is highly topical but also extremely complicated. The final outcome should be a system that gives due consideration to fundamental rights while protecting all from threats to internal and external security.

In the administrative sector of the Ministry of the Interior, the working group's remit concerns primarily the police, including the Security Intelligence Service. On 12 March 2007, the Ministry of Justice and the Ministry of the Interior appointed a committee (Criminal Investigation and Coercive Measures Committee) with the remit to prepare the overall reform of the Criminal Investigation Act, the Coercive Measures Act and the Police Act. Special attention was to be paid to issues such as performance of searches in or via data networks. However, the first priority in this project was not intelligence gathering from telecommunications networks by the police and other law enforcement agencies. While this theme was discussed, it was not until after the committee's report (Ministry of Justice, Committee Report 2009:2) was submitted on 17 April 2009 that subsequent technical advancements and developments in society have made it clear that the time has come to address this issue with great determination. The undersigned was the only member of the present working party who also served on said committee. The new Criminal Investigation Act, the Coercive Measures Act and the Police Act took effect at the beginning of 2014. Covert intelligence gathering by the police – and the Security Intelligence Service – is based on this set of laws.

As far as the efforts of the working group now submitting its report is concerned, I wish to say that there is broad understanding within the police for the reasons why this project was launched in the Ministry of Defence's administrative sector. Similarly, there are valid grounds for a review of the intelligence gathering needs of the Security Intelligence Service insofar as they differ from those of the police. Even though there are a number of clear distinctions between internal and external security, it is, in the final analysis, a question of an undivided whole that can be perceived as security in the widest sense of the concept. The work carried out by the working group suggests that solutions applicable to the police and the defence forces may be different from the legal point of view. This also applies to some of the duties of the Security Intelligence Service. This is because cyber threats are usually – if not always – linked to suspected crimes. After all, the police is the authority with the general powers of action in crime prevention.

The authorities responsible for security have a fully justified need to obtain information from data networks for the purpose of preventing threats related to their respective fields of activity. Anti-virus protection and other such indispensable technical tools alone are not enough to neutralise cyber threats. In fact, the most serious threats are unaffected by such arrangements. Finland will not be an exception in the international context. However, it is clear that this is a highly sensitive area because, fundamentally, it is a question of where the line should be drawn between the protection of privacy and access to information by the authorities. This question will be resolved on constitutional grounds unless such drastic steps as to amend the Constitution are taken.

In my opinion, due consideration in the future efforts should be given to the possibility that the intelligence needs of the defence and police administrations can be satisfied through different procedures. In this sense, the Security Intelligence Service stands on the watershed: some of the gaps in its powers may be filled through amendments applicable to the regular police while others may have to be assessed in other contexts. As far as the police is concerned, my view is that progress could be made within the framework of section 10 of the Constitution by following the regular legislative process with regard to criminal procedures. This is an area that was, in a way, by-passed in the work carried out by the Criminal Investigation and Coercive Measures Committee. However, in the light of recent developments, it has proved to be necessary to address this issue. It should be pointed out that extensive efforts were made by the working group to take the intelligence needs of the Security Intelligence Service into account.

As already indicated, the powers of the Security Intelligence Service should be assessed separately from those of the rest of the police force. This applies to intelligence gathering (in the widest sense of the word) unrelated to criminal investigations, such as the preparation of incident and threat assessments. In these situations, the powers cannot be based on a crime as described above because the issue is beyond the scope of the applicable legal framework. At any rate, it is clear that Finland needs intelligence-gathering capabilities – in addition to military intelligence – unrelated to criminal offences.

It is of great importance for the police that the totality of crime prevention is not split and that its powers extend to all situations arising in its area of responsibility. In the course of the work carried out by the working group, it became evident that a more detailed study is needed to determine the extent to which the covert coercive measures permitted under the Police Act are good for, and identify the purposes for which new intelligence-gathering powers are concretely required. I wish to draw attention to the fact that it was not possible – in the course of the preparation of the working group's report – to attach enough importance to the perception of the criminal process and crime prevention as a whole. Intelligence gathering is one way of collecting information, and is seen as an integral part of the totality of crime prevention from the police's point of view.

Consequently, it would appear that the needs of the police – as opposed to some of the needs of the Security Intelligence Service – to improve the efficiency of intelligence gathering in cyber networks could be satisfied within the Constitution by addressing the essential elements of crimes and criminalising criminal attempts. One option could be to extend the criminalisation of offences jeopardising security in society as in the case of acts of terrorism. With some criminal attempts, criminalisation covers planning, recruitment and similar, while others require concrete acts, such as acquisition of various items or firearms or similar. Evidently, it would be possible to safeguard access to crime-related information while staying within the limits of the legal framework in situations where the contemplated crime does not yet target any specific individual (unidentified

threat), but where such evidence of a conspiracy to plan a criminal act or an equivalent initial action exists as to warrant the issuance of permission to gather intelligence.

Urgent efforts to improve the efficiency of intelligence gathering by the police for the prevention of cyber crime are called for. It would be advisable to promptly commence the preparation of legislation which would permit this type of collection of information and also provide the Security Intelligence Service with the necessary additional powers.

Assistant National Police Commissioner Tomi Vuori

This document has been signed electronically in the Aspo case management system. National Police Board, 16 December 2015 at 11.20 The signature can be verified by contacting the Registry.

Attachments None

Distribution Ministry of Defence

C.C. National Police Commissioner Mikko Paatero