Estonia Country Report

enisa
European Network and Information Security Agency

www.enisa.europa.eu

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on the Country Reports, please use the following details: Mr. Jeremy Beale, ENISA Head of Unit - Stakeholder Relations, Jeremy.Beale@enisa.europa.eu

Internet: http://www.enisa.europa.eu/

Acknowledgments:

ENISA would like to express its gratitude to the National Liaison Officers that provided input to the individual country reports. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity.

ENISA would also like to recognise the contribution of the Deloitte team members that prepared the **Estonia Country Report** on behalf of ENISA: Dan Cimpean, Johan Meire and Jan D'Herdt.

Table of Contents

Estonia

The structure of the individual country reports

The individual country reports (i.e. country-specific) present the information by following a structure that is complementary to ENISA's "Who-is-who" publication and is intended to provide additional value-added to the reader:

- *NIS national strategy, regulatory framework and key policy measures*
- *Overview of the NIS governance model at country level*
    - *Key stakeholders, their mandate, role and responsibilities, and an overview of their substantial activities in the area of NIS:*
        - *National authorities*
        - *CERTs*
        - *Industry organisations*
        - *Academic organisations*
        - *Other organisations active in NIS*
    - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
- *Country specific NIS facts, trends, good practices and inspiring cases.*

For more details on the general country information, we suggest the reader to consult the web site: http://europa.eu/abc/european_countries/index_en.htm

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

Estonia is one of the most rapidly developing information societies in Central and Eastern Europe. Estonia attracted a lot of attention in 2005 when it carried out its first round of internet-based voting in the local government elections of 2005 (in 2007, Estonia even became the first country in the world to feature e-voting in parliamentary elections). These elections were the results of constant and ambitious efforts to foster the information society. The uninterrupted functioning of information and communication infrastructures (ICTs) provides the basis for such a highly developed information society.

Every year the RISO, Department of State Information Systems, publishes a report or yearbook about the recent IT in public administration developments. This report contains information such as the NIS-IT Strategy and regulations but it also covers topics such as cyber security and eID. The reports are national publications and available on the website of RISO[1].

Estonian Cyber Security Strategy[2]

The Cyber Security Strategy Committee – led by the Ministry of Defence in cooperation 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 – submitted "Estonia's Cyber Security Strategy for 2008–2013" to the Government of the Republic. This strategy was adopted by the government in May 2008.

The Estonian Cybersecurity Strategy lays out the priorities and activities aimed at improving the security of country's cyberspace. The Cybersecurity Strategy concentrates on the following areas: the responsibilities of state and private organizations, vulnerability assessments of critical national information infrastructure, the response system, domestic and international legal instruments, international cooperation, and training and awareness-raising issues.

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 realization of the objectives. The implementation plan will also define the membership, meeting procedures, and tasks of the council.

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

[1] *http://www.riso.ee*

[2] *http://www.crn.ethz.ch/publications/crn_team/ciip_by_chapter/partI/estonia.pdf*

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.

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 defence will be addressed in greater detail in a document entitled "National Defence Development Plan 2009–2018".

Estonian Information Society Strategy 2013[3]

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. The strategy sets out the general framework, objectives, and respective action fields for the development of the information society in Estonia. It emphasizes the importance of cooperation between the public and private sectors and the need for coordination among all ministries involved. The strategy aims to place more emphasis on the development of a citizen-centric and inclusive society, a knowledge-based economy as well as a transparent and efficient Public Administration.

The Implementation Plan of the Estonian Information Society Strategy specifies priorities in the short-term perspective, proceeding from the objectives of the strategy and considering the current situation. The Government of the Republic approved in January 2009 the Implementation Plan 2009-2010 of the Estonian Information Society Strategy. The priorities of this implementation plan are the following:

- Improving skills of and widening opportunities for participation;
- Development of eBusiness environment;
- Transition to digital management of business;
- Development of public e-services, including information services;
- Large-scale take-up of eID;
- Increasing the interoperability of the state information system;
- Raising the quality of statistical analysis through improved use of data in the state information system.

The document stresses the importance 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.

[3] *http://www.epractice.eu/en/document/288215*

Emergency Act

This act provides the legal bases for crisis management, including preparing for emergencies and responding to emergencies as well as ensuring the continuous operation of vital services. In relation to critical ICT infrastructure, there are provisions regulating the management of the organisation of protection of data banks and telecommunications including: telephone networks; data communication networks; cable casting networks; broadcasting networks; mobile telephone networks, and marine radio communication.

The Act identifies and allocates responsibility to the relevant Ministries for, 41 vital services, amongst which are the following ICT-related services: telephone networks, mobile telephone networks, broadcasting networks, marine radio communication networks, cablecasting networks, and data communicating networks.

Information Security Policy

The Estonian Ministry of Economic Affairs and Communications (MEAC) has prepared a nation-wide information security policy that specifies and coordinates the upcoming eSecurity-related initiatives. The main goal of the Estonian Information Security Policy is to found a secure, security-aware, internationally cooperating and enabling Estonian Information Society. Specific goals include the elimination of non-acceptable risks, the defence of basic human rights, information security awareness and training, participation in international eSecurity-related initiatives, as well as the competitiveness of the economy.

The regulatory framework

Personal Data Protection Act [4]

The Act protects the fundamental rights and freedoms of persons with respect to the processing of their personal data, in accordance with the right of individuals to obtain freely any information that is disseminated for public use.

Information Society Services Act [5]

The Information Society Services Act was passed on 14 April 2004 and entered into force on 1 May 2004. It implements EU Directive 2000/31/EC on certain legal aspects of Information Society services, in particular electronic commerce, in the Internal Market. It establishes the requirements pertaining to Information Society service providers, as well as the organisation of supervision and liability in the case of violation of these requirements.

Electronic Communications Act [6]

The purpose of this Act is to create the necessary conditions to promote the development of electronic communications networks and communications services while

[4] *http://www.epractice.eu/en/document/288216*
[5] *http://www.epractice.eu/en/document/288216*
[6] *http://www.epractice.eu/en/document/288216*

ensuring the protection of the interests of users of such services. The Act provides requirements for: publicly available electronic communications networks and communications services; radio-communication; management of radio frequencies and numbering; apparatus and State supervision over the compliance with the requirements.

Following the recommendation of the European Commission inviting Member States to complete the transition to digital television broadcasting by 2012 at the latest, Estonia started the transition process in January 2006. The necessary measures have been adopted by the Government and the legislative process is currently under way.

Digital Signature Act [7]

Approved on 8 March 2000, the Digital Signatures Act (DSA) entered into force on 15 December 2000. It grants similar legal value to digital and handwritten signatures.

Public Information Act

The purpose of this Act is to ensure that the public and every person has the opportunity to access information intended for public use, based on the principles of a democratic and social rule of law and an open society, and to create opportunities for the public to monitor the performance of public duties.

System of security measures for information systems

Government of the Republic Regulation No. 252 of 20 December 2007

The Regulation establishes the system of security measures for information systems used for processing the data contained in state and local government databases and for information assets related therewith. The system of security measures consists of the procedure for the specification of security measures and the description of organisational, physical and IT security measures to protect data.

Emergency Act
This act provides the legal bases for crisis management, including preparing for emergencies and responding to emergencies as well as ensuring the continuous operation of vital services.

Providers of vital services are obligated to ensure the continuous application of security measures in regards to the information systems used for the provision of vital services and the related information assets.

Cyber-crime legislation[8]

The following articles in the penal code are related to cyber crime and security:

§ 206. Computer sabotage: (1) Unlawful replacement, deletion, damaging or blocking of data or programs in a computer, if significant damage is thereby caused, or unlawful entry of data or programs in a computer, if significant damage is thereby caused, is punishable by a pecuniary punishment or up to one year of imprisonment. (2) The same

[7] *http://www.epractice.eu/en/document/288216*
[8] *http://www.coe.int/t/e/legal_affairs/legal_co-operation/fight_against_terrorism/4_Theme_Files/Estonia.pdf*

act, if committed with the intention to interfere with the work of a computer or telecommunications system, is punishable by a pecuniary punishment or up to 3 years' imprisonment.

§ 207. Damaging of connection to computer network: Damaging or obstructing a connection to a computer network or computer system is punishable by a pecuniary punishment.

§ 208. Spreading of computer viruses: (1) Spreading of a computer virus is punishable by a pecuniary punishment or up to one year of imprisonment. (2) The same act, if committed: at least twice, or in a manner which causes significant damage, is punishable by a pecuniary punishment or up to 3 years' imprisonment.

§ 217. Unlawful use of computer, computer system or computer network: (1) Unlawful use of a computer, computer system or computer network by way of removing a code, password or other protective measure is punishable by a pecuniary punishment. (2) The same act, if it: causes significant damage, or is committed by using a state secret or a computer, computer system or computer network containing information prescribed for official use only, is punishable by a pecuniary punishment or up to 3 years'imprisonment.

§ 284. Handing over protection codes: Unlawfully handing over the protection codes of a computer, computer system or computer network, if committed for the purpose of personal gain and in a manner which causes significant damage or results in other serious consequences is punishable by a pecuniary punishment or up to 3 years' imprisonment. Computer-related offences is covered by computer-related fraud (§ 213).

Self-regulations

There is currently no code of conduct adopted by the Estonian mobile telecom operators.

NIS Governance

Overview of the key stakeholders

We included below a high-level overview of the key actors with relevant involvement, roles and responsibilities in NIS matters.

National Authorities	• Ministry of Economic Affairs and Communications, Department of State Information Systems (RISO) • Ministry of the Interior • The Foreign Ministry • Ministry of Defence of the Republic of Estonia • IT Crimes Office, Central Criminal Police • Estonian Data Protection Inspectorate • Estonian Technical Surveillance Authority (ETSA) • Estonian National Security Authority (NSA) • Estonian Competition Authority • State Chancellery, Office of the National Security Coordinator – • Estonian Informatics Centre (RIA), Department for Critical Information Infrastructure Protection (CIIP) • Estonian Educational and Research Network (EENet)
CERTs	• CERT-EE - Estonia Computer Emergency Response Team • SKY-CERT - Skype Computer Emergency Response Team
Industry Organisations	• Estonian Information Technology Society (EITS) • Estonian Association of Information Technology and Telecommunications (ITL)
Academic Organisations	• Faculty of Information Technology – Tallinn University of Technology • Estonian IT College • University of Tartu
Others	• AS Sertifitseerimiskeskus (SK) • Cybernetica Ltd. • Look at World Foundation • ISACA Estonia Chapter • ETL (Estonian Consumers Union - Eesti Tarbijakaitse Liit)

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who" – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory[9]

NOTE: only activities with at least a component of the following eight ENISA focus points have been taken into account when the stakeholders and their interaction were highlighted: CERT, Resilience, Awareness Raising, Emerging Risks/Current Risks, Micro-enterprises, e-ID, Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

[9] http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country

Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS

Co-ordination via the Ministry of Economic Affairs and Communication (MEAC)

In Estonia there are several ministries and their respective subunits directly involved in NIS. The main tasks of NIS are assigned to the Ministry of Economic Affairs and Communication or MEAC. The MEAC plays a leading role with regard to information security, two central agencies for the national IT policy are subordinated to the MEAC:

- The Department of State Information System (RISO), the central body for overall ICT coordination;
- The Estonian Informatics Centre (RIA), which constitutes the implementing body under the MEAC.

Co-operation via the Estonian Informatics Centre (RIA)

Recently a central unit - department for Critical Information Infrastructure Protection (CIIP) - was founded and placed under the supervision of the Estonian Informatics Centre (RIA). The department analyzes the state's vital services and the influence of various IT systems to one another. The aim of the department is creating the defence system for Estonia's critical information infrastructure as well as running the system.

Co-operation via the Estonian Technical Surveillance Authority (ETSA)

The Estonian Technical Surveillance Authority (ETSA) is a governmental organisation established in 2008 by merging the Communications Board, the Railway inspectorate and the Technical Surveillance Inspectorate in the administrative area of the Ministry of Economic Affairs and Communications (MEAC). The aim is to be an effectively operating, competent and reliable regulatory and surveillance authority with high reputation in Europe.

Co-operation via EENET

Since 1997 EENet has been operating as a state agency administered by the Estonian Ministry of Education and Research. The mission of EENet is to provide a high-quality national network infrastructure for Estonia's research, educational and cultural communities.

Co-operation via CERT-EE

The CERT-EE is a department within the Estonian Informatics Centre and responsible for the management of security incidents in Estonian (.ee) computer networks. Its task is to assist Estonian internet users in the implementation of preventive measures in order to reduce possible damage from security incidents and to help them in responding to security threats. CERT-EE deals with security incidents that occur in Estonian networks, whether started there or abroad. CERT-EE is also a national contact point for international cooperation in the field of IT security and works closely with Police, Prosecutors and Child protection organisations. CERT-EE is also influencing IT education in Estonia. As far as cooperation between ISPs and the national CERT is concerned, the legal basis for such cooperation is unclear.

Computer Protection 2009 Initiative[10]

A cooperation agreement was signed in 2006 between the leaders of Estonia's largest banks and telecom companies and the ministry of economic affairs and communications. The agreement envisaged the launch of the Computer Protection 2009 initiative, which aims at making Estonia the most secure information society in the world through appropriate investments in PC protection, user awareness and widespread use of the electronic identity card.

Other co-operation of NIS-stakeholders to deal with NIS in Estonia

Other important public agencies that are dealing with NIS are located within the Ministry of the Internal Affairs and within the Ministry of Defense. These two ministries are responsible for internal security and crisis management. With the project Computer Protection 2009 by the Look@World Foundation, there is also an important public-private partnership. Computer Protection 2009 is a joint project of the Look@World Foundation and the Ministry of Economics and Communications. The Computer Protection 2009 project aims to foster the security of the Estonian information society, so that Estonia will be the country "with the most secure information security in the world".

In Estonia there is a high demand for high-level IT professionals. A solution for this high demand was proposed by the government, the Ministry of Education, that the largest Estonian universities – Tallinn Technical University and Tartu University – and the Estonian ICT industry create an Estonian Information Technology College. The College is a private institution, established and financed by the Estonian Information Technology Foundation (EITF). The college works very closely with both universities as well as with IT and telecoms industries. The EITF will have a further role in supporting IT research and development activities of the academic universities and the private sector.

Information exchange between providers and public authorities

The exchange of information between providers and public authorities is not required by ETSA. Information is not shared with ETSA. Other authorities exchange information with providers, which is needed for performing certain tasks according to the laws, regulations and agreements between different parties. Later on the collected information is used for development or changing strategies, policies, acts etc, - according to the needs and problems. In Estonia, there are public-private partnerships in the field on incidents' handling, in developing cyber security strategy, PKI infrastructure development and so forth. Between different providers there are different ad-hoc workgroups and some initiatives e.g. Providers, who are connected to the Tallinn Internet Exchange have a cooperation agreement.

International co-operation on cyber- crime and security

An important area of international co-operation for Estonia involves how to react to new security threats, especially when it comes to ensuring cyber security. The vulnerability of cyberspace is a serious security risk in today's world, which affects all nations and needs to be tackled on a global level. In May 2008, the Estonian government approved its national cyber security strategy. According to the plan, Estonia would like to actively participate in working out international cyber security policy, making the problem known

[10] http://www.riso.ee/en/pub/2006it/index.php?mn=13

through various international organisations (NATO, EU, UN, OSCE, European Council, etc.), and developing international co-operation networks that deal with cyber security. Estonia would like to unite as many nations as possible through international conventions addressing cyber crime and attacks, and achieve international moral condemnation of cyber attacks. The NATO Centre of Excellence in Cyber Defence is being established in Estonia, and as before, Estonia plans to continue sharing its cyber security-related experiences around the world.

International co-operation via the Cooperative Cyber Defence Centre of Excellence (CCD COE[11])

Estonia is participating in the Cooperative Cyber Defence Centre of Excellence (CCD COE) together with other sponsoring nations: **Germany, Italy, Latvia, Lithuania**, **Slovak Republic and Spain**. CCD COE is located in Estonia and is open to all NATO nations and may cooperate with other nations as contributing participants.

The CCD COE first priorities are to provide insight, subject matter expertise, and assistance to NATO on various aspects of cyber defence: input to concept development, training and exercises, publishing lessons learned, and the development of a legal framework for cyber defence.

[11] http://www.ccdcoe.org/

Country-specific NIS facts, trends, good practices and inspiring cases

Security incident management

In April 2007, Estonia came under cyber attack in the wake of relocation of the Bronze Soldier of Tallinn. Estonian authorities, including Estonian Foreign Minister Urmas Paet accused the Kremlin of direct involvement in the cyber attacks. Estonia's defence minister later admitted he had no evidence linking cyber attacks to Russian authorities. Most of the attacks that had any influence on the general public were distributed denial of service type attacks ranging from single individuals using various low-tech methods like ping floods to expensive rentals of botnets usually used for spam distribution. Spamming of bigger news portals commentaries and defacements including that of the Estonian Reform Party website also occurred. This case is studied intensively by many countries and military planners as, at the time it occurred, it may have been the second-largest instance of state-sponsored cyber warfare.

In 2008, over 150 computer related fraud cases were registered in Estonia.

It is interesting to mention that during the first half of 2009, Estonia was mentioned in the global report[12] published by the Anti-Phishing Working Group (APWG)[13] with the following relevant statistics:

- 11 unique phishing attacks reported for this country
- 9 unique domain names used for phishing reported for this country
- A score of 1.4 phish per 10.000 domains registered in this country
- A score of 1.7 attacks per 10.000 domains registered in this country

Emerging NIS risks

The national risk management process

There is a general risk management process, which is implemented to ICT sector also. The Estonian Ministry of Interior is responsible for the general level risk management issues in Estonia. According to the Emergency Act all providers of vital services are obligated to prepare a risk assessment of the continuous operation of the vital services provided by them. Also a continuous operation plan is mandatory.

Relevant emerging NIS risks

The Cyber Security Strategy of the Estonian Ministry of Defence identifies the following key risks applicable to NIS:

- The cyber attacks against the Estonian critical infrastructure
- The cyber crime.

---

[12] http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf

[13] *The Anti-Phishing Working Group (APWG) is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types.*

Resilience aspects

Besides several laws and acts, which directly and/or indirectly regulate network resilience issues; Regular audits of network and resilience are organized. After the adoption of a governmental decree on Information Systems Security Standard implementation, the organizations, who handle state registers have obligation to order IT audits after a certain time period – dependant on register security level after 2, 3 or 4 years Random audits or audits after an incident may be done by the National Audit Office of Estonia, Data Protection Inspectorate etc. According to ETSA, at the moment there is no regulation which would be demanding those audits. If service providers are auditing their networks, they are doing it voluntarily.

Regarding good practices on network and resilience aspects there is no official repository of good practices. Within the CERT community of Estonia, different guidelines and/or good practices and according to the certain situation are given.

Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented by the Personal Data Protection Act (Isikuandmete kaitse seadus) (the "DPA") dated 15 February 2007.

The competent national regulatory authority on this matter is the Data Protection Inspectorate (the "Inspectorate")

Personal Data and Sensitive Personal Data

According to the DPA personal data means any information relating to an identified and identifiable natural person irrespective of the form or format of the data. Therefore, the definition of personal data in the DPA is closely based on the standard definition of personal data.

Under the DPA, sensitive personal data includes the following: (i) the standard types of sensitive personal data; (ii) data regarding genetic information; (iii) biometrical data (such as data regarding fingerprints, handprints, eye irises and genetic data); and (iv) information about committed criminal offences (or being a victim of these) prior to a public court hearing.

As indicated in the section entitled "Notification or registration scheme and timing" above, processing of sensitive personal data is subject to registration with the Inspectorate. The exemptions provided in Article 8 (2) of the Data Protection Directive are not transposed into the DPA, however in practice these exemptions are relied upon extensively.

Also, in the case of processing sensitive personal data, the data subject shall have to be informed that the data being processed is sensitive personal data and the data subject's consent shall have to be in a format which can be reproduced in writing.

Information Security aspects in the local implementation of the Data Protection Directive

Data controllers must fulfil the general data security obligations. Additionally, data controllers have an obligation to keep records of devices and software under their control which are used for the processing of personal data, by recording the following data: (i)

name, type, location and manufacturer of the devices; and (ii) name and version of the software and name and contact details of its manufacturer.

Data protection breaches

The DPA does not contain any obligation to inform the Inspectorate or data subjects of a security breach.

Enforcement

Enforcement can be taken both by the Inspectorate, which is authorised to apply administrative coercion, initiate misdemeanour proceedings, and, if necessary, impose punishments, as well as the courts, who may impose pecuniary punishments for disclosure of information, obtained in the course of professional activities, relating to the health, private life or commercial activities of another person by a person who is required by law to maintain the confidentiality of such information.

NIS awareness at the country level

Programme "Increasing awareness of the information society" [14]

The aim of the programme funded by the Structural Funds of the European Union is to widen the uptake of existing e-solutions; promote the development of new e-services; and ensure, by raising awareness of information security, the sustainable development of the information society. The programme will be carried out in the years 2007-2013.

The target groups of the programme include consumers of both existing and future e-services; parties related to the development of e-services; and entrepreneurs, whose increased awareness of the information society will increase their motivation to apply IT solutions. The programme contains activities aimed at increasing the awareness of opinion leaders and representatives of media, contributing to increased interest and positive attitudes towards new e-solutions. In 2009, activities aimed at increasing awareness about information security both within the public sector and among the general public of Estonia were organised.

Awareness actions targeting the consumers/citizens

"Come Along!" (Ole Kaasas!) [15] is an Internet promotion project launched by EMT, Elion, MicroLink and the look@world foundation in the framework of the My Estonia initiative. The project aims to provide basic and advanced computer training to 100,000 people and connecting 50,000 more families to the Internet over the next three years. The target group includes members of the Estonian as well as Russian communities without the skills and opportunities to use the Internet: families with children; rural population; older generation; people on low and medium income. "Come Along!" focuses on: training and user assistance; hardware; connection.

Computer Protection 2009 is a joint project of the Look@World Foundation and the Ministry of Economics and Communications. The Computer Protection 2009 project aims to foster the security of the Estonian information society, so that Estonia will be the country "with the most secure information security in the world". To achieve this ambitious goal, the signing partners of the initiative started broad promotion programs

[14] *http://www.riso.ee/en/files/Yearbook2008/html/1.1.2.html*
[15] *http://www.olekaasas.ee*

to raise public awareness of IT security. They try to encourage citizens to use their ID card for electronic personal authentication. The main activities of the foundation include sharing of information among companies, public agencies, and citizens on how to adequately recognize threats to information security and to protect oneself against them. They also improve and promote internet security-related dialog and cooperation between the public and private sector.

Awareness actions targeting the Industry

The International Forum "Baltic IT&T"[16] is one of the largest and most significant ICT events in the Baltic Sea Region, bringing together senior government representatives, experts from European Commission and international organisations, as well as top level executives from the world's leading ICT companies and other business sectors. The major objective is to establish and promote effective partnerships among the public and the private sectors, associations and other IT&T industry related organisations in the Baltic Sea region to promote innovation and competitiveness.

Baltic IT&T Review is published quarterly by the Ministry of Economic Affairs and Communications, Republic of Estonia, the Secretariat of Special Assignments Minister for Electronic Government Affairs, Republic of Latvia, the Information Society Development Committee, and Government of Lithuania. The journal is intended mainly for government and academic institutions, ICT providers and users in the Baltic States and beyond, international organizations, embassies and institutions of cross-border cooperation that operate / are interested in the Baltic region.

The journal is a unique publication which promotes the exchange of information and experience among the countries of the Baltic Sea region, reflecting important activities and events which take place, spotlighting significant ICT projects and initiatives in the region.

The journal contains articles about:

- ICT Events and Forums;
- E-Government;
- E-Society;
- ICT Market;
- Communications.

Awareness actions on cyber-security

The Ministry of Economic Affairs and Communications of Estonia hosted the EU Ministerial Cyber Security Conference in Tallinn which took place two years after large scale cyber-attacks against Estonia. The main agenda in Critical Information Infrastructure Protection Conference (CIIP) in Tallinn was: How to warn? How to prepare? How to defend? How to co-operate globally? Last years have shown that cyber-attacks have reached an unprecedented level of sophistication and are increasingly performed for profit or political reasons.

[16] *http://www.ebaltics.com/?sadala=106*

Awareness measures to combat spam and/or malware

Awareness measures – Several websites have been launched in Estonia to raise awareness of the general public, one of them specifically addressed at children and youth. The national CERT website contains educational videos on actual cases of persons falling victim to online malpractices and instructional videos on how to reduce online risks.

Also, the Estonian data protection supervision authority informs and warns about spam on its website. Finally, the consumer protection authority has a website section with information on how to safely use the internet, including information on spam.

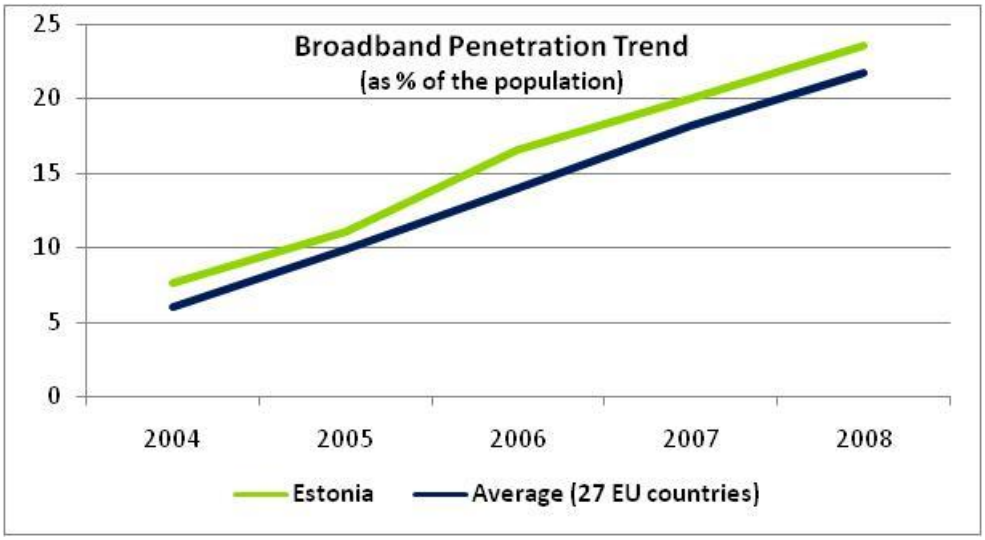
Other awareness-raising actions

Next to the major awareness raising campaigns a lot of smaller NIS awareness campaigns are set up by the Estonian Informatics Centre, these campaigns are rather small sized but have a stronger targeted audience.

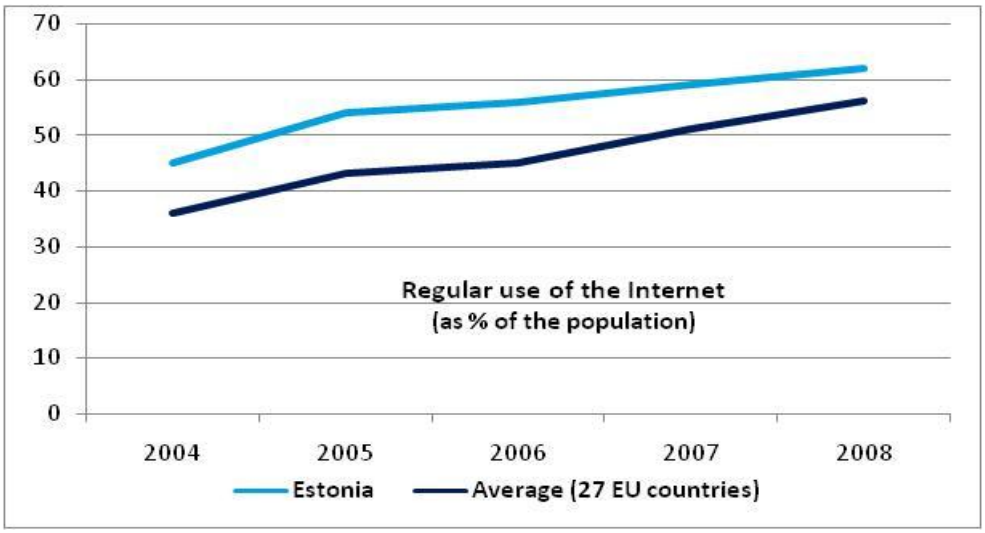
Relevant Statistics for the country

The information society in Estonia is at a relatively advanced stage of development. Progress has taken place since in the last years in the areas of broadband and internet usage; there is still room for improvement: above average rankings on broadband penetration, of Internet usage and e-Governance show that Estonia is above the European Average.

Based on the Eurostat[17] information, it appears that the broadband penetration trend for Estonia is above the EU average:



Based on the same source of information, the regular use of Internet by the population (use as % of the population) is constantly above the EU average and it continues on an increasing path. Rates of internet usage have been improving over the last few years. Take-up of the Internet in Estonia is average and more than half of the population has used the Internet. Usage of Internet services is correspondingly average and above the EU average.



[17] *Source: Eurostat*

APPENDIX

National authorities in network and information security: role and responsibilities

National authorities	Role and responsibilities	Website
1. Ministry of Economic Affairs and Communications	The Ministry of Economic Affairs and Communications is responsible for developing and implementing Security Technology and Standards Policy.	http://www.mkm.ee
2. Ministry of the Interior	The Ministry of Interior is an agent in the domain of crisis management, cyber-crime, critical infrastructure and responsible for the coordination of Information Security of Estonia. The Ministry of the Interior cooperates for these domains with MEAC (1).	http://www.siseministeerium.ee
3. The Foreign Ministry	The Foreign Ministry is responsible for the safeguarding of Estonia's security and welfare, as well as the promoting of Estonia's interests in the world, by planning and implementing the nation's foreign policy and co-ordinating its foreign relations.	http://www.vm.ee/?q=en/node/4104
4. Ministry of Defence of the Republic of Estonia	The Ministry of Defence is a government agency that performs the duties pursuant to laws and follows the guidelines given by the Government of the Republic. The Ministry of Defence cooperates with MEAC (1) on information security policy in two domains, crisis management and cybercrime and education and training.	http://www.mod.gov.ee/
5. IT Crimes Office, Central Criminal Police	The IT Crimes Office, Central Criminal Police is responsible for detecting and investigation of IT crimes.	http://www.pol.ee
6. Estonian Data Protection Inspectorate	The Estonian Data Protection Inspectorate is a national supervision agency responsible for the protection of personal data and managing public information on the internet.	http://www.dp.gov.ee
7. Department of State Information Systems (RISO)	The Department of State Information Systems is responsible for the coordination of state IT-policy actions and development plans in the field of state administrative information systems (IS). The department of State Information System is a subdivision of the MEAC (1).	http://www.riso.ee
8. Estonian Technical Surveillance Authority (ETSA)	The Estonian Technical Surveillance Authority is responsible for issues related to resilience of public communications networks and is a general regulatory authority in the field of electronic communication.	http://www.tja.ee
9. Estonian National Security Authority (NSA)	The Estonian National Security Authority is responsible for the receipt and protection of classified information of foreign states in the Republic of Estonia. NSA is a part of the Ministry of Defence of the Republic of Estonia.	http://www.mod.gov.ee/?op=body&id=522
10. Estonian Competition Authority	The Communications Division of the Estonian Competition Authority is responsible for the management of limited communication resources (e.g., radio frequencies) as well as for the	http://www.konkurentsiamet.ee/

National authorities	Role and responsibilities	Website
	regulation of the electronic communications market in Estonia.	
11. Office of the National Security Coordinator – State Chancellery	The Office of the National Security Coordinator advises the Prime Minister on issues related to national security and manages the operations of the National Security Committee of the Government of the Republic of Estonia.	http://www.riigikantselei.ee/?id=670
12. Estonian Informatics Centre (RIA)	RIA or the Estonian Informatics Centre is responsible for the development and administration of the state information system, so that the state could serve the citizens in their best possible way by implementing wisely IT capabilities.	http://www.ria.ee
13. Estonian Educational and Research Network (EENet)	EENet is a governmental non-profit organization administered by the Estonian Ministry of Education and Research; the mission of EENet is to provide a high-quality national network infrastructure for Estonia's research, educational and cultural communities.	http://www.eenet.ee
14. Department for Critical Information Infrastructure Protection (CIIP)	CIIP deals with the vital element of the protection of important information systems in Estonia – the IT systems of both the public and private sector. CIIP coordinates the general protective actions, yet the owner of every vital service will still be responsible for the daily defense of their system. The CIIP is a separate department inside the Estonian Informatics Centre and works on the strategic level of Information Security.	http://www.ria.ee/26267

Computer Emergency Response Teams (CERTs): roles and responsibilities

CERT	FIRST member	TI Listed	Role and responsibilities	Website
15. CERT-EE	No	Yes	CERT-EE is the Estonia Computer Emergency Response Team. CERT-EE is an organisation responsible for the management of security incidents in .ee computer networks. Also CERT-EE is a national contact point for international co-operation in the field of IT security.	http://www.cert.ee
16. SKY-CERT	Yes	Yes	SKY-CERT is the Skype Computer Emergency Response Team.	http://www.skype.com

Industry organisations active in network and information security: role and responsibilities

Industry organisations	Role and responsibilities	Website
17. Estonian Information Technology Society (EITS)	ETIS is responsible for National surveillance over the lawfulness of processing personal data, keeping databases and access to public information, and proceeding matters of administrative law breaches in cases provided for in the law, also exercising other duties assigned to it with laws and acts laid down by law. The EITS cooperates with the National Authorities.	http://www.eits.ee
18. Estonian Association of Information Technology and Telecommunications (ITL)	ITL's aim is to unite the Estonian information technology and telecommunications companies and promote co-operation between them to develop an information society. ITL acts to protect their members' interest and express their common positions.	http://www.itl.ee

Academic organisations active in network and information security: role and responsibilities

Academic bodies	Role and responsibilities	Website
19. Faculty of Information Technology – Tallinn University of Technology	The Faculty of Information Technology provides Information and communications technology programs for specialists who develop the resources for the information society in Estonia. Knowledge and skills of those specialists establish a sound foundation to the high-tech and science-based industry. The Faculty trains specialists in the main fields of information and communications technology, including informatics, computer and systems engineering, and electronics and telecommunications. NIS-related courses include Computer Network Attacks and Defence Mechanisms, Network Applications, Computer Networks, and Introduction to Data Security.	http://www.ttu.ee
20. Estonian IT College	The Estonian IT college satisfies the demand for high-level IT professional. The College is a private institution, established and financed by the Estonian Information Technology Foundation (EITF). NIS-related courses include Network Applications, Network Administration, Software Protection, and Data Security and Cryptology.	http://www.itcollege.ee
21. University of Tartu	The University of Tartu has different computers related faculties such as Faculty of Mathematics and Computer Sciences. The University is also active in the area and research of cyber security.	http://www.ut.ee

Other bodies and organisations active in network and information security: role and responsibilities

Other organisations	Role and responsibilities	Website
22. AS Sertifitseerimiskeskus (SK)	The goal of SK is to be the leading provider of certification products and services in Estonia. Its main service is provision of different certificates to individuals and organizations. Currently, the largest project handled by SK involves issuing authentication and digital signature certificates for Estonian ID cards. The core function of SK is to ensure the reliability and integrity of the electronic infrastructure behind the Estonian ID Card project. SK provides certificates for the card and also the services necessary for utilizing the certificates and giving legally binding digital signatures. SK also functions as a competence center for the ID card and assists with the creation of electronic applications for the card.	http://www.sk.ee
23. Cybernetica Ltd.	Cybernetica is a private research and development company, original equipment manufacturer and solutions provider active in the field of Information and Communication Technologies (ICT). They offer a wide range of original communication, visual navigation, light signalling and telematics products as well as off-the-shelf and tailored hardware/software system solutions.	http://www.cyber.ee
24. Look at World Foundation	The Look at the World Foundation is an IT security portal targeting citizens and providing information about using the Internet safely.	http://www.arvutikaitse.ee
25. ISACA Estonia Chapter	ISACA is a Worldwide association of IS professionals dedicated to the audit, control, and security of information systems. The chapter in Estonia organizes local events such as education and training, workshops and other specific events.	http://www.isaca.ee
26. ETL (Estonian Consumers Union - Eesti Tarbijakaitse Liit)	A consumer organisation, its aim is to protect and educate consumers.	http://www.tarbijakaitse.ee

Country specific NIS glossary

CCD COE	Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CIIP	Department for Critical Information Infrastructure Protection
DPA	Data Protection Act
DSA	Digital Signatures Act
EENet	Estonian Educational and Research Network
EITF	Estonian Information Technology Foundation
EITS	Estonian Information Technology Society
EMT	High technology service company operating in the field of telecommunications and information technology.
ETL	Eesti Tarbijakaitse Liit (Estonian Consumers Union)
ETSA	Estonian Technology Surveillance Authority
Isikuandmete kaitse seadus	Estonian Personal Data Protection Act
ITL	Estonian Association of Information Technology and Telecommunications
MEAC	Ministry of Economic Affairs and Communication
NSA	Estonian National Security Authority
Ole Kaasas!	"Come Along!" Internet promotion project
PIA	Public Information Act
RIA	Estonian Informatics Centre
RISO	Department of State Information Systems
The Inspectorate	Data Protection Inspectorate

References

- An overview of the eGovernment and eInclusion situation in Europe, available at http://www.epractice.eu/en/factsheets
- ENISA, Information security awareness in financial organisation, November 2008, available at http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
- Estonia - ENISA CERT Directory: http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/estonia

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu