National Cyber Security Strategies

Setting the course for national efforts to strengthen security in cyberspace

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

Resilience and CIIP Program at ENISA
Email: resilience@enisa.europa.eu

Contents

1. Introduction

Reliable communications networks and services have long been a critical element in ensuring public welfare and economic stability. Malicious attacks on the Internet, disruptions due to physical phenomena, software and hardware failures, and human errors all affect the proper functioning of essential public services that run over public telecommunication networks. Such disruptions reveal the increased dependency of our society on these networks and their services. This is echoed in the German cyber security strategy which states that, "The availability of cyberspace and the integrity, authenticity and confidentiality of data in cyberspace have become vital questions of the 21st century. Ensuring cyber security has thus turned into a central challenge for the state, business and society both at national and international level."[1]

Several of the European Commission's communications[2] have highlighted the importance of network and information security and resilience for the creation of a single European Information Space. The existing and recently proposed updates of Regulatory Framework Directives[3] and the recent Commission's Communication on Critical Information Infrastructure Protection[4] (CIIP) propose concrete policy and regulatory provisions for the improvement of the security and resilience[5] of public telecommunications.

Cyber security is increasingly regarded as a horizontal and strategic national issue affecting all levels of society. A national cyber security strategy (NCSS) is a tool to improve the security and resilience of national infrastructures and services. It is a high-level, top-down approach to cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe. As such it provides a strategic framework for a nation's approach to cyber security.

To assist the EU Member States in the important task of developing and maintaining a successful national cyber security strategy, ENISA is developing a Good Practice Guide[6]. The guide will present good practices and recommendations on how to develop, implement and maintain a cyber security strategy.

This paper presents some of the preliminary findings from the project that is developing the guide. It includes a short analysis of the current status of cyber security strategies within the European Union (EU) and elsewhere; it identifies common themes and differences, and concludes with a series of observations and recommendations.

---

[1] *P. 1 of the German Strategy*

[2] For example: COM/2005/0229 final "i2010 – A European Information Society for growth and employment"; COM(2006) 251 "A strategy for a Secure Information Society"; COM(2010) 245 final/2 "A Digital Agenda for Europe"; COM(2009) 149 on Critical Information Infrastructure Protection.

[3] *DIRECTIVE 2009/140/EC*

[4] *COM(2011) 163 final "Achievements and next steps: towards global cyber-security"*

[5] The ability of a network to provide and maintain an acceptable level of service in the face of various challenges to normal operation, 'Stock Taking of Member States' Policies and Regulations related to Resilience of public eCommunications Networks', ENISA, 2008.

[6] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss

2. Evolution of Cyber Security Strategies of EU Member States

The first national cyber security strategies began to appear during the first years of the previous decade. One of the first countries to recognise cyber security as a national strategic matter was the United States. In 2003 they published the National Strategy to Secure Cyberspace[7]. It was a part of the overall National Strategy for Homeland Security, which was developed in response to the terrorist attacks on September 11th 2001.

Developed for similar reasons, action plans and strategies with limited focus began to spring up across Europe in the following years. In 2005, Germany adopted the "National Plan for Information Infrastructure Protection (NPSI)"[8]. The following year, Sweden developed a 'Strategy to improve Internet security in Sweden'. Following the severe cyber-attack on Estonia in 2007, the country was the first EU Member State to publish a broad national cyber security strategy in 2008[9]. Since then considerable work has been done in this area on a national level and in the last four years, ten EU Member States have published a national cyber security strategy. These are briefly summarised below.

Across the EU there are also several Member States which are currently developing strategies – and some are very far in the process, close to publication. In addition, a few more EU Member States have unofficial or informal NCSS.

- ***Estonia*** (2008): Estonia emphasizes the necessity of a secure cyberspace in general and focuses on information systems. The recommended measures are all of a civil character and concentrate on regulation, education and cooperation.
- ***Finland*** (2008): The basis of the strategy is a view of cyber security as a data security issue and as a matter of economic importance that is closely related to the development of the Finnish information society.
- ***Slovakia*** (2008): Ensuring information security is viewed as being essential to the functioning and development of society. Therefore the purpose of the strategy is to develop a comprehensive framework. The strategic objectives of the strategy are mainly focused on prevention as well as readiness and sustainability.
- ***Czech Republic*** (2011): Essential objectives of the cyber security strategy include protection against threats which information and communication systems and technologies are exposed to, and mitigation of potential consequences in the event of an attack against ICTs. The strategy focuses mainly on unimpeded access to services, data integrity and confidentiality of the Czech Republic's cyberspace and is coordinated with other related strategies and concepts.
- ***France*** (2011): France focuses on the enablement of information systems to resist events in cyberspace which could compromise the availability, integrity or confidentiality of data. France

[7] http://www.dhs.gov/files/publications/editorial_0329.shtm

[8] http://www.bmi.bund.de/cae/servlet/contentblob/560098/publicationFile/27811/kritis_3_eng.pdf

[9] *Please see the annex for references to EU National Cyber Security Strategies*

stresses both technical means related to the security of information systems and the fight against cybercrime and the establishment of a cyber-defence.

- ***Germany*** (2011): Germany focuses on preventing and prosecuting cyber-attacks and also on the prevention of coincident IT failures, especially where critical infrastructures are concerned. The strategy sets the ground for the protection of critical information structures. It explores existing regulations to clarify whether, and if so, where additional powers are required to secure IT systems in Germany by means of providing basic security functions certified by the state and also supporting SMEs by setting up a new task force.
- ***Lithuania*** (2011): Lithuania aims to determine the objectives and tasks for the development of electronic information in order to ensure the confidentiality, integrity and accessibility of electronic information and services provided in cyberspace; safeguarding of electronic communication networks, information systems and critical information infrastructure against incidents and cyber-attacks; protection of personal data and privacy. The strategy also defines the tasks, which when implemented would allow total security of cyberspace and entities operating in it.
- ***Luxembourg*** (2011): Recognising the pervasiveness of ICTs, the strategy states that it is a priority to prevent any adverse effects on health and public safety or on the economy. It also mentions the importance of ICTs for citizens, society and for economic growth. The strategy is based on five action lines. These can briefly be summarised as CIIP and incident response; modernizing the legal framework; national and international cooperation; education and awareness; and promoting standards.
- ***Netherlands*** (2011): The Netherlands aims towards safe and reliable ICTs and fears abuse and (large-scale) disruption – and at the same time acknowledges the need to protect the openness and freedom of the Internet. The Netherlands include a definition of cyber security in the strategy: "Cyber security is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be comprised of a limitation of the availability and reliability of the ICT, breach of the confidentiality of information stored in ICT or damage to the integrity of that information."
- ***UK*** (2011): The UK approach is concentrating on the national objectives linked to evolving cyber security: making the UK the major economy of innovation, investment and quality in the field of ICT and by this to be able to fully exploit the potential and benefits of cyberspace. The objective is to tackle the risks from cyberspace like cyber-attacks from criminals, terrorists and states in order to make it a safe space for citizens and businesses.

3. Cyber Security Strategies of non-EU Nations

Below is a short introduction to three strategies from non-EU countries. Many other countries have also published NCSS, for example, India, Australia, New Zealand and Colombia. The list is by no means exhaustive. However, it does illustrate that the importance of cyber security is recognised globally.

United States of America

The United States released the International Strategy for Cyber-space in May 2011[10], which describes a set of activities across seven interdependent areas, based on a collaborative model involving government, international partners and the private sector:

- Economy: Promoting International Standards and Innovative, Open Markets.
- Protecting Our Networks: Enhancing Security, Reliability, and Resiliency.
- Law Enforcement: Extending Collaboration and the Rule of Law.
- Military: Preparing for 21st Century Security Challenges.
- Internet Governance: Promoting Effective and Inclusive Structures.
- International Development: Building Capacity, Security, and Prosperity.
- Internet Freedom: Supporting Fundamental Freedoms and Privacy.

Canada

Canada's cyber security strategy was published in 2010[11] and is built on three pillars:

- Securing government systems.
- Partnering to secure vital cyber systems outside the federal Government.
- Helping Canadians to be secure online.

The first pillar aims to establish clear roles and responsibilities, to strengthen the security of federal cyber systems and to enhance cyber security awareness throughout the government.

The second pillar covers a number of partnering initiatives with the provinces and territories and involving the private sector and critical infrastructure sectors.

Finally, the third pillar covers combatting cybercrime and protecting Canadian citizens in online environments. Privacy concerns are notably addressed in this third pillar.

Japan

Japan's cyber security strategy of May 2010[12] can also be decomposed into a number of key areas of action:

- Reinforcement of policies taking account of possible outbreaks of cyber-attacks and establishment of a response organization.
- Establishment of policies adapted to changes in the information security environment.
- Establishing active rather than passive information security measures.

---

[10] *http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf*

[11] *http://publications.gc.ca/site/eng/379746/publication.html*

[12] *http://www.nisc.go.jp/eng/*

The main action points covered by the strategy include:

- Overcome IT risks to realize safety and security in the nation's life.
- Implementation of a policy that strengthens national security and crisis management expertise in cyberspace, and integrity with ICT policy as the foundation of socioeconomic activities.
- Establishment of a triadic policy that comprehensively covers the viewpoints of national security, crisis management, and nation/user protection. An information security policy with a focus on the nation's/users' viewpoint is particularly important.
- Establishment of an information security policy that contributes to the economic growth strategy.
- Building up international alliances.

4. Common themes

At both the European level and international level a harmonised definition of Cyber Security is clearly lacking[13]. The understanding of cyber security and other key terms[14] varies considerably from country to country. This influences the different approaches to cyber security strategy among countries. The lack of common understandings and approaches between countries may hamper international cooperation, the need of which is acknowledged by all countries.

The main points covered by a typical NCSS are usually:

- To define a governance framework for cyber security.
- To define an appropriate mechanism (often a public private partnership) that allows all relevant public and private stakeholders to discuss and agree on different policy and regulatory cyber security issues.
- To outline and define necessary policy and regulatory measures and clearly defined roles, responsibilities and rights of the private and public sector (e.g. new legal framework for fighting cybercrime, mandatory reporting of incidents, minimum security measures and guidelines, new procurement rules). For example, the strategy from Slovakia identifies a need to define a legal framework for the protection of cyberspace[15].
- To set the goals and means to develop national capabilities and the necessary legal framework to engage in the international efforts of diminishing the effects of cybercrime. In several strategies there is a particular focus on cybercrime. For example in The Netherlands which aims to intensify investigation and prosecution of cybercrime[16]. France also stresses this point and wish to promote the strengthening of current legislation and international judicial cooperation[17].
- To identify critical information infrastructures (CIIs) including key assets, services and interdependencies.
- To develop or improve preparedness, response and recovery plans and measures for protecting such CIIs (e.g. national contingency plans, cyber exercises, and situation awareness). The Lithuanian strategy states that "To ensure cyberspace security it is necessary to establish a continuous and properly managed system covering all phases of incident management, such as early warning, prevention, detection, elimination and investigation."[18] This also includes defining integrated organisational structures that develop, implement and test these preparedness, response and recovery plans and measures. This may also mean an integration of existing structures (e.g. national/governmental CERTs).
- To define a systematic and integrated approach to national risk management (e.g. trusted information sharing and national registries of risks).

---

[13] *H. Luiijf, K. Besseling, M. Spoelstra, P. de Graaf, Ten National Cyber Security Strategies: a comparison, CRITIS 2011 – 6th International Conference on Critical information infrastructures Security, September 2011.*

[14] *The definition of cyberspace, cyber-attacks and cyber security policies also varies from country to country.*

[15] *P. 10 of the Slovakian strategy*

[16] *P. 12 of the strategy from the Netherlands*

[17] *P. 8 of the French strategy*

[18] *P. 4 of the Lithuanian strategy*

- To define and set the goals for awareness raising campaigns that instil changes in the behaviour and working patterns of users.
- To define the needs for new curricula with emphasis on cyber security for IT and security professionals and specialists; and also training programs that allow the improvement of skills of users. For example, the UK strategy aims to improve training and education for information security specialists to create a strong cyber security profession[19].
- International co-operation with EU and non EU Member States (e.g. adoption of international conventions).
- Comprehensive research and development programs that focus on emerging security and resilience issues of current as well future systems and services (e.g. smart devices).

[19] *P. 29 of the strategy from the UK*

5. The EU Internet Security Strategy

There is currently no overall EU cyber security strategy. However, as part of the Commission Work Programme for 2012[20], the Commission will develop an Internet Security Strategy for Europe. This work will be carried out by DG CONNECT (DG INFSO[21]). The objectives of the initiative are to:

- Describe the main risks and challenges as well as the economic and geopolitical opportunities.
- Compare states of preparedness or political attention given to the topic in other third countries.
- Describe the major issues at stake or problems to be addressed.
- Assess the on-going or planned actions and also highlight the areas where more EU action is needed.[22]

It is not a cyber security strategy but it is likely to have common elements and objectives, for example, in defining and proposing suitable governance frameworks and setting goals for incident response capabilities.

Overall it will aim to place existing and planned actions in a global political framework. Also, it will prepare the agenda for further work by looking ahead to propose how to achieve a more comprehensive, consistent and structured EU approach to Internet security[23]. This will have a wide effect, which goes beyond issues for just DG CONNECT, which is why Vice President Commissioner Kroes has stated that this work is done in close collaboration with Commissioner Malmström (home affairs) and Vice President Ashton (the High Representative for foreign affairs and security policy)[24].

The need to focus on and achieve a more holistic and coordinated approach has been highlighted several times - ENISA recognised this in the 2011 paper *Cyber security: future challenges and opportunities*[25] and the House of Lords report on the EU Internal Security Strategy[26] also makes this point.

---

[20] *COM(2011) 777 final VOL. 1/2* http://ec.europa.eu/atwork/programmes/docs/cwp2012_en.pdf

[21] *As of 1st of July 2012, DG INFSO changes name to DG CONNECT.*

[22] *COM(2011) 777 final VOL. 2/2* http://ec.europa.eu/atwork/programmes/docs/cwp2012_annex_en.pdf

[23] *ROADMAP: Proposal on a European Strategy for Internet Security*
http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf

[24] *SPEECH/12/204* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/204

[25] http://www.enisa.europa.eu/publications/position-papers/cyber-security-future-challenges-and-opportunities

[26] http://www.publications.parliament.uk/pa/ld201012/ldselect/ldeucom/149/149.pdf

6. Conclusions and recommendations

In an environment with constantly emerging and evolving cyber threats, EU Member States would greatly benefit from flexible and dynamic cyber security strategies to meet new, global threats. The cross-border nature of threats makes it essential to focus on strong international cooperation. Cooperation at pan-European level is necessary to effectively prepare, but also respond to cyber-attacks. Comprehensive national cyber security strategies are the first step in this direction.

We make the following recommendations to the Member States:

In the short-term:

- Develop, re-evaluate and maintain a National Cyber Security Strategy as well as action plans within the framework of the strategy.
- Clearly state the scope and objectives of the strategy as well as the definition of cyber security used in the strategy.
- Ensure that input and concerns from across governmental departments, national regulatory authorities and other public bodies are heard and addressed.
- Ensure the input and engagement of industry, academia and citizen representatives.
- Collaborate with other Member States and with the European Commission to ensure that the cross-border and global nature of cyber security are addressed in a coherent fashion.
- Recognise that the constant development and evolution of cyberspace and cyber security issues means that the strategy will have to be a living document.
- Be aware that the above point does not just mean emerging threats and new risks, but also opportunities to improve and enhance the use of information and communication technologies for government, industry and citizens.
- Ensure that strategies recognise and take account of the work that has been done to date in improving the level of security of national and pan European CIIP, by avoiding duplication of effort and concentrating on new challenges.
- Support the EU Commission in the definition of the Internet Security Strategy.

In the long-term:

- Agree on a commonly accepted working definition of cyber security that is precise enough to support the definition of common goals across the EU.
- Ensure that the cyber security strategies of the EU and of its Member States do not conflict with the goals of the international community, but rather support the efforts to tackle cyber security challenges globally.

The public and the private sector should work closely together to implement these cyber security strategies. This should be done through sharing of information, deployment of good practices (e.g. on incident reporting and handling) and through national exercises and pan-European exercises.

To assist the Commission and the Member States in this important task ENISA is developing a Good Practice Guide. This will present good practices and recommendations on how to develop, implement

and maintain a national cyber security strategy. The Good Practice Guide is intended to be a useful tool and practical advice for those, such as regulators and policy makers, responsible for and involved in cyber security strategies. The guide is being developed in collaboration with public and private stakeholders from across Europe with participation of a few international stakeholders to expand on the intermediate analysis and recommendations from ENISA as presented in this paper.

Annex – References to EU NCSS

Czech Republic: http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF

Estonia: http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

Finland: http://www.lvm.fi/c/document_library/get_file?folderId=57092&name=DLFE-5405.pdf&title=Valtioneuvoston%20periaatep%C3%A4%C3%A4t%C3%B6s%20kansalliseksi%20tietoturvastrategiaksi%20%28su/ru/eng%20LVM62/2008%29

France: http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011

Germany: http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1

Lithuania: http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf

Luxembourg: http://www.gouvernement.lu/salle_presse/actualite/2011/11-novembre/23-biltgen/dossier.pdf *(in French)*

Netherlands: http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011

Slovakia: Not available online

United Kingdom: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu