ENISA Guidelines for developing National Cyber Security Strategies

Desktop Research Report 2012

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact details

Nicole Falessi nicole.falessi@enisa.europa.eu Razvan Gravila razvan.gravila@enisa.europa.eu
Maj Ritter Klejnstrup majritter.klejnstrup@enisa.europa.eu

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

Table of Contents

Executive summary

In a constantly changing cyber threats environment, EU Member States need to have 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.

At a European and International level a harmonised definition of Cyber Security is lacking[1]. The understanding of cyber security and other key terms[2] varies from country to country. This influences the very different approaches to cyber security strategy among the countries. The lack of common understandings and approaches between countries may hamper international cooperation, the need of which is acknowledged by all countries.

In light of this, ENISA has conducted an initial research study aiming to identify the most common and recurrent elements of National Cyber Security Strategies (NCSSs), in the EU and non-EU countries. ENISA has studied the existing NCSS, structure and content wise, in order to determine the relevance of the proposed measures for improving security and resilience. We have been analysing the components of a Cyber Security Strategy in 9 EU countries[3] and 3 non-EU countries[4].

The components of a NCSS have been categoried under sub-headings of preparedeness, response and recovery. It's worth noting that many of the components and issues that should be addressed in a NCSS are horizontal or can fall into more than one of the categories. For example, national contingency plans should be developed and exercised as part of a countries preparedness measures. If such a plan is put into action, then it will be part of a countries responses and perhaps also of the recovery.

The findings of an initial research are presented in this Study. A final report, in the form of a Good Practice Guide, will be developed, highlighting good practices and recommendations on how to develop, implement and maintain a 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 and involved in cyber security strategies.

---

[1] *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.*

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

[3] *Czeck Republic, Estonia, Finland, France, Germany, Lithuania, Netherlands, Slovakia, United Kingdom.*

[4] *United States of America (USA), Canada and Japan. Information about USA and Canada has been provided by the European Commission as an informal input to our research activity.*

Introduction

A national cyber security strategy (NCSS) is a plan of actions designed 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 framework for a country's approach to cyber security.

During 2008-2011 a number of EU Member States have developed a NCSS but there are still EU countries which appear not to have a comprehensive cyber security strategy even though cyber threats have become more complex and various.

Developing a comprehensive NCSS is a challenge. A document which ticks all the right boxes for what should be included can easily be made. However, this is unlikely to achieve any real impact in terms of improving the cyber security and resilience of a country. To develop a NCSS it is necessary to achieve cooperation and agreement from a wide range of stakeholders to agree on a common course of action – this will not be an easy task. It should be realised that the process of developing a NCSS is probably as important as the final document. This should, in any case, not be a static product.

The European Policy context

Some of these ICT systems, services, networks and infrastructures form a vital part of the European economy and society. Hence they are typically regarded as critical information infrastructures (CIIs) as their disruption or destruction would have a serious impact on vital societal functions. Security of IT factors is one essential component for a well-functioning information society. *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*[5] sets among its objectives[6] to raise the levels of security for citizens and businesses in cyberspace also by providing guidance for citizens on cyber security and cybercrime[7]. This is recognised in the Digital Agenda for Europe[8] which addresses issues related to cybercrime, cyber security and security for network users. Under its Work Programme 2012, the European Commission announced, among its forthcoming initiatives, a European Internet Security Strategy[9]. Based on the description of scope of objectives *'The initiative will aim to: describe the main risks and challenges as well as the economic and geopolitical opportunities; compare with "preparedness" or political attention given to the topic in other third countries; describe the major issues at stake or problems to be addressed;*

---

[5] *Communication from the Commission to the European Parliament and Council 'The EU Internal Security Strategy in Action: Five steps towards a more secure Europe', COM (2010), 673.*

[6] *See in particular Objective n. 3, COM (2010), 673, page 9.*

[7] *Communication from the Commission to the European Parliament and Council 'The EU Internal Security Strategy in Action: Five steps towards a more secure Europe', Annex: Summary of objectives and actions, COM (2010), 673, page 17.*

[8] *Communication from the Commission to the European Parliament the Council the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, COM (2010), 245.*

[9] *Annex to the 2012 Commission Work Programme – Action 23 under the Digital Agenda Section, available at http://ec.europa.eu/atwork/programmes/index_en.htm*

assess the ongoing or planned actions where and when they exist, but also highlight the areas where more EU action'.

Methodology

To perform this first data and information collection and assessment we have researched and analysed the cyber security strategies within EU and non-EU countries publicly available or made available to us. Part of the data and information included in the annexes has been provided by the European Commission as an informal input to our research activity.

The Study introduces the suggested components for a NCSS. These have been categoried under sub-headings of preparedeness, response and recovery. For each component, it is explained what it means, who should be involved and examples are given as to how this can be done, how it has been done in other countries, and where more detailed guidance is available.

The Study also gives an overview of the policy priorities and initiatives of Cyber Security Strategies in non-EU countries, namely the USA, Canada and Japan. Finally, all the information and data provided in this research study have been collected and categorised in three different tables containing:

- A comparison of approaches of selected components of each cyber security strategy;
- Overview of common components of Cyber Security Strategies in EU countries;
- Common[10] statements in the strategies including some detailed measures[11].

Target audience

The main audience for this study is mainly public stakeholders responsible and involved in preparing and implementing a Cyber Security Strategy within a country. For example, it can help:

- Policy makers;
- Regulators;
- Institutions involved in the preparation and implementation of a NCSS.

[10] *The measure is stated as 'common' if more than four countries proposed it.*

[11] *Data and information provided by the European Commission as informal input to ENISA's study.*

Components of a National Cyber Security Strategy

A national cyber security strategy:

- ✓ defines the governance framework to achieve the objectives (e.g. PPPs), clarifies the role of existing competent authorities and paves the way for the creation of new authorities when existing ones cannot meet the challenges;
- ✓ introduces policy and regulatory measures that address certain gaps (e.g. new legal framework for fighting cybercrime, new procurement rules, standards/guidelines);
- ✓ explains the role, responsibilities, rights and obligations of the private sector (e.g. ISPs) in addressing the challenges and objectives of the strategy;
- ✓ defines preparedness measures to be followed during a crisis (e.g. situation awareness, crisis management units, trusted information sharing);
- ✓ develops strategies to address threats from criminals, terrorists and state actors;
- ✓ proposes a systematic approach to national risk management;
- ✓ raises awareness and supports a culture change by instilling changes in behaviour and working environments;
- ✓ enhances skills and education by the development of trainings, provisions of accreditation or incentives and viable career paths;
- ✓ defines actions for co-operation with other countries and the European Union (e.g. adoption of international conventions);
- ✓ suggests actions for new R&D investments that would improve the security of future systems and services (e.g. co-operative networks).

PREPAREDNESS

Preparedness is referring to the mechanisms set up by a National Cyber Security Strategy in order to avoid and mitigate the impact of disruptions affecting electronic communications and services. The measures included in prepredness program may include: the establishment of new organizations with responsabilities in the area of cyber security, a new legal framework, Public Private Partnerships (PPPs), research programs or awareness raising. As part of the life cycle of a NCSS, these measures would be revisited as response to such disruptions.

Who

Who is in charge: during our research, we have identified a growing tendency of Member States towards establishing National Cyber Security Centres. These new type of entities incorporate functions which, until recently, were distributed among a number of operational units and other bodies responsible with the dissemination of cyber security information. Such an approach raises the overall situational awareness in a country and sets the ground for a common operational picture in case of major ICT related crisis.

Other practices include defining specific tasks for bodies based on the area of expertise and national duties. Such bodies could include: national and governmental CERTs (alerts, awareness raising, etc.), law enforcement (cybercrime), regulators (policies), or academia (research and training curricula).

The Netherlands

Since January 2012 the National Cyber Security Centre in the Netherlands has become operational. The former GOVCERT.NL was the foundation of the new organization. The new entity will incorporate functions of the former national CERT and add new capabilities in order to mitigate existing and future threats.

The Dutch government wants public and private parties, acting within their statutory scope, to collect information, knowledge and expertise in a National Cyber Security Centre, which will help improve understanding of developments, threats, and trends and help parties deal with incidents and make decisions in crises.

When

Target dates: Based on the current stocktaking, the NCSS tend to be a set of priorities and objectives set for the mid-term future (3 to 5 years). Considering the dynamic nature of ICT threats, such an option gives prospect for upcoming changes in the security environment, but also keeps focus on the tactical aims set by the strategy.

The United Kingdom

The UK NCSS sets a vision for UK's cyber security in 2015. The UK aims to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace, to increase the resilience and shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies.

The strategy states that UK's vision for 2015 is: "to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society."

Estonia

The Implementation Plan of Estonia's NCSS was developed on the basis of proposals from different state agencies and working groups which have been set up for development of the strategy. Attention was given to the actions and funds needed to achieve the objectives of the strategy in its various fields of competence. Implementation plans have been developed for two periods: 2008–2010 and 2011–2013.

How

Implementation measures: NCSS contains a set of goals in order to ensure national security, by tackling the challenges of ICT threats. The implementation of security measures set by the NCSS is done by using action plans for responding to cyber-attacks and for the rapid recovery of damaged information systems. These action plans are sometimes included as part of, or annexes to the NCSS. The measures would also specify the course of actions to be taken in the event of cyber-attacks that jeopardise national cyber security, which are usually captured in a National Cyber Contingency Plan.

Other implementation measures may include: expanding the expertise and awareness of information security, national risk management, defining a regulatory framework to support the secure use of information systems or consolidating the nation as one of the leading voices in the area of cyber-security.

Governance Framework

What: The governance framework is the set up which ensures adequate input to scope and content of a NCSS in every phase of the life cycle. The governance framework should also include a definition of roles and responsibilities.

A NCSS may set the ground for the establishment of new bodies or PPPs which will ensure the achievement of the strategies' objectives. During our research, the roles and responsibilities described in NCSS are guidelines for future operational measures that need to be put in place by either existing bodies or by future entities. It also includes the responsibilities of those providing and making use of ICT services and it also determines the cooperation forms between the private sector and the general public.

Shared trust between the public and private sectors is vital in the area of sharing information and expertise. PPPs set the ground for effective cooperation models with define tasks, responsibilities, powers, and guarantees. Usually PPPs is an opportunity to avoid regulation by following a bottom up, soft law approach.

Who: Depending on the area of responsibility, NCSS may define roles and responsibilities of public and private bodies in the area of assuring the national cyber security. National cyber security agencies and national CERTs tend to play a leading role. Other actors involved could include academia, security experts, ICT operators, owners of CII or NGOs. It may also be

appropriate to mention end-users or citizens, and their responsibilities in contributing to the national cyber security.

Public bodies responsible with the security of ICT infrastructures and the general safety of the population may engage private sectors which are either part of CII or can play a vital role in the area of awareness rising.

How: NCSS may define a coordination body or define separate roles for different categories of threats. The distribution of responsibilities may include public organizations which deal with cybercrime, counter-terrorism, counterintelligence, CIIP, awareness raising or emergency responders.

NCSS define public-private groups which could work as a public-private expert group that can provide expertise to senior policy makers. Also, such groups have proven to be efficient in cases of major ICT related crisis.

ENISA has published a *'Good Practice Guide on Cooperative Models for Effective Public Private Partnerships'*[12] that sets out the principles underpinning Public Private Partnerships and reviews the range of partnership options available. It describes some of the ways in which partnerships can be used, and gives advice on the issues that need to be addressed when implementing them. The Guide is designed to help and support stakeholders in choosing options that will add value when they set up and run a PPP.

The Netherlands

In the NCSS of Netherlands a public-private partnership set the ground for the ICT Response Board which gives advice on measures to counteract major ICT disruptions to decision-making organisations. The Board began its activities in 2011 under the auspices of the National Cyber Security Centre.

Policy and regulatory measures

What: Policy and regulatory measures refers to the tasks assigned to and performed by the public authority (or authorities) in charge of and responsible of cyber security.It may also include the legislation which directly or indirectly affects cyber security, such as legislation on cybercrime or obligations of CII providers to ensure security and availability.

Who: The policy and regulatory framework is highly dependent on the national practices and institutional setup. Organizations involved in setting up the legal framework could include ministries, national security agencies, NRAs or the national and regional legislative bodies.

How: Bodies which are usually responsible with the initiation of legislation may involve private and civil entities in order to assure the transparency of the process. Other steps may include the improvement of existing legislation so that the cyber security field ultimately

12 http://www.enisa.europa.eu/act/res/other-areas/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps

comprises prevention, detection and response. An overview of national regulatory frameworks can be found in ENISA's Country Reports[13].

To tackle cross-border threats it is important that there is coordination, and that EU policy and regulatory measures are implemented in a coherent manner in Member States. Therefore it may be helpful for MSs to participate in working groups and follow recommendations from specialist bodies such as ENISA, for example on how to implement Article 13a of the Telecommunications Regulatory Directive[14].

Other relevant conventions should also be addressed in this part of the NCSS, such as for example the Council of Europe Convention on Cybercrime[15].

The Czech Republic

In the Czech NCSS it's stated that an appropriate legislative framework for the purpose of ensuring cyber security will be defined. This framework will not impose any restrictions on rights to freedom of speech, access to information for all population segments, and protection of privacy and confidentiality of information guaranteed by the national Constitution, taking into account international commitments of the Czech Republic, in particular to EU and NATO.

Also, the Czech Republic aims to actively participate in the drafting of legal acts and standards, and other forms of cooperation in the field of cyber security in the framework of EU and other international organizations.

Awareness Raising

What: NCSS aim towards increasing awareness of information security and the dissemination of information on secure computer use and the basic principles of information security. The objective is to increase the overall cyber security culture at the national level.

Who: Awareness raising is described as being the responsibility of both public and private bodies. Usually, in NCSS the security of information systems is considered to be depending on personal caution and on the sets of measures introduced by companies and the action of governments.

How: The national CERTs may organise information security awareness raising for the wider public in co-operation with the private sector. Other actions may include the raising of the awareness of cyber culture in public agencies and private companies by training staff in the promotion of secure computer and internet use.

---

[13] http://www.enisa.europa.eu/act/sr/country-reports

[14] http://www.enisa.europa.eu/act/res/reporting-incidents

[15] CETS no. 185 http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

ENISA has produced several guides and material to support awareness raising activities in organisations[16].

France

In the French NCSS, the national cyber security agency, ANSSI, will provide targeted support to decision-makers in order to help them draw up measures and make the necessary decisions regarding the security of information systems that are critical to the running of their organisations and the protection of their technical, scientific, commercial and financial assets.

Also, appropriate communication campaigns will be conducted by ANSSI targeting the general public and companies

National Risk Management

What: NCSSs recommend the usage of risk analyses and management for supporting the identification of measures needed to protect the national critical information infrastructures. Risk management should be an integral part of the NCSS life cycle.

Who: Risk management at national level requires efforts from both the private and public sector. The risk analysis is done based on the information collected, but during our research we have identified a tendency of NCSSs towards the establishment of a central 'analysing hub'.

How: Designated bodies will collect relevant information and perform the risk analysis. Information could have as a source both the private and the public sector. An NCSS could also state that privacy, fundamental rights and liberties, free access to information and other democratic principles should not be put at risk.

ENISA has worked extensively on risk management methodologies and guidelines. It may be useful to consult this work for the establishment of a national risk management process[17].

[16] http://www.enisa.europa.eu/act/ar

[17] http://www.enisa.europa.eu/activities/risk-management

The Netherlands

The Dutch NCSS considers that analysing knowledge and information from national and international public and private parties will increase the understanding of current and potential new threats and vulnerabilities. The NCSS aims for a framework which will permit the cataloguing of risks and the identifying of capacities that need to be strengthened in order to prevent threats and respond to disruptions.

International cooperation

What: In a global networked environment, there will only be an optimal response if issues that transcend national boundaries are managed and controlled correctly. Hence, a NCSS should address what approach a country will take to international cooperation.

Who: The strategy could assign the responsibility for international cooperation to one body. It is perhaps better to assign coordination of international cooperation to one body, and then leave the specifics to an appendix or supporting document.

How: The strategy should identify what kind of international counterparts, what sectors and on what issues the international cooperation should focus. This could be to enhance effective information sharing in case of cyber threats and in general on cyber security, tools for better cross-border investigations, participating in creating and implementing international standards, and collaboration on harmonized legislation and regulations on cybercrime and cyber security. ENISA has published a study on the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe[18].

Germany

The German strategy makes general statements about the importance of international cooperation; the aspects of importance, "the enforcement of international rules of conduct, standards and norms" and the cooperation of law enforcement authorities worldwide in the fight against cybercrime. The strategy also lists a number of organization with whom it is important to cooperate, United Nations, the EU, the Council of Europe, NATO, the G8, the OSCE and others.

The strategy also gives more details about selected initiatives in this area. For example, within the G8 framework Germany is working on intensifying anti-botnet activities.

Early Warning systems

What: Data on security incidents are fundamental for developing a clear understanding of the nature and extent of the challenges at stake, as well as for making effective business decisions

[18] http://www.enisa.europa.eu/act/cert/support/legal-information-sharing/legal-information-sharing-1

and addressing policy issues. It is important to have mechanisms in place to be able to recognise and detect dangers in due time. This can be complex to achieve because the threats can come from, and be aimed at, many different places.

The importance of incident reporting and data collection has also been highlighted at the policy-making level. The recently adopted reform of the Telecommunications Regulatory Directive specifies that European Union Member States must ensure that telecommunication operators notify the competent national regulatory authorities of a breach of security or loss of integrity that has had a significant impact on the operation of their networks.

Who: The stakeholders involved in this may be public bodies, academia or from the private sector, for example Internet Service Providers (ISPs). Because there are many different parties involved, it should be clearly defined who is responsible for reporting what to whom.

How: ENISA has published a '*Good Practice Guide on Incident Reporting*'[19] which examines the whole lifecycle of a reporting scheme, from the first steps in designing the scheme, through engaging the constituency's cooperation, setting the reporting procedures, and the continuous management and improvement of the scheme.

Also, ENISA provides guidance to National Regulatory Authorities (NRAs) on the implementation of Article 13a of the EU Telecommunications Regulatory Directive and in particular two types of incident reporting mentioned in Article 13a: the annual summary reporting of significant incidents to ENISA and the European Commission and the *ad hoc* notification of incidents to other NRAs in case of cross-border incidents.

The National Cyber Security Strategy should only address these issues at a high level and make reference to those responsible for the detailed guidelines and implementation.

Slovakia

The Slovakian strategy highlights the importance of providing statistics on security incidents to relevant stakeholders so that they can monitor and evaluate security levels in order to effectively manage cyber security.

Therefore it identifies the creation of an early warning system which notifies relevant stakeholders about threats and warns potential target groups as a task for improving the effectiveness of the country's information security management.

Research and Development

What: The pace of change and development in ICTs and accompanying threats is very fast. Therefore it is prudent to include in the strategy a component which suggests actions for new

[19] http://www.enisa.europa.eu/act/res/reporting-incidents/good-practice-guide-on-incident-reporting

R&D investments that would improve the security of future systems and services (e.g. co-operative networks).

Who: This is one of the areas, which possibly most clearly cuts across departments, sectors and industries. Hence it is important to define where the responsibility lies for defining and coordinating research topics and priorities for cyber security.

How: The strategy can identify how research, to develop expertise in cyber security, future technologies, national defence needs, emerging opportunities and threats, can best be supported. The strategy may contain details on the setting up of a dedicated research programme, how research will be funded and how international research cooperation will be enhanced.

United Kingdom

The strategy from the UK, has a multi-facetted approach to research and development. It is explained as important both in terms of developing a strong profession with appropriate cyber security skills, as an importunity for innovation and business, and also as necessary for improving the national level of cyber security.

The United Kingdom has been quite detailed in committing funds and assigning responsibility in the strategy, which states that the National Cyber Security Programme will a coherent cross-sector research agenda on cyber, building on work done by the UK Government Office for Science. In addition it will establish a research institute in cyber security, and it is stated in the strategy itself that this will have an indicative budget of £2 million over 3.5 years.

Also the Department for Business, Education and Skills (BIS) is assigned the task of research into cyber security breaches including research into security breach disclosure in UK business.

In addition the Government Communication Headquarters (GCHQ) will work with BIS, the Technology Strategy Board and the Engineering and Physical Sciences Research Council to explore strategic vehicles for bringing together industry, academia and Government to develop and exploit innovations in cyber security.

France

The French strategy emphasises the need for research as the only way of limiting the tactical advantage of attackers. Thus one of the seven action areas of the French strategy is to enhance “scientific, technical, industrial and human capabilities”.

RESPOND

Respond is referring to the capability of coping with the initial impact of an incident or emergency. This might include Computer Security Incident Response Support, Exercises, Emergency Planning and Crisis management[20]. International cooperation needs and information sharing should be address as well in the NCSS.

National Contingency Plans

What: National Contingency Plans (NCPs) for the Critical ICT Infrastructures (CIIs) are the interim structures and measures to respond and recover CII services following a cyber-crisis. CIIs are the Information and Communication Technology systems, services, networks and other infrastructures which form a vital part of European economy and society. The NCP should be developed well in advance and the existence and exercising of such response plans should be identified in the preparedness section of the NCSS.

Who: The national cyber or ICT contingency plan may be part of a broader general response plan in case of emergencies. In this case, the authority responsible for the management of general crisis management may facilitate the process of preparing the cyber contingency plan. In other cases the national cyber security agencies will assure the management of the document.

How: A strategy gives direction on how the country will deal with cyber security threats. Within this strategy, the country should come up with a view on the national response structure. In addition, the relation of the NCP for CII with other policy initiatives in the cyber domain should be stated. The cyber strategy, and related documents such as the NCP, should be regularly reviewed and updated in line with operational needs.

In 2012, ENISA will release a Good Practice Guide on National Contingency Plans which will enable the development of NCPs and their lifecycle and will help Member States (MSs) to develop, test, improve and maintain good and well-functioning NCPs for CII.

Estonia

The Estonian NCSS mentions the need to implement a system of cyber security measures which will 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.

[20] *Good Practice Guide on Cooperative Models for effective public Private Partnerships (ENISA 2011) available at* http://www.enisa.europa.eu/act/res/other-areas/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps

CERTs

What: Computer Emergency Response Teams (CERTs) sometimes also called Computer Security Incident Response Teams (CSIRTs) are a key tool for cyber security. All countries that are connected to the internet must have capabilities at hand to effectively and efficient respond to information security incidents. A country will have to be able to deal with many large and small incidents and CERTs will have a key role for coordinating the response and mitigation of such incidents.

Who: Many private organisations and academic institutions operate CERTs. However, there should also be a national or governmental CERT in each EU Member State.

This may be set up from scratch, or the role of national / governmental CERT may have been assumed de facto by an existing body. The 'Who' is not so important for this, but rather that the scale, scope and mandate of the CERT is clearly defined. The responsibility for incident response could also be shared among government and private sector organisations depending on the type of incident.

How: ENISA has published several guidelines to support the work of setting up, training, exercising and improving on the work of national and governmental CERTs. The framework and high-level responsibilities for incident handling should be addressed in the NCSS. Detailed plans for incident handling should be developed for different types and severity of incident. Some of this may fall under CERT mandates or under national contingency plans.

ENISA has published a report *'Baseline Capabilities for national/governmental CERTs'*[21] which defines the baseline capabilities of such a CERT in four categories:

- *Mandate / official framework* covers the powers and justification that need to be granted to the team by the respective government.
- *Service portfolio* covers the services that a team provides to its constituency or is using for its own internal functioning.
- *Operational capabilities* cover technical and operational requirements a team must comply with.
- *Cooperation capabilities* cover the requirements with regards to information sharing with other teams that are not covered by the previous three categories.

[21] http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs

The Netherlands

The strategy from The Netherlands includes references to strengthening the work of the governmental CERT, GOVCERT.NL and the setting up of a National Cyber Security Center. In practice with the setting up of the centre, the CERT function (along with tasks and employees of GOVCERT.NL) has all been transferred to the centre. In this way, The Netherlands are aiming to have an integral approach to cyber security and bring existing initiatives and expertise together, and to have a more visible single point of contact for cyber security.

France

The French strategy aims to improve and enhance the role of the French Network and Information Security Agency (ANSSI) by making it a national and centralised authority for incidence response.

United Kingdom

In the UK strategy there are actions included to both strengthen the Government Communication Headquarter's expertise and also to improve the capabilities for tackling cybercrime by creating a new national cybercrime capability as part of the new National Crime Agency.

RECOVERY

Recovery is referring to the capability of repairing the final impact of an incident. Whereas responding might involve using back up equipment, recover involves returning systems to business as usual. This might include Exercises, Emergency Planning, Mutual Aid and Crisis Management[22].

The recovery measures are not explicitly stated in the Strategies and should be elaborated from the interviews' outcome to be conducted by the Contractor.

[22] *Good Practice Guide on Cooperative Models for effective public Private Partnerships (ENISA 2011)* http://www.enisa.europa.eu/act/res/other-areas/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps

Overview of Cyber Security Strategies in non-EU -countries

United States of America

Based on the International Strategy for Cyber-space of May 2011, the United States Government organizes its activities across seven interdependent areas, each demanding collaboration within government, with international partners, and with the private sector.

Policy priorities are identified as follows:

- ✓ 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

Based on Canada's cyber security strategy the Strategy is built on three pillars and specific initiatives:

Securing government systems:

- ✓ Establishing clear federal roles and responsibilities;
- ✓ Strengthening the security of federal cyber systems;
- ✓ Enhancing cyber security awareness throughout government.

Partnering to secure vital cyber systems outside the federal Government:

- ✓ Partnering with the provinces and territories;
- ✓ Partnering with the private sector and critical infrastructure sectors.

Helping Canadians to be secure online:

- ✓ Combating cybercrime;
- ✓ Protecting Canadians online (privacy).

Japan

Based on Japan's cyber security strategy of May 2010 the overall aims are:

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

IT threat assessment:

- ✓ An increase in threats such as large-scale cyber attacks
- ✓ New external conditions and increasing importance of ICT to society and the nation

Key actions:

- ✓ 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

Concrete Measures:

- ✓ Preparation for a Potential Large-Scale Cyber Attack (organizing Counteractive Arrangements, building Up and Reinforcement of Day-To-Day Cyber Attack Information Collection and Sharing System);
- ✓ Reinforcement of Information Security Policy Adapted to Changes in the Information Security Environment (reinforcement of critical infrastructures, reinforcement of other infrastructures, enhancement of the functions of the National Information Security Center (NISC));
- ✓ Reinforced Protection of the Nation/Users (conducting an information security campaign, suggestion to set up the 'Information Security Safety Support Service', promotion of private information protection, tighten policing against cybercrime);
- ✓ Reinforcement of International Alliances (strengthening alliances with the United States, ASEAN, and EU countries, building an information sharing system through international conferences, such as APEC, ARF, ITU, Meridian, and IWWN, enhancement of the NISC's function as a point of contact);
- ✓ Furtherance of Technological Strategies (strategic furtherance of information security research and development, cultivation of information security human resources, establishment of information security governance);
- ✓ Organization of Legal System concerning Information Security (identify measures to improve cyberspace safety and reliability, comparison of information security legal systems of different countries).

Annex I - Comparison of approaches of selected components of each cyber security strategy

1.1 How is cyber security viewed in terms of importance to society?	
FRANCE (FR)	Objectives: ✓ Be at state of the art of Cyber-defence; ✓ Guarantee France Independence on Information protection; ✓ Ensure Security in Cyberspace.
GERMANY (DE)	'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' (available at http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile, **page 1** DE Strategy).
THE NETHERLANDS (NL)	'The increasing dependence on ICT makes society increasingly vulnerable to abuse and (large-scale) disruption'. 'Investing in cyber security means to invest in our future, our economic growth and our innovation' (available at http://www.govcert.nl/actueel/Nieuws/nationale-cyber-security-strategie-gepresenteerd.html , **pages 2 and 3** NL Strategy).
CZECH REPUBLIC (CZ)	'Safe, secure and reliable operation of ICTs is necessary for the functioning of government and public structures and is an indispensable prerequisite for prosperity and a sustainable economic growth….. The Czech Republic has an ambition to rank among advance nations in this respect' (**page 4** of the CZ Strategy, see **Annex I**).
ESTONIA (EE)	Estonia's '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' (available at http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf **page 6** EE Strategy).
UNITED KINGDOM (UK)	'While cyberspace fosters open markets and open societies, this very openness can also make us more vulnerable to those – criminals, hackers, foreign intelligence services – who want to harm us by compromising or damaging our critical data and systems'. 'The digital architecture on which we now rely was built to be efficient and interoperable. When the internet first started to grow, security was less of a consideration. However, as we put more of our lives online, this matters more and more. People want to be confident that the networks that support our national security, our economic prosperity, and our own private lives as individuals are safe and resilient' (available at http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy_0.pdfpages **1 and 15** of the UK Strategy). 'Our national security, as well as our economic prosperity, will depend on our ability to protect ourselves in cyber space' (available at http://www.cabinetoffice.gov.uk/resource-library/strategic-defence-and-security-review-securing-britain-age-uncertainty Factsheet 18, **page.1**).

FINLAND (FI)	The Strategy 'aims to make everyday life in the information society safe and secure for everyone in Finland – for people as individuals and business, administrative authorities, and all other actors in society'. 'It is crucial for a competitive information society that its most important information and knowledge capital, such as industrial property rights and business secrets, is protected' (**page 3** of the FI Strategy see **Annex II**).
LITHUANIA (LT)	'[…] the increasing significance of electronic information processed and transmitted by means of information and communication technologies'. 'The strategic objective of the programme is the development of the security of electronic information in Lithuania' (**page 1** LT Strategy).
SLOVAKIA (SK)	ICTs 'have a considerable effect on the development of human society… Ensuring information security of a country is essential to the functioning of society'. 'Given the fact that the state guarantees critical processes, its task is to take care of an overall level of competitiveness of society, thus preserving national welfare, including knowledge and information, therefore it cannot afford to have low security level criteria in place' (**page 3-4** SK Strategy).

1.2 How IT threats are assessed?

FRANCE (FR)	The increased usage of Information Technology has led to many new risks: ✓ Identity theft; ✓ Collection of payment or banking credentials; ✓ Gathering of Private information for reselling; ✓ Remote controlling applications; ✓ Botnets.
GERMANY (DE)	✓ Attacks more frequent and complex; ✓ Perpetrators more professional (perpetrators mentioned are criminals, terrorists and spies); ✓ Cross-border attacks; ✓ Covert attacks and difficulty in tracing attacker; ✓ CII are coming under attack. 'Given the increasing complexity and vulnerability of information infrastructures the cyber security situation will remain critical also in the future. In Germany, the public and the private sector as well as society at large are all equally affected by targeted or coincidental IT failures' (**page 2** of the DE Strategy).
THE NETHERLANDS (NL)	✓ Cross-border attacks and disruptions; ✓ Difficult to determine cause or source. More interconnectedness and interdependencies. ICT failure (no matter what the cause is) can lead to social disruption. 'The complexity of ICT facilities and our increasing dependence on them lead to new vulnerabilities and can facilitate disruption' (**page 2** of the NL Strategy).

CZECH REPUBLIC (CZ)	Speedy progress of ICTs brings new opportunities and threats. 'Attacks may be a new type of warfare, or may have a criminal, economic or terroristic motive and be launched to destabilize the society'. Increasing sophistication of attacks. Attacks aimed at critical infrastructures (**page 4** of the CZ Strategy).
ESTONIA (EE)	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. '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. Cyber warfare' (**page 10** of the EE Strategy).
UNITED KINGDOM (UK)	✓ Criminals; ✓ States; ✓ Terrorists; ✓ Hacktivists. 'Over the last decade the threat to national security and prosperity from cyber-attacks has increased exponentially. Over the decades ahead this trend is likely to continue to increase in scale and sophistication, with enormous implications for the nature of modern conflict. We need to be prepared as a Country to meet this growing challenge, building on the advanced capabilities we already have'. The risks from cyber space (including the internet, wider telecommunications networks and computer systems) have been identified in the National Security Risk Assessment as a Tier One risk. This means that they are judged to be one of the highest priorities for UK national security over the next five years, taking into account both likelihood and impact' (Factsheet 18, **page 1**).
FINLAND (FI)	'Electronic services and communications are increasingly to be found at the heart of the service system in both the public and the private sectors. At the same time, dependence on information technology is making services more vulnerable than ever' (**page 2** of the FI Strategy).
LITHUANIA (LT)	'The global cyberspace and the public services delivered online have become an attractive target for individuals, criminal groups, political forces and other subjects' (**page 1** LT Strategy).
SLOVAKIA (SK)	There is no specific threat assessment, but it is envisaged that this and evaluation of the effectiveness of measures will be assessed later. 'To measure whether the funds have been spent effectively will only be possible after the data on the number and impacts of security incidents before and after the implementation of security safeguards is available. So far, impacts may only be estimated based on information from abroad.' (**page 20** SK Strategy).

1.3 What are the Strategies' framework conditions?

FRANCE (FR)	Strategy consists in: ✓ Systematic Education of Enterprises and Consumers; ✓ Establishment and enforcement rules; ✓ Governmental systematic communication.
GERMANY (DE)	Strategy 'mainly focuses on civilian approaches and measures. It is complemented by measures taken by the Bundeswehr (German Army) to protect its capabilities and measures based on mandates to make cyber security a part of Germany's preventive security strategy' (**page 3** of the DE Strategy). ✓ Set up national Cyber Response Centre; ✓ Set up a National Cyber Security Council.
THE NETHERLANDS (NL)	✓ Division of responsibility between departments: '[…] the Minister of Security and Justice is in charge of the coherence and cooperation within the field of cyber security and is accountable in this respect. Besides this, each party retains its own tasks and responsibilities' (**Page 4** of the NL Strategy); ✓ Public-Private Partnerships; ✓ Set up Cyber Security Board; ✓ Set up National Cyber Security Centre (expand and reinforce the current GOVCERT.NL and place it within this centre).
CZECH REPUBLIC (CZ)	✓ The cyber security strategy is linked to the overall security strategy; ✓ All parts of society are responsible for security and there must be cooperation; ✓ Overall responsibility for cyber security issues are with the Ministry of the Interior of the Czech Republic; ✓ Important role for the Interdepartmental Coordination Board for Cyber Security (ICBCS) which initiates cooperation among government institutions and agencies; ✓ National CERT to be established.
ESTONIA (EE)	✓ The development and large-scale implementation of a system of security measures; ✓ Increasing competence in cyber security; ✓ Improvement of the legal framework for supporting cyber security; ✓ Bolstering international co-operation; ✓ Raising awareness on cyber security.
UNITED KINGDOM (UK)	'Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society'. The main principles are: ✓ A risk-based approach […]; ✓ […] working in partnership; ✓ […] balancing security with freedom and privacy' (**Page 21** and **22** of the UK Strategy);

	✓ National cyber security programme funded with 650 million pounds over four years; ✓ Create new organisation, the UK Defence Cyber Operations Group; ✓ Public-Private partnerships (Factsheet 18).
FINLAND (FI)	'The overall responsibility for the … [strategy] lies with the Government… The Information Security Group of the Ubiquitous Information Society Advisory Board appointed by the Ministry of Transport and Communications supports the coordination of the Strategy's implementation and monitors the implementation process. The Information Security Group submits an annual report to the Government on the implementation of the Strategy and on the need to update it, and reports to the Ubiquitous Information Society Advisory Board on the progress of the work. […] an action plan will be drawn up' (**page 4** of the FI Strategy).
LITHUANIA (LT)	'The purpose… is to determine the objectives and tasks… which would allow total security of cyberspace and entities operating in this medium'. 'Coordination of Programme implementation shall be carried out by the Ministry of the Interior' (**pages 1** and **5** LT Strategy). Responsibility for the implementation of objectives and tasks is defined for each objective and task.
SLOVAKIA (SK)	The relevant EU and national law is listed, as is bodies and institutions in the Slovak Republic that deal with aspects of cyber security and data protection. It is indicated if there is coordination in different fields. Strategic objectives: ✓ Prevention; ✓ Readiness and sustainability.

1.4 What are the strategic objectives and measures?

	CIIP	***Responsibility*** ***Awareness***	***Legislation*** ***Crime***	***Products*** ***Hardware***	***Incident*** ***Response***	***Research***
FRANCE (FR)	Analyse and Prevent: follow up on new threats, new risks.	***Not mentioned***	Adapt Legislation	Establish Public-Private Partnerships with CIIs owners, and vendors.	Detect, Alarm, and respond: ANSSI's role is improved and enhanced in this respect, and becomes a national authority for this area.	Increase means for research and scientific development of countermeasures.
GERMANY (DE)	'The availability of cyberspace and the integrity, authenticity and	SME and citizens: information and advice; possibly greater	Effective crime control.	Use of reliable and trustworthy information	Tools to respond to cyber- attacks (including permanent	'Continue and intensify research on IT security 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' (**page 1** DE Strategy).	responsibility to providers: incentives and funds for security functions certified by the state.		technology. 'Our aim is to use components in critical security areas which are certified against an international recognized standard'. (**page 7** DE Strategy).	exercise process).	on critical infrastructure protection.' (**page 11** of DE Strategy).
THE NETHERLANDS (NL)	Resilience against ICT disruptions and cyber attacks.	Individual responsibility: 'All users… take suitable measures to secure their own ICT systems and networks and to prevent security risks for others' (**page 3** NL Strategy).	Intensify investigation and prosecution of cyber crime Adequate legal protection in the digital domain.	Look for options for improving the security of hard- and software.	Reinforce response capacity.	Stimulate research and education.
CZECH REPUBLIC (CZ)	Mandatory standards for elements of critical national infrastructure.	'Duty of the Czech Republic and a responsibility of all levels of government and administration, the private sector and the general public' (**page 3** CZ Strategy).	Adequacy of measures, balancing the need to guarantee security against respect for fundamental rights and liberties.	Interest of the state and business sector to define and implement minimum standards and require that they are strictly complied with.	Establish national CERT to identify attacks and coordinate countermeasures. Develop a national early warning system. Implement and regularly update plans.	Cooperation of the State, Private Sector and Academia. Platform for sharing information and lessons learnt. Supporting research and

						development.
ESTONIA (EE)	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.	***Not mentioned***	***Not mentioned***	***Not mentioned***
UNITED KINGDOM (UK)	The UK to tackle cyber-crime and be one of the most secure places in the world to do business in cyberspace.	The UK to be more resilient to cyber-attacks and better able to protect our interests in cyberspace. Develop cyber security professionals.	The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies.	Encourage the development of clear indicators of good cyber security products. (**page 9** of UK Strategy) Work with industry to develop rigorous cyber security and IA standards for ICT products and services supplied to Government and its Public Services Network (**page 27** of UK Strategy).	Improving incident response. (**page 36-39** of UK Strategy).	Developing a coherent cross-sector research agenda. Establish, with GCHQ's help, a research institute in cyber security, with an indicative budget of £2 million over 3.5 years. (**page 29** of UK Strategy).
FINLAND (FI)	Safeguarding functions that are vital to society in all circumstances.	Everyone's actions have impact on their own and other's security.	Develop a simpler and more predictable national	Provide secure electronic services and ensure confidentiality.	Threats require not only comprehensive preparedness and efficient networks	***No t mentioned***

	Improve risk management and service reliability.	Everyone must have adequate basic skills. Increase awareness and competence.	regulation environment for businesses.		of international cooperation but also a forward/looking approach and the identification of signs and signals of threats.	
LITHUANIA (LT)	Ensure an efficient functioning of critical information infrastructure Approve security requirements for CII (Annex –page 6).	'Secure cyberspace is the concern of all entities whose activities are related to the provision of services in cyberspace'. Enhance the culture of protection of electronic information security (Annex – page 8).	Improve the regulatory framework of electronic information security (Annex- page 2).	Reinforce the security of services delivered in cyberspace. Use services that comply with the requirements of electronic information security (Annex-page 11).	'Establish a continuous and properly managed system covering all phases of incident management, such as early warning, prevention, detection, elimination and investigation' (**page 4** LT Strategy)	Encourage the implementation of cyber - security projects on basis of cooperation between entities engaged. In government activities (Annex – page 4).
SLOVAKIA (SK)	Framework conditions, guidelines and recommendations for CII. Analyse the security level of CII (**page 12** SK Strategy).	Better awareness, education and competence at different levels (citizens to IT personnel) (**page 10** SK Strategy).	Necessary to define a legal framework for the protection of digital space (**page 9** SK Strategy).	Basic requirement and standards. Promote use of secure products and services (**page 12** SK Strategy).	Threat monitoring. Early warning. Collecting incident data. Assist in incident handling. (**page 11** SK Strategy).	'Promote research and development aimed at possible and existing problems in information security' (**page 13** SK Strategy).

1.5 International coordination and cooperation

FRANCE (FR)	Cooperation will happen as follows: ✓ Establishment of Information Sharing mechanisms about threats and new vulnerabilities of products and services; ✓ Fight Cybercrime.
GERMANY (DE)	Requires 'major efforts by the state both at national level and in cooperation with international partners'. Requires 'enforcement of international rules of conduct, standards and norms'. 'Enhancing the framework conditions for drawing up common minimum standards (code of conduct) with allies and partners'. Requires 'close cooperation between law enforcement authorities worldwide'. Cooperation with UN, EU, the Council of Europe, NATO, the G8, the OSCE and other multinational organizations. The aim is to ensure the coherence and capabilities of the international community to protect cyberspace. (**page 3** DE Strategy).
THE NETHERLANDS (NL)	'Digital society is global'. 'Cooperation between existing parties in the digital society is necessary, including at an international level'. 'The cross-border nature of threats makes it essential to focus on strong international cooperation….The Netherlands supports and actively contributes to the efforts of, e.g., the EU (Digital Agenda for Europe and the Internal Security Strategy), NATO (development of cyber defence policy in the framework of the new strategic concept), the Internet Governance Forum… The Netherlands is a proponent of a broad ratification and implementation of the Cyber Crime Convention of the Council of Europe' (**page 3** and **4** NL Strategy).
CZECH REPUBLIC (CZ)	Mainly focused on EU and NATO. Within EU and NATO, The Czech Republic 'will participate in the drafting of standards and international policies, as well as in activities of joint institutions and, at the same time, adequately apply the standards and relevant mechanisms in its own national cyber security legislation'.
ESTONIA (EE)	Estonia considers active participation in international organisations vital for increasing global cyber security. ✓ European Union (EU); ✓ United Nations (UN); ✓ North Atlantic Treaty Organisation (NATO); ✓ Council of Europe; ✓ Organisation for Security and Co-operation in Europe (OSCE); ✓ Organisation for Economic Cooperation and Development (OECD); ✓ Professional organization and international co-operation networks (**pages 23-26** EE Strategy).
UNITED KINGDOM (UK)	'We will work internationally to develop international principles or 'rules of the road' for behaviour in cyberspace. We will work with other countries on practical confidence-building measures to reduce the risk of escalation and avoid misunderstandings' (**page 26** UK Strategy). 'Establishing stronger alliances with international counterparts, including by working on a UK-US Memorandum of Understanding to enable us to share information and plan and conduct operations jointly' (Factsheet 18, p.2)
FINLAND (FI)	Finland must be active in international cooperation between national authorities to prevent information security threats and minimise any possible damage. Globalisation is not just a threat but also an opportunity.
LITHUANIA (LT)	'Cyberspace is a global space which has no national borders… The European Union and NATO devote much attention to the security of electronic information and critical information infrastructure. It would be appropriate to apply the principle of collective security not only on a national, but also on international level.

	Cooperation among highly competent experts, exchange of available information and experience is a prerequisite for an efficient early warning and preventive action' (**page** 3 LT Strategy).
SLOVAKIA (SK)	'International cooperation in information security is necessary in order to ensure compatibility of solutions and sufficient level of protection of the global ICT' (**page 7** SK Strategy). 'Active involvement in the activities carried out by key international organisations… is necessary' (**page 12** SK Strategy).

Annex II - Overview of common components of cyber security strategies in EU countries

The table below gives an overview of whether the analysed national strategies have incorporated topics and areas which should be addressed in a countries overall framework and approach to cyber security. Except for *'defining preparedness measures',* most issues are addressed in some way by most countries. However, it is very different from Country to Country how concretely the issues are addressed and in what level of detail.

	UK	NL	CZ	EE	FI	FR	DE	LT	SK
Defines the governance framework to achieve the objectives, clarifies the role of existing competent authorities	✓ p. 9	✓ p. 3 p. 9	✓ p. 5 p. 8	✓ p. 8-9 p. 14 -15	✓ p. 4	✓ p.7	✓ p. 6 p. 12	✓ p. 3 p. 7 p. 17	✓ p.6-7
Introduces policy and regulatory measures	✓ p. 21-23	✓ p. 10	✓ p. 7	✓ p. 17-21	✓ p. 1-2	✓ p. 8	✓ p. 6-7	✓ p. 7 p.17	✓ p.13-14
Explains the role, responsibilities, rights and obligations of the private sector	✓ p. 28	✓ p. 12		✓ p. 14-16		✓ p. 17		✓ p. 3	
Defines preparedness measures to be followed during a crisis									

Develops strategies to address threats from criminals,	✓ p. 21	✓ p. 13-14	✓ p. 7	✓ p. 18-20		✓ p. 11	✓ p. 10-11		✓ p.9
Proposes a systematic approach to national risk management	✓ p. 25-27	✓ p. 6	✓ p. 6	✓ p. 27-29	✓ p. 2-3	✓ p. 15	✓ p. 7	✓ p. 7 p.17	✓ p.18-20
Raises awareness	✓ p. 31	✓ p. 15	✓ p. 15	✓ p. 29-30	✓ p. 2	✓ p. 18	✓ p. 7	✓ p. 7-17	✓ p.10
Enhances skills and education	✓ p. 31	✓ p. 15	✓ p. 9	✓ p. 16-17		✓ p. 16	✓ p. 12	✓ p. 7-17	✓ p.10
Defines actions for EU and international cooperation	✓ p. 26	✓ p. 6	✓ p. 6	✓ p. 17-18	✓ p. 3	✓ p. 18	✓ p. 11	✓ p. 11	✓ p.4 p.12
Suggests actions for new R&D investments	✓ p. 32	✓ p. 15	✓ p. 9	✓ p. 16-17	✓ p. 3	✓ p. 16	✓ p. 12	✓ p. 10	✓ p.13

Annex III - Common statements in the strategies including some detailed measures

The data contained in the table below have been provided by the European Commission as an informal input to ENISA research activity. The measures/statements below are stated as common if more than four countries proposed it.

Understanding of cyber security	- different understanding of 'Cyber Security' among the countries - earlier strategies concentrate on general security in ICT and data protection; later ones concentrate on protection from danger or damage caused by cyber-crime or disruption - Definition by the Netherlands: "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."
Basic assumptions and aims	- need for a balance between security and fundamental rights *(common)* - support of public-private-partnerships and cooperation with the academia *(common)* - all already taken initiatives shall be connected and reorganised by the new strategies *(common)* - clarify and diversify the responsibilities of citizens, companies and public authorities (NL)
International	- general agreement among the countries on international cooperation (different suggestions like a network of allies (FR) or participation in UN, OSCE, OECD, NATO (DE, EE), G8 (DE), IGF (NL), the Council of Europe (DE,EE) or the International Watch and Warning Network (NL)) - countries want to influence international cyber security regulations according to their aims *(common)* - smallest content internationalisation considered by the UK - detailed measures: effective information sharing in case of cyber-threats and in general on cyber-security (FR); code for state conduct in cyber space (DE); better cross-border investigations (DE, NL); international standards (DE, FI), legislations and regulations on cyber- crime and cyber-security (EE, DE, NL)

European Union		- ask for uniform implementation of existing directives (FI) - support of the action plan for the protection of critical infrastructures, the Internal Security Strategy and the Digital Agenda (DE) and the European disclosure obligation for data leaks (NL) - criticism on the Council Framework Decision 222/2005/JHA, the Data Protection Directive and the EU Electronic Commerce Directive (EE) - asking for more cooperation and regulations (common); detailed measures: cross border investigations (NL); cooperation among CERT organisations and cyber-crime units of the member states (NL); more activities of the EU in fields of penalty law and cooperation of law enforcement agencies and judicial authorities (DE, EE); enlargement of ENISA (DE,FI); research and development; development of an EU position in international areas and the initiation of international projects (EE)
Domestic measures	General organisation	- analysis of threats, risks and gaps in cyber space to figure out useful measures *(common)* - installation of (mostly) two boards to organise all stakeholders and to organise response capacities and the work on the policy on cyber security (DE, UK)
	IT infrastructure	- ensuring the information and communication infrastructure by help of technical arrangements, education, research, regulation and prosecution *(common)* - detailed measures: use of technologies certified by international standard (DE); provision of basic security functions certified by the state (DE, FI); improvement of risk management by guidance, information and training (FI, NL)
	Cyber attacks	- reinforcement of the response capacities by the development and usage of tools to detect, alert and react to cyber-attacks *(common)* - communication and information sharing among businesses to tackle cyber-attacks (FR,NL,UK, CZ)
	Administration	- train the staff *(common)* - installing a common, uniform and secure network infrastructure (DE, EE, FR) - establish standards for procurement requirements (FI, UK)
	Business	- development and implementation of an industrial strategy (FR, UK) - special support for SMEs by education and trainings and the offer of basic security technologies (EE, DE, FI) - vital infrastructure: obligation to report disruption and fall-out (NL), defining a minimum standard in the continuity of service (NL), supporting the use of measures to prevent digital espionage (NL) and the use of minimum security standards in ICT (EE, NL, UK)

	Education	- education of the citizens to increase their awareness of cyber-crime and cyber security and to improve their knowledge on the safe use of computers *(common)* - education and training of employees of the public as well as of the private sector *(common)* - starting campaigns (EE, NL) and offering trainings in schools and in universities (EE, FI, CZ) - establishment of common requirements for IT staff competence (EE)
	Research	- support research to develop expertise in cyber security, future technologies and to ensure national defence *(common)* - detailed measures: setting up a research program *(common),* support research by additional funding (UK), enhancement of international research cooperation (EE, UK)
	Law and Prosecution	- regulations for safeguarding the measures described in the strategies *(common)* - clarification of the responsibilities, rights and obligations of the concerned IT players (FI, UK, CZ) - evaluation and evolvement of the laws to meet technical developments (DE, FR, UK) - intensification of investigation and prosecution (DE, NL): establishment of an expert pool, establishment of a steering group for priority crimes, reorganisation of the police to have more specialists and Internet police monitors, increasing the number of specialists at the law enforcement agencies and the judiciary (NL)

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