Cyber Security Strategy

Cyber Security Strategy Committee

Ministry of Defence

ESTONIA

Tallinn 2008

CONTENTS

Summary

The asymmetrical threat posed by cyber attacks and the inherent vulnerabilities of cyberspace constitute a serious security risk confronting all nations. For this reason, the cyber threats need to be addressed at the global level. Given the gravity of the threat and of the interests at stake, it is imperative that the comprehensive use of information technology solutions be supported by a high level of security measures and be embedded also in a broad and sophisticated cyber security culture.

It is an essential precondition for the securing of cyberspace that every operator of a computer, computer network or information system realises the personal responsibility of using the data and instruments of communication at his or her disposal in a purposeful and appropriate manner.

Estonia's cyber security strategy seeks primarily to reduce the inherent vulnerabilities of cyberspace in the nation as a whole. This will be accomplished through the implementation of national action plans and through active international co-operation, and so will support the enhancement of cyber security in other countries as well.

In advance of our strategic objectives on cyber security, the following policy fronts have been identified:

- application of a graduated system of security measures in Estonia;
- development of Estonia's expertise in and high awareness of information security to the highest standard of excellence;
- development of an appropriate regulatory and legal framework to support the secure and seamless operability of information systems;
- promoting international co-operation aimed at strengthening global cyber security.

Policies for enhancing cyber security

1. The development and large-scale implementation of a system of security measures

The dependence of the daily functioning of society on IT solutions makes the development of adequate security measures an urgent need. Every information system owner must acknowledge the risks related to the disturbance of the service he or she provides. Up-to-date and economically expedient security measures must therefore be developed and implemented. The key objectives in developing and implementing a system of security measures are as follows:

- to bolster requirements for the security of critical infrastructures in order to increase its resistance, and that of related services, against threats in cyberspace; to tighten the security goals of the information systems and services provided by the critical infrastructure;

- to strengthen the physical and logical infrastructure of the Internet. The security of the Internet is vital to ensuring cyber security, since most of cyberspace is Internet-based. The main priorities in this respect are: strengthening the infrastructure of the Internet, including domain name servers (DNS); improving the automated restriction of Internet service users according to the nature of their traffic, and increasing the widespread use of means of authentication;
- to enhance the security of the control systems of Estonia's critical infrastructure,
- to improve on an incessant basis the capacity to meet the emergence of newer and technologically more advanced assault methods;
- to enhance inter-agency co-operation and co-ordination in ensuring cyber security and to continue public and private sector co-operation in protecting the critical information infrastructure.

2. Increasing competence in cyber security

In order to achieve the necessary competence in the field of cyber security, the following objectives have been established for training and research:

- to provide high quality and accessible information security-related training in order to achieve competence in both the public and private sectors; to this end, to establish common requirements for IT staff competence in information security and to set up a system for in-service training and evaluation;
- to intensify research and development in cyber security so as to ensure national defence in that field; to enhance international research co-operation; and to ensure competence in providing high-level training;
- to ensure readiness in managing cyber security crises in both the public and private sectors;
- to develop expertise in cyber security based on innovative research and development.

3. Improvement of the legal framework for supporting cyber security

The development of domestic and international legislation in the field of cyber security is aimed at:

- aligning Estonia's legal framework with the objectives and requirements of the Cyber Security Strategy;
- developing legislation on protection of the critical information infrastructure;
- participating in international law-making in the field of cyber security and taking steps internationally to introduce and promote legislative solutions developed in Estonia.

4. Bolstering international co-operation

In terms of developing international co-operation in ensuring cyber security, the Strategy aims at:

- achieving worldwide moral condemnation of cyber attacks given their negative effects on people's lives and the functioning of society, while recognising that meeting the cyber threats should not serve as a pretext for undermining human rights and democratic freedoms;
- promoting countries' adopting of international conventions regulating cyber crime and cyber attacks, and making the content of such conventions known to the international public;
- participating in the development and implementation of international cyber security policies and the shaping of the global cyber culture;
- developing co-operative networks in the field of cyber security and improving the functioning of such networks.

5. Raising awareness on cyber security:

Raising public awareness on the nature and urgency of the cyber threats might be achieved by:

- presenting Estonia's expertise and experience in the area of cyber security at both the domestic and international level, and supporting co-operative networks;
- raising awareness of information security among all computer users with particular focus on individual users and SMEs by informing the public about threats existing in the cyberspace and improving knowledge on the safe use of computers;
- co-ordinating the distribution of information on cyber threats and organising the awareness campaigns in co-operation with the private sector.

1 Introduction

The numerous cyber attacks launched in recent years against advanced information societies aimed at undermining the functioning of public and private sector information systems have placed the abuse of cyberspace high on the list of novel security threats. The acknowledgment that such attacks pose a threat to international security reached new heights in 2007 owing to the first-ever co-ordinated cyber attack against an entire country - Estonia – and also because of large-scale cyber attacks against information systems in many other countries as well. The recurrence and growing incidence of cyber attacks indicate the start of a new era in which the security of cyberspace acquires a global dimension and the protection of critical information systems must be elevated, in terms of national security, on a par with traditional defence interests.

The co-ordinated cyber attacks against Estonian government agencies, banks, and media and telecommunications companies demonstrated that the vulnerability of a society's information systems is an aspect of national security in urgent need of serious appreciation. We have clearly and unambiguously acknowledged the need to protect information systems in advanced information societies, but the measures we have taken have not always been sufficient for that purpose. The protection of a country’s entire cyber assets calls for a comprehensive effort involving all sectors of national society, a clear and efficient allocation of responsibilities therein for the prevention of cyber attacks, and increased general competence and awareness regarding threats in cyberspace.

Our overall task rests on a prescient awareness of the need to balance, on the one hand, the risks associated with the use of information systems and, on the other hand, the indispensability of extensive and free use of information technology to the functioning of open and modern societies — and the understanding that this is a challenge confronting not only Estonia but also the rest of the world. The growing threats to cyber security should not hinder the crucial role of information and communications technology in impulsing the future growth of economies and societies. Furthermore, the global and asymmetrical nature of the cyber threats impede efforts at defining the national boundaries of cyberspace. It is clear from the nature of the challenges before us that nothing short of a global and comprehensive effort will suffice: the responsibilities of each citizen, each information system owner, and every state need to be stressed. So too the conduct of cyber attacks must be recognised by the international community as a morally condemnable action.

1.1 Principles for ensuring cyber security

National cyber security is a broad term encompassing many aspects of electronic information, data, and media services that affect a country's interests and wellbeing. Ensuring the security of a country's cyberspace thus comprises a range of activities at different levels. Toward this end, the most important policy domains include reducing the vulnerability of cyberspace, preventing cyber attacks in the first instance and, in the event of an attack, ensuring a swift recovery of the functioning of information systems. Thus, a cyber defence strategy must appraise the vulnerability of a country's critical infrastructure, devise a system of preventive measures against cyber attacks, and decide upon the allocation of tasks relating to cyber security management at the national level. Moreover, it is also important to improve the legal framework against cyber attacks, to enhance international and institutional co-operation, and to raise public awareness and develop training and research programmes on cyber security.

The vulnerability of cyberspace can be reduced by the following measures: increasing the security of information systems; implementing data security standards; and providing specialised training to computer users. It is also necessary to endorse co-ordinated action at the national level and the delegation of cyber-security responsibilities to different public and private institutions.

The procurement of national cyber security should be based on the following principles and guidelines:

- cyber security action plans should be integrated into the routine processes of national security planning;
- cyber security should be pursued through the co-ordinated efforts of all concerned stakeholders, of public and private sectors as well as of civil society;
- effective co-operation between the public and private sectors should be advanced for the protection of critical information infrastructure;
- cyber security should be based on efficient information security, meaning that every information system owner should be aware of his or her responsibilities in the prudent use of information systems and should also take the necessary security measures to manage the identified risks;
- a general social awareness of threats in cyberspace and the state of readiness to meet them should be fostered; these are important prerequisites, since every member of the information society is responsible for the security of the network-based instruments or systems in his or her possession;
- Estonia should co-operate closely with international organisations and other countries to increase cyber security globally;
- proper attention should be paid to the protection of human rights, personal data and identity;
- the development and administration of IT solutions for the provision of public services should be brought into compliance with the Estonian IT Architecture and Interoperability Framework, including the information security framework. In addition, consideration should be given to the internal security

policies of individual public and private institutions and recommendations made therefrom for the continuity and recovery plans of their information systems.

1.2 Cyber Security Strategy and its relation to other national development plans

In order to reduce the vulnerability of Estonia's cyberspace and to better protect Estonian information systems, the Government has tasked the Ministry of Defence — in co-operation with the Ministry of Education and Research, the Ministry of Justice, the Ministry of Economic Affairs and Communications, the Ministry of Internal Affairs and the Ministry of Foreign Affairs — to develop a "Cyber Security Strategy for 2008–2013".[1] The inter-agency committee tasked with developing the Strategy included also information security experts from the Estonian private sector.

In developing the Cyber Security Strategy, the committee has taken into account national development plans that might also be relevant to information security and the information society, as well as plans relating to internal security and national defence. The principles of the current Strategy are in line with the Information Security Interoperability Framework that was adopted by the Ministry of Economic Affairs and Communications on 31st January 2007. This framework lays down the principles, means of co-ordination and regulatory framework for Estonia's information security, the principles for training in information security, and the activities necessary for the protection of the information infrastructure. The document was the first step towards establishing common standards for both state agencies and the private sector in order to protect the country's critical infrastructure and to ensure the country's information security.

A second document related to the Cyber Security Strategy is the "Estonian Information Society Strategy 2013", drafted by the Ministry of Economic Affairs and Communications in 2007. This document stresses both the importance that the whole population be integrated into the information society and also of improving the competitiveness of the Estonian IT sector. Furthermore, the Strategy is also related to the Ministry of Education and Research's "Knowledge-based Estonia: Estonian Research and Development Strategy 2007–2013", which designates as top priorities for research and development the country's IT competence and the development of e-solutions in various fields. However, the Cyber Security Strategy does not include national measures to target cyber crime; this is because the Ministry of Justice has already devised a criminal policy addressing the fight against cyber crime and also because the Ministry of Internal Affairs has prepared a draft of Estonia's internal security priorities until 2015. As a final note, measures to secure the information systems which pertain to national

[1] Order of the Government of the Republic No 497 on the development of the "Cyber Security Strategy 2008–2013" entered into force on 19th November 2007. The development of the Strategy should follow the Government of the Republic Regulation No. 302 of 13th December 2005 on the types of strategic development plans and the procedures for preparation, amendment, implementation, assessment and reporting thereof.

defence will be addressed in greater detail in a document entitled “National Defence Development Plan 2009–2018”, to be completed by the Ministry of Defence by the third quarter of 2008.

2 Threats in cyberspace

The asymmetrical threat posed by cyber attacks and the vulnerabilities of cyberspace have become a significant concern of security and must be addressed by all societies that employ information systems. The danger of cyber attacks lies in the attacker's ability to cause, from a distance and with minimum resources, considerable damage. This can be achieved through the short-term disruption of everyday activities, through significant economic damage or even through a catastrophe involving human casualties. Although cyber attacks have not so far resulted in casualties, this possibility cannot be ruled out in attacks against the critical information infrastructure. The use of cyberspace by terrorist organisations, organised criminals and state-sponsored actors already poses a serious global security threat.

Threats in cyberspace are difficult to define as it is hard to identify the source of attacks and the motives that drive them, or even to foresee the course of an attack as it unfolds. The identification of cyber threats is further complicated by the difficulty in defining the boundaries between national, international, public and private interests and actors. Because threats in cyberspace are global in nature and involve rapid technological developments, the struggle to meet them is ever-changing and increasingly complicated. It requires high-level training, an advanced legal framework, effective organisational co-operation and the allocation of considerable resources.

Threats in cyberspace can be classified in many ways. One of the most common is a threefold classification based on motivational factors: cyber crime, cyber terrorism and cyber warfare. However, as advanced technologies and attack methods make it difficult to define with any certitude or clarity the motives impulsing an attack, threats can also be classified on the basis of methods employed and on the extent of damage inflicted. The damage may be substantial owing to the high degree of interaction between computer networks and also the interdependence of services related to the information infrastructure. For instance, an attack against the server of one service provider might also cause disruption to the information systems of an unrelated agency, which may be part of the critical infrastructure, using the services of that very same provider. It should be stressed that any abuse of cyberspace for whatever purpose, from foolish or mischievous computer hacking to organised attacks against the critical infrastructure of a country, is harmful to society.

Cyber attacks against the critical infrastructure. Potentially, the most harmful cyber attacks are those against a nation’s critical infrastructure and its associated information systems. As the functioning of societies has grown to be highly dependent on information technology, their vulnerability has become a very serious security concern. Failures of or disruptions to critical information systems may impact extensively upon the normal functioning of society with unforeseen and potentially disastrous consequences. In order to ensure the security of a society’s critical infrastructure, both its IT and physical vulnerability need to be taken into consideration, as well as the fact that the interdependence of information systems further increases vulnerability. A breakdown in a vital information system may have severe implications for critical public services or other significant services provided by private companies, which are integral to the critical infrastructure.

For instance, a successful cyber attack against a public telecommunications network might leave customers without a telephone service. A cyber attack against the control systems of a chemical or natural gas facility might result in considerable physical damage and even the loss of human life. An infrastructure breakdown might also occur by way of a “domino” effect in which a failure in one component leads to the failure of others, again with serious potential consequences and disruptions to vital services. Large-scale information system breakdowns may result in considerable physical and financial damage and even human casualties. Among the most serious threat scenarios are likely to be those involving a combination of cyber attacks and physical attacks or cyber attacks launched during a major natural disaster.

Cyber crime. The majority of attacks against information systems and the data stored therein are crimes committed for financial gain. These crimes may manifest themselves in a disruption to a particular financial service or in a violation of the confidentiality, integrity or availability of financial data. Other forms of cyber crime include harassment, fraud, the distribution of illegal materials or the violation of intellectual property rights. To the criminal, the use of cyberspace for securing material profit might seem attractive because of the simplicity and remoteness with which such crimes can be committed. Other factors which lend to the appeal of cyber crime are: anonymity, deficiencies in international regulation of the use of cyberspace and the negligence of information system owners and end-users in ensuring the security of cyberspace.

The fight against cyber crime is complicated by wide differences in the type of attack, the extent of damage caused, and the motives involved. These motives can vary from the pursuit of economic gain to mere curiosity or hooliganism. In recent years, the efforts of cyber criminals have become more sophisticated, as these have acquired substantial resources, improved their organisational structures and implemented a clear division of labour between disparate criminal networks. Attacks via the Internet have become systematic and may often be aimed at specific high-value yet vulnerable targets. Moreover, the state of malware for cyber crime has become increasingly more sophisticated and the activities of criminal groups that organise cyber attacks are continuously expanding in scope.

3 Fields of activity supporting cyber security: Description and analysis

3.1 Estonia's information society and information infrastructure

In our modern, globalising world, economic success and a high quality of life can be achieved only through recognising the great importance of the efficient handling of knowledge and information to the proper functioning of our societies. The very term 'information society' denotes a setting in which human values of all kinds are created, maintained, manipulated and transmitted in a standardised digital form; it is a further feature of an 'information society' that all members have access to such information through a complex data exchange network.

The development of Estonia's information society, alongside other transitional reforms, has been an important driver in the country's spectacular economic growth: it has led to a high standard of living that we wish to maintain and will, if necessary, protect. In Estonia we are accustomed to the availability of e-services in a wide range of private and public fields. This is reflected in our people's exceptionally high confidence in the use of information systems. In 2007, 98% of all bank transactions were made using electronic channels; 82% of all tax declarations were submitted through the Internet; nearly every school in Estonia uses the e-learning environment; and the use of ID cards and digital signatures have become routine in both public and private sector administration. Furthermore, Estonia has been recognised internationally as a pioneer in e-government and e-election practices.

In 2007, 51% of all Estonian households leased high-speed broadband Internet services. Because there are several computer users in each household, the actual proportion of Internet home users is approximately 70% of the total population.[2] The growth of computer ownership and Internet use in Estonia has been facilitated by the Tiger Leap and VillageWay initiatives, launched in the early 1990s. These efforts led to an extensive network of public Internet services that reached all members of society regardless of geographical location. Thus, today every citizen has opportunities to employ e-services and to participate in all aspects of the modern economy and society.

The growing number of Internet services means that the dependence of our daily activities and lifestyle on the security and proper functioning of information technology increases incessantly. The Internet is an important element of Estonia's critical information infrastructure: it is used daily by the majority of Estonian enterprises and state agencies as well as by more than half the population. The key components of Estonia's critical information infrastructure, which constitute the IT infrastructure used by enterprises and agencies in the provision of e-

[2] A study by "TNS Emor" on the use of public e-services, October 2007.

services, include: Internet service providers, the name servers of the state, Estonia's root domain, network nodes, service servers and the firewalls of public and private organisations. The seamless operation of this infrastructure is vital to the daily functioning of the Estonian economy.

The main component of the Estonian public information system architecture is the secure data exchange layer, X-Road, which is based on the public Internet. Although X-Road uses the Internet, it meets all three objectives of information system security – availability, confidentiality and integrity. The number of X-Road's central components has been minimised and data exchanges between two information systems using X-Road are able to continue in case of its disruption. X-Road's infrastructure includes countermeasures against both temporary disruptions and attacks aimed at hindering the provision of services. But because new forms of attack and threats in cyberspace are constantly emerging, it is necessary to develop further X-Road's security measures.

The functioning of society depends greatly on the seamless operability of the information infrastructure that supports the critical infrastructure and on its resilience against attack. All sectors of critical importance – the water and food economies, health care, transport, energy systems, telecommunications and financial services[3] – depend on the operation of the information infrastructure. However, the information systems and services of many critical economic sectors do not rely solely on the Internet and are thus less vulnerable to threats originating there. For example, the voice communications networks of Estonia's major telephone and mobile communication companies are run separately from the Internet, as are most of the automated control systems of the critical infrastructure. Although the SCADA systems and voice communications networks of the telecommunications network are not linked to the public Internet, cyber attacks might still be able to threaten these in cases of negligence or deliberate action. In the case of companies engaged in the production and sales of electricity, the information systems and communications networks related to the control of power stations are entirely separate from the Internet and the stations and distribution network can be operated manually if necessary; nevertheless, negligence and security holes might also render these systems vulnerable.

The financial sector is one of the most dependent on e-services. Virtually all Estonian bank transactions are conducted via electronic channels and 62% of the Estonian population uses Internet banking. For this reason, cyber attacks could have very serious consequences if the e-services provided by banks were to become partly or completely unavailable to customers. If financial services were to be disrupted in this way for a considerable period of time, the damage and consequences for Estonia's economy would be significant indeed, lessening the security of society and producing a significant disruption to our daily lives.

[3] The fields of Estonia's critical infrastructure have been listed separately in Annex 1.

3.2 Information system security

The Information Security Interoperability Framework,[4] which has been in force since 2007, describes the key aspects of information security to be taken into consideration at both national and agency levels. The Framework is recommended to both the public and private sectors. Since 2008, Estonian state agencies have been obliged to follow information security standards which lay down security measures for the information systems and related information assets used in processing data in state and local government databases.

Large Estonian enterprises, including critical Internet service providers, telecommunications companies and banks, are highly competent in information security. The major financial and telecommunications companies have excellent information security procedures and use a range of solutions in addition to firewalls and anti-virus software to identify and combat cyber attacks.

We can conclude that Estonia's key information and communications systems that were targeted in the 2007 cyber attacks were defendable against attacks of that nature and scale, despite a few discrepancies in the systems' level of technical and information security. This was largely possible due to the efficient and close horizontal co-operation between information security specialists of both the public and private sectors. Nevertheless, there were still a number of systems which operations were disrupted during the attacks. In any case, it is important to protect our information and communications systems against larger scale attacks for which it will be necessary to improve both technological and organisational readiness to combat cyber threats. In advance of this objective, three measures can be identified.

First, stricter security requirements should be imposed on the companies whose systems are included in the Estonian critical infrastructure, without neglecting owners of other information systems. The existing three-level baseline security system, ISKE, which has been implemented in recent years, is compulsory for state agencies only. In addition, the private sector's information security safeguards should also be increased to provide high security for all information systems.

Second, the availability of the IT infrastructure, including the load capacity of public and private sector service servers, should be increased and the availability of services should be tested. As regards the identification and management of cyber attacks, the efficiency of network traffic monitoring and the ability to perform strategic and tactical analyses should also be improved.

Third, it is necessary to specify better the distribution of tasks and responsibilities between agencies in order to achieve a more efficient organisation of cyber security of the critical infrastructure and a better co-ordination of activities in combating cyber threats. To this end, proposals to amend the legal framework and increase the

[4] Information Security Interoperability Framework, Ministry of Economic Affairs and Communications, 31st January 2007, http://www.riso.ee/et/files/InfoturbeRaamistik.pdf (in Estonian only).

regulation of national cyber security should be developed. In addition, it is necessary to acknowledge cyber threats much more widely, and to improve interdepartmental coordination system related to the prevention and combating of cyber attacks on a national level. Since a large part of the critical infrastructure belongs to the private sector, co-operation between the public and private sectors is vital to reducing vulnerability of the critical infrastructure.

The regular updating of security measures is yet another important aspect of developing information security. The current and well known security objectives – confidentiality, availability and integrity of information – are no longer sufficient to ensuring cyber security. To secure the critical infrastructure, it is necessary also to address the severity of disturbances in its functioning, non-repudiation and authenticity of information sources. Further, ensuring cyber security also involves fields that have so far received little attention, such as physical protection measures to combat electronic attacks against information and communications systems.

Although Estonia can count on a large number of high-level experts in information security, Estonian enterprises, agencies and households have paid less attention to cyber threats and information security and in many senses the level of awareness is insufficient. As well as protecting the information infrastructure of critical economic sectors, an important element of ensuring cyber security in society relates to the information security awareness of small- and medium-sized enterprises, smaller state and local government agencies, educational institutions, home users and all other owners of network computers. The security awareness of Internet users is exceptionally low worldwide, including in Estonia. International research has shown that 97% of Internet users cannot distinguish between secure and insecure websites, meaning that their computers are at constant risk of infection with malware. 80% of the computers surveyed had programmes that were dangerous in terms of information security.[5] The low security awareness of Estonian computer users has been confirmed in a survey conducted by the Look@World Foundation, which revealed the following: while 82% of computers have installed and run anti-virus software, 59% of users do not know whether or how frequently it is updated; 50% of Internet users have installed a programme that is dangerous in terms of information security; and approximately one out of every three computers potentially hosts a malicious programme. At the same time, 70.1% of respondents believe themselves to be competent users and a large number consider their computer to be an unattractive target for cyber criminals.[6] Unfortunately, the survey's figures suggest just the opposite and many home PCs might very well be infected with malware or spyware.

The above surveys make clear that, along with technical countermeasures, greater attention needs to be paid to increasing the awareness of computer users. Raising the public's awareness of threats in cyberspace and of the necessary remedies is an important precondition for ensuring cyber security in Estonia and elsewhere. In addition

[5] "Adware and Spyware: Unraveling the Financial Web". McAfee White Paper, August 2006.

[6] "Eesti arvutikasutajate turbealased hoiakud", SA Vaata Maailma study paper (in Estonian only), 2005.

to know-how, it is essential to have the skills to prevent risks and manage breaches of information security. Work in this field is already underway in Estonia: in 2007, a public-private sector co-operation project called Data Protection 2009 was launched with the aim of developing Estonia into a highly secure information society.[7]

3.3 Training in the field of information security

Estonia has considerable competence in the information systems security measures necessary to combat serious cyber attacks. However, there is a growing need for qualified mid-level information security experts in both the public and private sectors. At the end of 2007, there were no public or private universities in Estonia providing in-depth training in information security at the Bachelor's, Master's or Doctoral levels. Practical expertise in information security has been built up in the private sector, particularly in the banks. In 2007, a survey of the institutions belonging to Estonia's critical infrastructure revealed that the biggest shortcoming in the field of information security is the shortage of qualified labour.

Training and in-house training in information security matters has emerged spontaneously in Estonia without any state support. The curricula of the University of Tartu and the Tallinn University of Technology include courses on cryptography as well as a few general courses on data security, but this is not sufficient to cover the entire field of information security. There is insufficient training and preparation in information security in ICT-related fields and there is a shortage of experienced teachers in the universities capable of providing basic education in this field. Some companies provide practical training courses, but up-to-date training is often to be found only abroad.

Scientific competence is an essential precondition in the provision of high-quality tertiary education. Information security-related research in Estonia is limited largely to the field of cryptography, in which Estonian researchers have produced world-class results and created innovative solutions such as secure public sector services to citizens through the X-Road data exchange layer, a well-functioning system of time stamps and the use of digital signatures. Developments and services in this subfield are, to some extent, also offered by IT companies. Estonia thus has a good starting base in developing the field of information security: the necessary research teams are already in place at the Cybernetics Institute of the Tallinn University of Technology and the University of Tartu, but their funding should be substantially increased.

It is important to stress that when it comes to cyber security, research and development cannot be separated from defence-related activities. Scientific research is important primarily because the implementation of protective measures for information systems is a rapidly advancing high-technology field. Efficient protection against malware is possible only if new versions of the threat are immediately identified and neutralised. The priority areas for development include intelligent protection software and the simulation of cyber attacks to ensure cyber security and provide training. This line of research is also supported by the NATO Centre of Excellence of

[7] Website of Computer Protection 2009: http://www.arvutikaitse.ee (in Estonian only).

Cooperative Cyber Defence, based in Estonia. In Fall 2008, a Master's course on cyber security will be launched in Estonian universities as a result of the joint efforts of the Tallinn Technical University, the Estonian National Defence College, and the Training and Development Centre in Communication and Information Systems of the Estonian Defence Forces.

3.4 Cyber security and the legal framework

3.4.1. International law

The use of cyberspace is under-regulated in the world, in terms of both national and international law. So far, no binding international law on cyber security exists which expresses the common will of countries and which can serve as a basis for shaping national laws. As this is a rapidly developing field of law, all the possible cyber threats have yet to be defined. New threats emerge constantly, as do the measures to combat them.

A few instruments of international law are already in place to deal with general issues such as the fight against terrorism and crime. But there are no general regulations for the prevention and combating cyber threats, nor even a set of common definitions of these threats. Several terms, such as *cyber war*, *cyber attack*, *cyber terrorism* or *critical information infrastructure*, have not been defined clearly. Everywhere they are used, but their precise and intended meaning will vary depending on the context.

As the Internet is a global network, it is quite clear that regulation within individual countries alone will prove ineffective in combating the cyber threat. Since every country can decide for itself whether to co-operate in criminal procedures dealing with cyber attacks, legal solutions for the protection of cyberspace serve their purpose only when implemented in individual countries or when co-operation with other countries on an *ad hoc* basis is possible. The legal framework for cyber security is thus related to international public law and Estonia can co-operate only with individual countries with which we have concluded corresponding legal aid agreements. Co-operation with other countries requires either bilateral agreements or additional international legal instruments. The Parliamentary Assembly and various committees of the Council of Europe are of the opinion that existing international legislation has already criminalised cyber terrorism and attacks against computer systems; so, it is claimed, there is no need for additional international legal instruments. European Union law establishes minimum guidelines through which member states can apply, through national law, additional sanctions against cyber attacks; some countries have already implemented such measures.

Two international legal instruments that cover crimes against computer systems should be highlighted. The first is the Council of Europe Convention on Cybercrime, which was submitted for member-state ratification in 2001 and which entered into force in 2004. One of its major shortcomings is the small number of countries that have so far ratified the Convention. (Estonia ratified in 2003.) By the beginning of 2008, 22 countries had ratified the Convention and another 22 countries had signed it, but it is significant that several member states of the Council of Europe had not yet signed, much less ratified it. However, the number of parties to the Convention is constantly

growing and ratification is under way in several countries; and, on this basis, several countries have already begun to amend their legislation in accordance with the Convention. It is an open convention, meaning that countries not members of the Council of Europe are also invited to ratify. For example, the United States, Canada, Japan and the Republic of South Africa have acceded. In this regard, the Council of Europe is making serious efforts to introduce the Convention to as many non-member countries as possible with the aim of increasing its global reach.

EU legal framework. The second legal instrument which regulates cyber crime-related issues at the EU level is the Council Framework Decision 222/2005/JHA on attacks against information systems. The substantive law within the Framework Decision basically embraces the provisions laid down in the Council of Europe Convention. One shortcoming of the Framework Decision is its applicability to EU member states alone, whereas cyber crime is a far more extensive cross-border phenomenon likely to cross the EU's external frontiers. A further deficiency, which applies also to Council of Europe Convention, is that it treats attacks against information systems as a criminal offence against private and public property, thereby disregarding the national security dimension of the threat. There is the further shortcoming: different computer systems are treated in a similar way without any differentiation between ordinary computer systems and critical infrastructure information systems; nor is there a distinction in scope between small- and large-scale attacks.

EU law contains various instruments related to the development of information society, which form a platform from which to develop legislation in that field. It should be noted that EU directives do not aim specifically at ensuring cyber security, but rather have the interest of the internal market in mind. EU directives cover the following fields of law:

- protection of personal data (95/46/EC and 2002/58/EC);
- electronic communications (2002/58/EC);
- retention of data (2006/24/EC);
- re-use of public sector information (2003/98/EC);
- information society services (2000/31/EC).

3.4.2 National legal framework

In order to develop a national legal framework for cyber security, the identification of areas which are either not covered or are insufficiently covered by legislation was begun in 2007. The analysis showed that Estonia's current legal policy for IT is decentralised and, in fact, partly contradictory. For instance, Estonia has adopted a liberal policy concerning the use of e-services and the information society generally; at the same time, the policy for personal data protection is rather conservative and the regulation of information society services complies only with the EU's minimum requirements. Moreover, different regulations have been adopted under different contexts and in different stages of development. Further, the law of information has not yet been codified.

The findings of the legal analysis alert us to the need of amending and harmonising the following elements of national law:

Penal Code. The elements necessary to constitute an offence as laid down in the Penal Code are insufficient to the needs of cyber security, nor are the sanctions and enforcement procedures therein adequate. To rectify this gap, the necessary elements for an offence were expanded in order to avoid situations where some modes of cyber attacks would not have been covered by law at all or where sanctions would prove insufficient to prevent or prosecute the crime. Another important amendment was made in order to cover acts of terrorism where a cyber crime was to be committed for terrorist purposes.

Electronic Communications Act. The Electronic Communications Act sets out the requirements for publicly available electronic communications networks and communications services. The Act lays down general terms and conditions for the provision of electronic communications services and specifies the minimum obligations for market participants, including data security and contracts with end-users. The Act thus serves as the basis for defining the general requirements of an information infrastructure.

In order to ensure that the obligations of the state and communications service providers as concerns national security are specified, it is necessary that the Act lay down the obligations of communications service providers in protecting the critical information infrastructure. Further, as it is not practical to compare logs of data collected by the communications service providers because the Act does not stipulate the basis and procedures for logging, obligations in this regard also need to be specified, including: the identification of those falling under such an obligation, the extent and time limits of their obligation and issues relating to the cost of fulfilling the obligation. As the security of networks largely depends on end-users' awareness of protecting their computers and their capability to do so, the obligations for such users also need to be specified. Finally, because name servers are part of the critical information infrastructure, their regulation should also be improved.

Personal Data Protection Act. It is essential for the purposes of cyber security to establish a clear legal basis for processing any kind of personal data. The Personal Data Protection Act aims to fulfil this function and applies in all relevant circumstances. The Act deals with operations relating to individual citizens. It also provides general organisational, technical and physical security measures to ensure the availability, integrity and confidentiality of data.

From the standpoint of cyber security, exceptions to the Personal Data Protection Act should be allowed when data are processed for the sake of national security. Such exceptions are allowed by EU Directive 95/46/EC on the protection of personal data and by the Council of Europe Convention ETS 108.

Such exceptions to the Personal Data Protection Act should be considered for issues relating to the security and protection of the critical information infrastructure. The question of exceptions in the interests of national security might be treated either by amending the Act itself or through a separate regulation addressing the protection of the critical infrastructure.

The extent of such exceptions should be determined together with the Ministry of Justice and the Data Protection Inspectorate, since the Directive allows exceptions only in specific circumstances.[8]

In addition, it is necessary to elaborate the principles for processing personal data for preventive and reactive purposes as they pertain to law enforcement authorities. Consideration should be given to introducing an obligation on critical infrastructure companies similar to the obligation to register for the processing of sensitive personal data. This would render security measures and their implementation more transparent and would also help to unify the various levels of cyber defence. In order to speed up the exchange of operational information, procedures for the exchange and publication of information should also be specified.

Public Information Act. As stipulated in the Constitution, the Public Information Act enables the state to exercise authority over the dissemination of high-quality public information. The Act regulates the basis and procedures for the accessing of public information, including requirements pertaining to the websites of information holders. This Act also defines the role of the Internet in the communication between state and citizen. The implementation of the Act might become difficult in the event of a cyber attack; for instance, the Act does not include a basis for restricting access to websites or for non-compliance with information requests. For this reason, the Act is due for comprehensive revision so that it covers scenarios when the state information infrastructure is only partly operational.

Revisions to the Act should address the legal basis for obtaining data from databases and the cross-use of data for preventive and reactive purposes, which would allow for the exchange and analysis of operative information concerning attacks. It would also be helpful to establish a basis for restricting access (entirely or partly) to state and local-government websites under certain circumstances. Moreover, an audit scheme should be established for critical infrastructure agencies and companies which would monitor compliance with the Personal Data Protection Act, the Public Information Act, the Information Society Services Act and the Electronic Communications Act.

Information Society Services Act. The Information Society Services Act limits the liability of Internet service providers for the content of their service, spam related issues and general requirements for the provision of information society services. These requirements provide the opportunity to contact website maintainers when incidents occur. The main problem with this Act is its concision and that it, in general, it does not relate to Estonia's legal framework. For example, in the case of spam only the information society service provider can be punished; supervision of compliance with the Act is decentralised; and sanctions are not sufficiently dissuasive.

[8] Member States may adopt legislation to limit the extent of rights and obligations laid down in Articles 6(1), 10, 11(1), 12 and 21, provided that such limitations are necessary to ensure:
(a) national security; (b) national defence; (c) law and order; (d) prevention, investigation, identification and prosecution of crimes or violations of professional ethics of regulated professions; (e) essential economic or financial interests of Member States or the European Union; (f) monitoring, control and regulatory functions related to exercising official authority, even if temporary, in the cases set out in clauses (c), (d) and (d); (g) protection of data subjects or the rights and freedoms of other persons.

Neither is there a clear legal basis for regulating the transmission of data by Internet service providers or for the termination of Internet connections in cases where computers have been compromised.

As Internet service providers have the most direct perspective on Internet activity, it would be useful to impose on them a more substantial obligation for co-operation and, in the case of critical infrastructure, an obligation of control as well. For this purposes it would be necessary to extend the regulations of the Act beyond the minimum requirements set out in EU directive 2000/31.

3.5 International co-operation

The global and diffuse nature of cyberspace and of cyber threats means that the potential consequences of attack reach across state borders. It also means, therefore, that ensuring cyber security necessitates close and extensive international co-operation. A global cyber culture — a key component of effective cyber security — can emerge only through a comprehensive co-operative effort involving a wide range of countries, international organisations, private companies and their associations, computer experts, the co-operation networks of law enforcement authorities, academic institutions, non-governmental organisations, etc. Frequent cyber attacks in different countries have put cyber security high on the agenda of various international organisations and countries. Many countries have established new institutions to monitor the vulnerability of cyberspace, analyse threats and improve the security of information technology. International co-operation within multilateral frameworks is becoming the prime driving force of efforts to ensure the security of cyberspace.

The issue of cyber security is from the standpoint of the international community a novel concern. Although advanced industrial countries are already highly aware of cyber security issues and have been taking measures for some time to protect their information systems, it is difficult to achieve international agreement in this field at the *global* level. The level of application of IT solutions varies significantly between countries and the rapid development of IT and pressure from national interest groups further complicate the adoption of international norms and regulations. This means that, in order to develop legal instruments to safeguard cyber security, countries must hold extensive consultations, thus rendering the process time-consuming and complex. At the same time, because cyber security has an eminently global dimension, efficient international legal instruments, extensive co-operation networks, and multi-lateral as well as bilateral co-operation are of the essence in combating cyber crime and securing cyber defence and information security.

Currently, the only international legal instrument directly aimed at preventing and solving cyber crimes is the Council of Europe Convention on Cybercrime. As mentioned, the foremost shortcoming of this Convention is the small number of participating countries, meaning that there is only limited international co-operation in the field of cyber crime. Moreover, the Convention treats attacks against information systems as unorganised criminal offences against property. However, Estonia's experience has shown that computers and networks may be used to prevent the state from functioning and also for propaganda purposes, either in the form of a spontaneous public initiative or as an organised action.

Besides developing an international legal framework, it is also necessary to develop a draft model act on cyber security that is applicable across countries. It should not be difficult to assemble such a document, drawing together and adapting countries' best practices, without specific legislative clauses. At the same time, it should be noted that ensuring cyber security is essentially a state function pertaining to the general maintenance of law and order and, further, relates directly to national defence.

Owing to Estonia's unique experience in dealing with cyber attacks in the spring of 2007 and subsequent policy initiatives, the international community expects a major contribution from us — and perhaps even a leadership role. In this regard, it is necessary first to analyse the potential contribution to international initiatives based on our capabilities and resources. Other countries have expressed a strong interest in Estonia's experiences given its higher-than-average IT penetration. From our standpoint, it is important to raise global awareness of cyber security and to support international co-operative, preventive and protective measures.

Estonia has assumed a leading role in introducing cyber security-related initiatives to international organisations and through bilateral co-operation. Estonia was a founding player in the development of NATO's cyber defence policy, adopted in 2008. Estonia has also been involved in consultations with the Council of Europe on combating cyber crime and with EU institutions on elaborating common principles for defending the critical information infrastructure. Overall, it has been a significant player in and stressing the importance of cyber security in strategic documents dealing with European security. In 2008, Estonia holds the presidency of the Organisation for Security and Co-operation in Europe (OSCE) and intends to raise the issue of cyber security at the OSCE security forum. Estonia has also taken an active part in the cyber security and IT initiatives of the United Nations and related agencies. In 2009, Estonia will join the Organisation for Economic Co-operation and Development (OECD) which will expand the opportunities for exchanging experiences with other OECD countries.

More extensive participation in international organisations is vital to ensuring recognition of the problems of cyber security generally and to drawing the attention specifically of policy-makers in other countries. Many countries still believe that cyber security is strictly a matter of technology that does not require any political intervention whatsoever. However, political attention is important in initiating efforts at drafting international norms and regulations necessary to ensure cyber security and to facilitate co-operation between countries.

The increase in crimes committed over the web has accompanied the overall development of information technology and has now evolved into the most widespread problem of international cyber security. As there are no physical barriers in the virtual environment and as time is of the essence in solving IT crimes, timely co-operation and exchange of operational information between law enforcement authorities is crucial. Law enforcement authorities should thus engage in close co-operation with Interpol, Europol and other intergovernmental organisations and professional networks engaged in the fight against cyber crime.

In addition to multilateral and bilateral co-operation, more attention should be paid to IT companies, associations representing multinational firms and other similar bodies dealing with the security of information systems. Co-

operation between the public and private sectors in Estonia is a good example of best practice which should be shared with other countries. Co-operation networks have a central role in ensuring the security of global cyberspace, as they allow for the exchange of expertise on the basis of mutual trust.

It is also necessary to encourage Estonia's participation in international research and development networks, to focus attention on enhancing the IT and information security competence of Estonian universities and to enhance co-operation with internationally-recognised research centres and development institutes. The contacts between Estonian universities and international academic networks will play an important role in the development of IT and information security studies and research, and will have a direct impact on ensuring national security through the training of specialists.

Estonia considers active participation in international organisations vital for increasing global cyber security.

UNITED NATIONS

It is necessary to raise the awareness of all United Nations members regarding the nature and importance of cyber security as an issue that affects not only technologically advanced countries but rather the entire world. Cyber crimes and cyber attacks should therefore be morally condemned at the global level. Resolutions on cyber security should be considered a priority. Countries should develop respective positions and seek increased international support for these.

In the UN, issues of cyber security are addressed by a high-level expert group of the Internet Governance Forum (IGF) and the International Telecommunication Union (ITU). Since 2006, Estonia has had an e-government senior expert working at the headquarters of the United Nations Institute for Training and Research (UNITAR) in Geneva.

EUROPEAN UNION

Ensuring cyber security and combating cyber crime concerns all EU member states. The common judicial area and institutions of the EU and the deep co-operation between member states constitute a foundation for the successful prevention of cyber crime and the management of its consequences. The EU first began to tackle cyber crime in 1999: the security of high technology was mentioned in the EU's Tampere programme and the Council of the European Union adopted a common position on the Council of Europe Convention on Cybercrime. The key legislation includes:

- Council Decision to combat child pornography on the Internet (2000);
- Commission Communication "Creating a Safer Information Society by Improving the Security of Information Systems and Combating Computer-related Crime" (2001);
- Council Framework Decision on attacks against information systems (2005).

In May 2007, the European Commission published a communiqué entitled “Towards a General Policy on the Fight against Cyber Crime” and on 8th-9th November 2007 the Council of Justice and Home Affairs adopted conclusions on this issue. We consider it important to develop a common, comprehensive and clear policy on the fight against cyber crime, covering as many relevant fields as possible. The policy should distinguish clearly between the national security dimension and the economic environment on the one hand, and the rights and security of individuals on the other.

In related areas, we consider it necessary to carry out a supplementary analysis of the EU’s legal framework in terms both of the security of cyberspace and the fight against cyber crime. More precisely, it is necessary to appraise the impact of cyber crime on the competitiveness of the EU, the adequacy of the EU’s legal basis for addressing new threats and the EU regulations that address cyber attacks against the interests of a country as a whole.

Co-operation between the public and private sectors is vital to cyber security in the EU, as the continuing development of IT solutions involves various private companies that provide strategic services and infrastructure to the state. The European Network and Information Security Agency (ENISA) provides support to EU member states, institutions and entrepreneurs in the prevention and management of breaches in information security. There is also a common EU research network relating to cyber security — the European Programme for Critical Infrastructure Protection (EPCIP) — which supports the protection of EU member states' critical information infrastructure, co-operation between member states and research activities.

NATO

NATO has developed a Cyber Defence Policy and a Cyber Defence Concept. In elaborating cyber defence principles, Alliance members have proceeded from the principles of Allied solidarity and recognition of national sovereignty. In other words, the common goal is that all NATO allies will be ready and able to support each other in the event of a cyber attack and, in advance of this aim, will develop cyber defence capabilities within their own countries. In this context, Estonia is interested in the establishment of closer multi- and bilateral co-operation networks under NATO's umbrella, and is ready to establish contacts with NATO's partner countries should NATO decide to proceed in this direction.

COUNCIL OF EUROPE

The Council of Europe Convention on Cybercrime came into force in 2004. The Convention includes definitions of various forms of cyber crime and lays the foundation for judicial co-operation between Convention countries. After joining the Convention, countries are obliged to align national legislation with its provisions. The Convention does not provide for any special control mechanisms. It is open for accession to countries that are not members of the Council of Europe.

The Council of Europe also runs a separate initiative, the Implementation of the Project on Cybercrime, designed to promote and encourage accession to the Convention. The Project aims to disseminate the Convention and its underlying normative basis to other countries and facilitate its adoption by non-members.

Considering the general opinion of the member states of the Council of Europe, current efforts should focus on expanding the number of parties to the Convention on Cybercrime as this is the main international legal instrument dealing with the issue. It is unlikely that countries will support the creation of new legal acts or additional protocols until this has been achieved. However, this does not preclude the possibility that Estonia might at some point launch a concrete initiative to amend the existing legal framework should further analysis indicate the need to do so.

Regardless of whether new judicial initiatives are launched or whether, instead, security-related activities remain within existing legal frameworks, it is vital that countries ensure smooth international co-operation and information exchange on legal matters and develop a common legal basis to facilitate political consultations and the exchange of information at all levels in the case of large-scale cyber attacks.

ORGANISATION FOR SECURITY AND CO-OPERATION IN EUROPE

The Organisation for Security and Co-operation in Europe (OSCE) associates cyber security mainly with the threat of terrorism. Estonia intends to raise the issue of cyber security more generally in the OSCE Security Committee and the Parliamentary Assembly when we hold the OSCE presidency (from spring to autumn 2008).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)

In the Organisation for Economic Co-operation and Development (OECD), the issue of cyber security is the responsibility of the Committee for Information, the Computer and Communications Policy and its working groups, including the Working Party on Information Security and Privacy. The Committee has adopted several recommendations, including the Recommendation Concerning Guidelines for the Security of Information Systems and Networks (2002) and the Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007).

Estonia began OECD accession proceedings in 2007 , a process that will take approximately two years to complete. Until then, it is still possible for Estonia to participate in OECD matters to a limited extent.

PROFESSIONAL ORGANISATIONS AND INTERNATIONAL CO-OPERATION NETWORKS

Securing cyberspace largely relies on the exchange of information which, at the international level, is best achieved through co-operation networks. Such networks bolster the ability to take immediate actions in ensuring cyber security and combating cyber crime. The professional co-operation networks of the public and private sectors allow for the exchange of information on innovative IT solutions, best practice and other expert information. The exchange of expert information on cyber security requires close co-operation between the

networks which deal with international data security, cyber defence and law enforcement. The most significant of these include the international network of national CERTs, the network of government CERTs (GovCERT), Interpol and Europol for co-operation in law enforcement, and organisations dealing with Critical Information Infrastructure Protection.

4. Enhancing cyber security in Estonia: Goals and measures

In order to reduce the vulnerability of Estonia's cyberspace, the following strategic goals have been identified:

- establishment of a multilevel system of security measures;
- expanding Estonia’s expertise in and awareness of information security;
- adopting an appropriate regulatory framework to support the secure and extensive use of information systems;
- consolidating Estonia’s position as one of the leading countries in international co-operative efforts to ensure cyber security.

Specific lines of action have been identified in advance of each goal above.

4.1. Development and implementation of a system of security measures

Estonia will develop a system of security measures in order to ensure national cyber security. The implementation of a system of cyber security measures would provide for action plans for responding to cyber attacks and for the rapid recovery of damaged information systems. The system would also specify the course of actions to be taken in the event of cyber attacks that jeopardise national cyber security, and the countermeasures to be taken immediately at both national and international levels.

The activities associated with this system concern organisational co-operation, physical security and technical measures. The technical measures must address all the systems and platforms used for the provision of critical information infrastructure services. Such security measures are indispensable: the increasing complexity of ensuring cyber security must not be allowed to diminish the role of information and communications technology as driving forces behind Estonia’s future economic growth.

State agencies ensure information security through the three-level baseline security system, ISKE. In order to protect the critical information infrastructure, a multilevel system of cyber security measures will be employed.

To this end, the focus will be on:

- Protection of the Critical Information Infrastructure (CII);
- Development and Implementation of a System of Security Measures;
- Strengthening of Organisational Co-operation.

Measure 1: Protection of the Critical Information Infrastructure (CII)

The Measure for the Protection of the Critical Information Infrastructure will include the following activities:

- **Definition of critical information infrastructure services**. The aim is to identify the information infrastructure services essential for the functioning of the critical infrastructure.
- **Determining the interdependence of the critical infrastructure and the critical information infrastructure**. The aim is to determine the degree of dependence of critical infrastructure services on critical information infrastructure services.
- **Assessment of critical information infrastructure services**. The aim is to develop a common methodology for assessing the vulnerability of critical infrastructure information systems and their support services.
- **Preparation of cyber security risk assessments**. The aim is to gather and process information about the current situation in cyberspace so as to plan preventive actions and identify the countermeasures necessary to deal with attacks on national cyber security. Periodic risk assessments prepared on the basis of critical infrastructure risk analyses will be integrated into the ongoing process of ensuring national security.

Measure 2: Development and Implementation of a System of Security Measures

The development and implementation of a system of security measures will include the following activities:

- **Development, revision and modification of security measures**. The aims are:
    - to determine additional security solutions in order to ensure the business continuity of information processes and the recovery of information systems, and related measures (in addition to those arising from data security requirements);
    - to determine the minimum required functionality of the information infrastructure and to ensure this level of operability in a crisis situation;
    - to determine the countermeasures permitted during an emergency situation in which the critical infrastructure is under attack;
    - to develop economically feasible and optimal methods for ensuring information security and to determine the activities necessary to implement such methods;
    - to develop testing methods for security solutions and to determine the activities necessary to apply these;
    - to improve the identification and monitoring systems of the EMI interference at both the critical infrastructure and state levels.

- **Implementation of security measures in the public and private sectors**. The aim is to apply up-to-date and efficient security measures. The following are necessary:
    - strengthening the Internet infrastructure;
    - increasing the security of control systems (SCADA[9] control systems);

[9] SCADA (Supervisory Control and Data Acquisition) – automated control systems used e.g., in the industrial and energy sectors.

- testing the security of CII server rooms against RF EMI interference;
- testing the security of CII information processing equipment (servers, business desktops, communication devices, etc.) against RF EMI interference.

- **Organisation of supervision of the implementation of security measures**. Every information system owner must implement the necessary security measures. Supervision of the implementation of security measures for the critical infrastructure will be conducted by the Ministry of Internal Affairs and the Ministry of Economic Affairs and Communications in co-operation with other ministries responsible for different sectors of the critical infrastructure.

Measure 3: Strengthening of Organisational Co-operation

The Measure for Strengthening Organisational Co-operation will include the following activities:

- setting up a Cyber Security Council of the Security Committee of the Government of the Republic with the responsibility to implement the goals of the Cyber Security Strategy;
- determining the duties of the structural unit within the Ministry of Economic Affairs and Communications responsible for the security of state information systems, and performing these duties to provide risk analyses at different levels (i.e., state as well as critical infrastructure agencies and companies);
- improving the methods of risk assessment developed by the ministries pursuant to the Emergency Preparedness Act and applying these methods to cyber security;
- setting up an expert working group with the responsibility of identifying information security shortcomings, assessing the necessary resources for updating security measures and exchanging operative information. The expert working group will provide professional advice on information security to the Cyber Security Council of the Security Committee of the Government of the Republic;
- increasing the capability for strategic analysis of cyber security incidents;
- developing proposals for amendments to national and international legislation;
- co-ordinating the raising of awareness in cyber security and designating a specific agency with this responsibility.

4.2. Increasing competence in information security

In order to achieve the necessary competence in cyber security, it is necessary to accomplish the following objectives in training and research:

- providing high quality and accessible information security-related training in order to achieve sufficient competence in both the public and private sectors, to establish common requirements for the competence of IT staff in information security, and to set up an appropriate system of in-service training and evaluation;

- intensifying research and development in cyber security so as to ensure national defence, to enhance international research co-operation and to ensure competence in providing high-level training.

To this end, the focus will be on:

- organising training in cyber security;
- enhancing research and development resources.

Measure 1: Organisation of Training in Cyber Security

The organisation of training in cyber security will include the following activities:

- organisation of studies in cyber defence and information security at all levels of education;
- organisation of in-service training in cyber defence and information security;
- establishment of requirements for competence in information security and cyber defence for both public and private sector staffs, and the organisation of appropriate evaluation processes;
- improvement of the preparedness for crisis situations both in the public and private sectors. The aim is to prepare different stakeholders in the handling of crisis situations. To this end, it will be necessary:
    - to integrate operational action plans for ensuring cyber security into the national crisis management system;
    - to organise preventive actions and crisis management at the government level;
    - to organise training exercises on handling crisis situations based on risk assessments, and to participate in international training exercises.

Measure 2: Enhancing Research and Development

The enhancement of research and development will include the following activities:

- support for research and development activities aimed at increasing competence in cyber security;
- establishment of closer ties with the international research community in the scientific fields which underpin cyber security;
- development of the NATO Centre of Excellence for Cooperative Cyber Defence in Estonia.

4.3. Development of a legal framework for cyber security

The development of legislation to ensure cyber security is aimed at creating a robust legal framework for combating cyber crime, for ensuring the cyber security of the critical infrastructure and for establishing common information security standards applicable to all computer users.

The main goals for the development of a legal framework are as follows:

- development of legal definitions for cyber security and cyber crime;

- development and implementation of legislation to ensure cyber security, including the introduction of compulsory security measures and standards in critical infrastructure companies and the establishment of minimum information security requirements for all information systems;
- improvement of existing legislation with a view to ensuring cyber security;
- drafting of new legislation to cover new areas or threats;
- launching of initiatives in international law-making.

4.4. Development of international co-operation

The objectives of this Strategy in the area of international co-operation are threefold: (1) to share the knowledge Estonia has gained from its experience and high level of IT use in its society ; (2) to raise global awareness of cyber security and ; and (3) to support co-operative prevention and protection measures. In terms of developing international co-operation on cyber security, the Strategy aims:

- to achieve worldwide moral condemnation of cyber attacks that affect the functioning of society and impinge directly on people's wellbeing, while recognising that the fight against cyber threats should not serve as a pretext for undermining human rights and democratic freedoms;
- to promote accession to the conventions on cyber crime and cyber attacks, and expand public awareness of such conventions;
- to participate in the development and implementation of international cyber security policies and the shaping of a global cyber-culture;
- to develop co-operation networks in the field of cyber security and to improve the functioning of such networks.

Activities for strengthening international co-operation in the field of cyber security:

- introducing the problems related to cyber security and defence, and ensuring these are addressed as *global* issues;
- encouraging ratification of the Council of Europe's Convention on Cybercrime and promoting the Convention throughout the globe;
- participating in professional conferences, seminars and forums in order to facilitate the regular discussion of cyber security issues;

- supporting the activities of international corporations, associations, research and development institutes and non-governmental organisations engaged in cyber security;
- promoting best practices in the field of cyber security at the international level;
- appointing representatives from Estonia to the expert groups of international organisations engaged in cyber security.

Participation in the work of international organisations:

United Nations

Active participation will be sought in:

- the work of the Information Society World Summit and the Internet Governance Forum;
- the high-level expert group on cyber security of the International Telecommunication Union;
- the Cyber Security Forum of the International Telecommunication Union.

Council of Europe

- Encouraging all countries, both members and non-members, to sign and ratify the Council of Europe Convention on Cybercrime;
- promoting the Convention, which is currently the only legally binding international instrument, especially among European countries;
- supporting the “Implementation of the Project on Cybercrime”, which aims to introduce the Convention and its ideology worldwide and provide assistance in accession to it;
- analysing the opportunities and needs for creating additional protocols to the Convention;
- gaining Estonian representation in the Parliamentary Assembly of the Council of Europe in order to engage in and promote cyber security.

European Union

- Efforts to strengthen operational co-operation between the law enforcement and judicial authorities of EU member states, and facilitate co-operation between the cyber crime units of member states and other competent authorities and experts;

- active participation in the fight against cyber crime, including the development of common EU positions in the international arena;

- co-operation with other member states in the investigation of co-ordinated and extensive attacks against their information infrastructures with a view to preventing such attacks and neutralising their impact. This entails, among other things, mutual co-ordination and the exchange of information;

- initiation, development and promotion of international projects in line with the Commission's policies on cyber security, and active participation in research and development activities in the area of cyber security within the framework of the European Defence Agency.

OSCE

- Raising of cyber security issues in the OSCE's security structures;

- introduction of cyber security issues at the OSCE Parliamentary Assembly and organisation of seminars and conferences within the framework of the OSCE.

NATO

- Implementation of the NATO cyber defence policy;

- establishment of the NATO Centre of Excellence for Cooperative Cyber Defence in Estonia and accreditation of the Centre by NATO;

- enhancement of scientific co-operation in the area of cyber security and defence with the NATO Research and Technology Organisation and the NATO Consultation, Command and Control Organisation;

- creation of a multi- and bilateral co-operation and information network for the NATO member states and, if necessary, a co-operation and information network for the members and partners of NATO.

OECD

- prior to OECD accession : active participation in the work of its Committee for Information, Computer and Communications Policy and its sub-working groups, and the drawing of attention to cyber security and defence issues;

- following OECD accession : initiation of discussions on cyber security and defence and the introduction of appropriate recommendations as necessary.

4.5. Raising awareness of cyber security

The goals include:

- increasing awareness of information security and the risks stemming from the cyber environment among all computer users;
- spreading awareness of secure computer use and the basic principles of information security among different target groups in society;
- promoting Estonia's positions on cyber security at both the national and international levels, and supporting the efficient functioning of co-operation networks.

In advance of these ends, the following additional tasks are necessary:

- organising information security awareness-raising for the wider public in co-operation with the private sector, with a particular focus on home users, small and medium-sized enterprises, employees of local governments and state agencies, teachers and students;
- conducting targeted media campaigns on cyber security and computer protection, and public advertising programmes;
- supporting to the objectives and activities of the public and private sector co-operation project "Computer Protection 2009";
- raising of the awareness of cyber culture in every Estonian agency and company by training senior executives and officials in the promotion of secure computer and Internet use in all fields;
- introducing Estonia's positions on and experience in cyber security at the international level.

5. Implementation of the Strategy

The Cyber Security Strategy Committee — led by the Ministry of Defence in co-operation with the Ministry of Education and Research, the Ministry of Justice, the Ministry of Economic Affairs and Communications, the Ministry of Internal Affairs and the Ministry of Foreign Affairs — has submitted "Estonia's Cyber Security Strategy for 2008–2013" to the Government of the Republic. The Strategy was adopted by the Government on 8 May 2008. In order to pursue the Strategy, an implementation plan will be developed, which will relate to the specific development plans of the relevant government agencies. The Implementation Plan for 2008–2010 will be submitted to the Government for approval within three months of the adoption of the Strategy.

The Implementation Plan will be developed on the basis of proposals from different state agencies and working groups which have been set up for development of the Strategy. Attention will be given to the concrete actions and funds needed to achieve the objectives of the Strategy in its various fields of competence. Implementation Plans will be developed for two periods: 2008–2010 and 2011–2013.

The responsibility for developing the “Implementation Plan for Cyber Security Strategy 2008–2010” lies with the Cyber Security Strategy Committee, led by the Ministry of Defence in co-operation with the Ministry of Education and Research, the Ministry of Justice, the Ministry of Economic Affairs and Communications, the Ministry of Internal Affairs, the Ministry of Foreign Affairs and private sector representatives.

The implementation and overall efficiency of the Strategy in meeting its stated objectives will be assessed by the Cyber Security Council of the Security Committee of the Government of the Republic. This effort will bring together representatives and experts from different ministries and other actors involved in bolstering national cyber security. The Council will monitor the success of the Strategy by submitting annual reports to the Government, which will detail the progress of implementation and the realisation of the objectives set out in the Implementation Plans. The Implementation Plan will also define the membership, meeting procedures and tasks of the Council.

ANNEX 1. Fields of Estonia's critical infrastructure

- Energy facilities and networks: electricity, oil and gas storage facilities and refineries, transmission and distribution systems.
- Communications and information technology: telecommunications, transmission and notification systems, software, hardware and networks, including the infrastructure of the Internet.
- Finance: banking, securities and investment.
- Health care: hospitals, health care facilities, laboratories and medicines, search, rescue and ambulance services.
- Food: safety, means of production, wholesale and food industry.
- Water: water reservoirs, water treatment plants and water networks.
- Transport: airports, ports, inter-modal transport facilities, rail and mass transit networks, traffic control systems.
- Production, storage and transport of dangerous goods: chemical, biological, radiological and other hazardous materials.
- State agencies: critical services, facilities, information networks; information systems ensuring national security and defence, resources, databases and court registers with legal effect, and national cultural assets.