An evaluation Framework for National Cyber Security Strategies

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (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.

ENISA project team

Dimitra Liveri, Resilience and CIIP Unit

Anna Sarri, Resilience and CIIP Unit

The project was conducted under contract with RAND Europe. Project team: Neil Robinson, Veronica Howarth, Nicole van der Meulen, Emma Harte, Minke van der Sar.

Contact

For questions related to this report or any other general inquiries about the resilience programme please use the following contact address: **resilience@enisa.europa.eu**

ISBN: 978-92-9204-109-0, DOI: 10.2824/3903

Executive summary

An increasing number of countries in Europe have a National Cyber Security Strategy (NCSS) as a key policy feature, helping them to tackle risks which have the potential to undermine the achievement of economic and social benefits from cyberspace. Eighteen European Union Member States have published a NCSS and some of these are now into the second iteration of their NCSS.

ENISA's work in supporting these strategies has focused on the analysis of existing NCSS; on the development and implementation of NCSS; and on outlining and raising awareness of good practice to provide guidance and practical tools to the Member States for evaluating their NCSS. Specifically, ENISA's 2012 Practical Guide on NCSS noted four important steps: the development, implementation, evaluation and adjustment of a NCSS.

The current study focuses on the evaluation aspect of the NCSS lifecycle, and has four goals, namely:

1. To perform a stocktaking exercise on the approaches currently used to perform evaluation of NCSS;
2. To present recommendations and identify good practices on the implementation and evaluation of NCSS;
3. To design and develop an evaluation framework;
4. To support the framework with a set of useful key performance indicators (KPIs) to adapt to the varying needs of countries at different levels of maturity in their strategic planning.

To accomplish these goals we analysed 18 existing EU National Cyber Security Strategies and eight non-EU strategies, conducted 11 key informant interviews and mapped out the components of NCSS. From reviewing and analysing the evaluation components of the NCSS, it was noted that many countries do not agree on the outcomes or impacts of their NCSS and on the ways to achieve them. Within Europe, the approach taken to evaluation differs largely among Member States. While almost all NCSS included in this study mention some elements of the review process, this was normally at a very high level and frequently orientated around spending reviews.

The core of this document is the description of an evaluation framework. This evaluation framework consists of the following elements: a blueprint logic model presenting conceptual building blocks and a structure and a list of possible key performance indicators (KPIs); This model illustrates the underlying logic behind recurring components of National Cyber Security Strategies, even though their own intervention logic may not be made explicit in the individual documents. It also serves as an illustration of a potential approach towards connecting the elements commonly contained within national strategies. The key objectives (that should be measured) of a cyber security strategy evaluation framework, based on the analysis are:

- To develop cyber defence policies and capabilities;
- To achieve cyber resilience;
- To reduce cybercrime;
- To support industry on cyber security;
- To secure critical information infrastructures.

The suggested KPIs are mapped to the objectives of the evaluation model, making it easier for each stakeholder to chooce the most useful (and measurable) key indicators according to their priorities. The report aims to be a flexible, pragmatic tool based on principles rather than prescriptive checklists.

Finally, we point out a number of pitfalls to avoid in the application of this guidance, including those relating to building capacity, securing budgetary support, achieving transparency and developing a lessons learned culture.

Table of Contents

1 Introduction

Cyberspace offers a significant opportunity for economic growth and social development. However, concerns about the security of this domain are becoming an increasingly pressing and salient issue. Senior business leaders and government officials placed cyber security risks as having a greater impact than those from terrorism when questioned by the World Economic Forum in 2013[1]. According to the European Commission's projections in the 2010 'Digital Agenda for Europe'[2] security is a high concern for 50% of EU citizens in order to engage in e-commerce and e-Government by 2015 and for around a third of Small to Medium Enterprises to offer online services. If citizens and business owners lack confidence in security, it stands to reason that they may avoid participating in online activities, thereby inhibiting further development opportunities on cyberspace.

To help address this, many European Union Member States have published or are in the process of publishing an NCSS. Of these, several (e.g., Czech Republic, Estonia, Netherlands and the United Kingdom) have also updated their strategies since their first edition. National Cyber Security Strategies aim to ensure that Member States are prepared to face serious risks, are aware of their consequences, and are equipped to appropriately respond to breaches in the network and information system. However, it is not always clear if and how the effectiveness of these strategies is evaluated. Evaluation can be interpreted as a tool to assess if and how well the expected objectives have been achieved and whether the costs involved were justified, given the changes which have been achieved[3].

The European Commission understands that "there are still gaps across the EU, notably in terms of national capabilities, coordination in cases of incidents spanning across borders, and in terms of private sector involvement and preparedness"[4]. The 2013 EU Cyber Security Strategy (EUCSS) asks ENISA to "encourage good practice in information and network security" to assist and support Member States in developing strong national cyber resilience capabilities, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure.

1.1 ENISA's activities in the area of NCSS

As already mentioned, National Cyber Security Strategies have not yet been established or implemented in all 28 Member States. Therefore, raising awareness of and promoting good practices in relation to cyber security among the EU Member States continues to be an important task to do in supporting national good practices.

In 2012, ENISA introduced the lifecycle of a NCSS in a practical guide on the development and execution phase of NCSS[5]. This Practical Guide highlights the fact that the ability to implement and evaluate the strategy is one of the two important steps governing NCSS (the other being the development and implementation of the strategy)[6].

[1] World Economic Forum (2013) Global Risks Report Eighth Edition; p4 Global Risks Landscape 2013 versus 2012; Zurich, Switzerland available at: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf

[2] Communication from the Commission of 19 May 2010 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 final]

[3] Communication of 2 October 2013 on "Strengthening the foundations of Smart Regulation – improving evaluation." [COM(2013)686]

[4] High Representative of the European Union for Foreign Affairs and Security Policy. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. JOIN(2013) 1 final - 7/2/2013. Available online at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[5] ENISA. (2012a). "National Cyber Security Strategies: Practical Guide on Development and Execution". December 2012. p. 7. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

[6] ENISA. (2012a).

To assist understanding of Member States' progress, ENISA has prepared an interactive map which shows how countries are developing and implementing NCSS[7].

1.2 Objectives

Given this context and ENISA's efforts to assist Member States in the design and implementation of NCSS, ENISA moved to the next phase and decided it was important to collate good practices in evaluation of NCSS. Therefore, the objectives of this project were:

1. To perform a stocktaking exercise on the approaches currently used to perform evaluation of NCSS;
2. To present recommendations and identify good practices on the evaluation of NCSS and to collect them in an evaluation framework;
3. To design a set of capacity building tools for evaluating NCSS that adapt to the varying needs of countries at different levels of maturity in their strategic planning.

1.3 Methodology

This project used a combination of three empirical techniques: 1) a literature review, 2) a documentation review of NCSS and 3) logic modelling – "a means to encourage systematic thinking about a programme" [8] - developed through internal interactions in the study team. Further information on the methodology can be found in (Annex B: Methodology).

1.4 Target audience

It is envisaged that policy practitioners, experts and government officials responsible for designing, implementing and evaluating an NCSS will find this report of use. In addition, it will be of value to cyber security policy experts and other practitioners and researchers at national, European and international level grappling with challenges of effectively managing cyber-security risks.

1.5 Structure

The remainder of this report is structured in the following way:

Chapter 2 discusses how the practice of evaluation can be applied to NCSS and why it is important to evaluate these policy instruments.

Chapter 3 presents empirical evidence on where and how evaluation has been included in the NCSS under analysis. This chapter summarises the landscape in the current practice of NCSS evaluation.

Chapter 4 describes a framework for evaluation of NCSS and elaborates on a roadmap for a NCSS evaluation by offering practical tips on:

1. The use of the consolidated logic model consistent with the headings of the EUCSS;
2. Possible key performance indicators (which would allow measuring progress against the objectives set out in the strategy);

Chapter 5 discusses some pitfalls to avoid for in the application of the guidance in Chapter 4.

Chapter 6 concludes the report.

[7] ENISA Interactive map on NCSS available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[8] Ling T and Villalba Van Dijk, V. (2009). Performance Audit Handbook: Routes to effective evaluation. Chapter 13: Logic Modelling. RAND Europe. TR-788-RE. RAND: Santa Monica

2 Benefits and challenges of evaluation of NCSS

Cybersecurity strategies present a few distinct challenges from an evaluation perspective such as need of investment on budget and resources, lack of good practices, difficulty to measure impact etc. However, evaluation going beyond financial audits (which are often already in practice due to legal obligations) can offer significant added value to the strategic planning and implementation of the policy on the medium- to long-term. The present guide, and this chapter in particular, look at the potential benefits of NCSS evaluation. Some of the delegated acts, such as legislation and implementation acts, which are foreseen by the strategies, may require their own impact assessments and evaluations for a consistent policy framework.

2.1 Benefits and challenges of NCSS Evaluation

Evaluation offers several benefits to the specific programme and has the potential to improve the wider policy environment by promoting evidence-based decisions. At the same time, implementing an evaluation approach and dealing with potentially controversial or unforeseen outcomes can present challenges. Table 1 below summarises these challenges and benefits based on the literature identified in our review[9].

Benefits	**Challenges**
a) Evaluation can inform about policy changes and the framing of issues in the long term; allow learning from past experience. b) Evidence of effectiveness or learning can support the accountability of political action. c) Evidence base can give credibility towards general public and international partners. d) Evaluation can support outreach and enhance public image as transparent organisation. e) Having facts on what works can help gain traction in policy process. f) Evaluation makes it necessary to compile data sources on policy and its implications for long-term planning. g) Catalyses discussion with stakeholders.	h) Evaluation needs investment of resources. i) Exposing flaws in policy can undermine political priorities even when the priorities themselves are supported. j) Good practices can be of limited use due to differences in national evaluation cultures. k) Outcomes are often challenging to define and measure. l) Attributing changes to the strategy itself can be difficult.

Table 1 Benefits and Challenges of NCSS Evaluation

[9] See e.g., Furubo, J. E. (2003). The Role of Evaluations in Political and Administrative Learning and the Role of Learning in Evaluation Praxis. OECD Journal on Budgeting, 3(3), 67-86; Knill, C. (1998). European policies: the impact of national administrative traditions. Journal of Public Policy, 18(1), 1-28; *Weiss, C.H. (1999). The interface between evaluation and public policy.Evaluation, 5(4), 468-486.*

2.2 Evaluation of cybersecurity strategies

2.2.1 Objectives in NCSS

The objectives of cyber security strategies reflect the differences in national contexts. However, there are some similarities between the European strategies. Cyber security strategies often have objectives articulated around the following clusters (Chapter 3), which are also reflected in the objectives of the European Cybersecurity Strategy[10]:

- To achieve cyber resilience: develop capabilities and cooperating efficiently within the public and private sector;
- To secure critical information infrastructures;
- To reduce cybercrime;
- To develop the industrial and technological resources for cybersecurity; and,
- To contribute to the establishment of an international cyberspace policy.

Within the national and international policy environment cyber security strategies have three further distinct purposes. As strategic documents, they serve to:

- Align the whole of government by defining strategic directions;
- Give a focus and a structure to discussions with stakeholders; and,
- Convey Member State priorities towards international partners[11].

2.2.2 Benefits and value of evaluation

Implementing evaluation frameworks can support reaching the objectives of NCSS in a variety of ways. Below we discuss two examples of this support[12].

Informing about policy change and supporting learning in the wider policy environment

One of the most important purposes of evaluation is that of informing affected stakeholders about policy change. In this case, the results of an evaluation serve to steer policy in subsequent review cycles. The evaluation shows which actions realised under the NCSS worked and helps policymakers learn from mistakes[13]. The feedback on the policy resulting from an evidence-based approach can help when using the cybersecurity strategies to drive discussion, prioritisation of objectives and funding decisions[14]. Evaluation is also an important instrument for gaining traction within the policymaking process. As such, evaluation results can help prove the legitimacy and credibility of interventions under the strategy (e.g., the necessity of allocating funds to a specific type of capability-building programme for fighting cybercrime) and increase the likelihood that CSS and the recommendations flowing from the evaluation have the appropriate attention in the policymaking process.

Engaging stakeholders

Evaluation processes can serve as a catalyst to engaging stakeholders in a discussion about moving the policy forward as well as offering a framework for engaging stakeholders during the

[10] High Representative of the European Union for Foreign Affairs and Security Policy. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. [JOIN(2013) 1 final] - 7/2/2013.

[11] Luijf, E. , Bessleing, K. & Graaf, P.D. (2013). Nineteen national cyber security strategies. *International journal of critical infrastructures*, 9, 3-3.

[12] Furubo, J. E. (2003). The Role of Evaluations in Political and Administrative Learning and the Role of Learning in Evaluation Praxis. OECD Journal on Budgeting, 3(3), 67-86.

[13] *Weiss, C.H. (1999). The interface between evaluation and public policy.Evaluation, 5(4), 468-486.*

[14] Luijf et al. (2013). Using evaluation for these purposes in the national context was considered particularly important by two of the interviewees.

implementation of the program[15]. For example, the data collection necessary to support the evaluation functions supports better overall availability of information on cybersecurity which can facilitate the provision of information to stakeholders. Similarly, providing data and an objective overview of the results of the policy can help focus discussions with stakeholders.

2.2.3 Challenges and limitations to evaluating NCSS

Difficulties in quantifying and measuring results

The nature of these outcomes is not easy to define and measure. Strategies often aim to improve confidence in doing business in the digital sphere, citizen/consumer trust in activities mediated by cyberspace. Indicators that would allow policymakers to capture progress towards these outcomes are often not readily available and can be challenging to construct in a reliable manner[16].

Reviews and assessments of NCSS in some countries have taken forms of financial or value-for-money audits in adherence to legal obligations. The US Government Accountability Office's GAO's review of the US cyber security strategy[17] and the UK National Audit Office's evaluation of the NCSS[18] are two examples of in-depth financial audits. Even in countries where specific financial audits are not published, government spending for implementing the NCSS is subject to the scrutiny of national audit bodies. Although these audits offer insights into certain aspects of the implementation, they serve different purposes than evaluation (that of verifying the correctness of financial statements, and assessing how economically, effectively and efficiently the funds are spent)[19].

From inputs to outcomes

The link between elements of the strategies and the explanation of how they support strategic outcomes is often difficult to establish without ambiguity. For instance, it is often challenging to assess what would have been the cyber security situation of the country if no action had been taken or in the case of different interventions. Similarly, even if the outcomes (e.g., increased trust in technology use by the population) are realised, it can be difficult to securely attribute them to the specific actions of the strategy (such as an awareness raising campaign).

Lack of evaluation culture

NCSS display the same diversity of approaches to incorporating evidence from evaluations. Despite the presence of good practices and implementation guides, implementation of evidence-based practices also depends on the institutional setup, administrative traditions and the "soft" characteristics of political systems, such as the national culture and traditions of transparency and accountability. Therefore, adapting practices to an evidence-based, evaluation-oriented cyber security policy framework may put considerable pressure on national administrative bodies, in particular in countries where evaluation practices have not been embedded in the administrative culture[20].

Implementing an evaluation culture in the field of cybersecurity also has to take into account the national contexts. Cyber security and digital policies in particular, form an area where robust and

[15] Luijf et al. (2013).

[16] Robinson, N. & Horvath, V. (2013). *Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts.* Report prepared for the European Parliament. Directorate General for Internal Policies. 2013.

[17] United States Government Accountability Office (GAO). (2009). *Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats- Statement on the evaluation of cybersecurity actions in the US.* GAO-10-230T United States Government Accountability Office GAO. (2011). Cybersecurity: *Continued Attention Needed to Protect Our Nation's Critical Infrastructure* GAO-11-865T: Published: Jul 26, 2011.

[18] National Audit Office. (2013). *The UK cyber security strategy: Landscape review.* London: The Stationery Office.

[19] Nothern Ireland UK Government Audit Office. (2014). Value for Money Standards available at: http://www.niauditoffice.gov.uk/index/about-niao/value_for_money_audit/vfm_standards.htm

[20] Knill, C. (1998). European policies: The impact of national administrative traditions. *Journal of Public Policy*, *18*(1), 1-28.

methodologically rigorous evaluations have not yet become the norm, even in countries with a more established track record in evaluation[21]. In addition, the configuration of the cyber security landscape varies greatly between Member States, which in turn reflects to some extent the constitutional setup of the country. This can for instance be illustrated by the establishment of computer emergency response teams (CERTs) in Europe. CERTs' presence, number and functions vary greatly between the Member States, according to a more or less centralised institutional system and assumptions about the role the new teams are supposed to play in implementing a secure cyberspace.

2.2.4 Evaluation in cyber security policy guidelines

ENISA's interest in facilitating evaluation and supporting strategic programming for NCSS fits into a larger picture of encouraging member states and EU institutions to incorporate evidence-based approaches in their cyber security strategies. In the European Union, these strategies are included in the "Digital Agenda for Europe" (DAE) and the proposal for a NIS Directive[22], which also links the purpose of the NCSS to the wider objectives of promoting an inclusive and secure digital society aimed to foster economic growth. Member States monitor the progress of cyber security in compliance with the relevant actions and submit monitoring reports on an annual basis. Based on these reports the European Commission (EC) compares the performance of Member States against the areas for action and objectives set up in the DAE.

The EU Cyber Security Strategy itself stresses the importance of establishing an "evidence-based risk assessment and management culture" within the cyber security community in the EU and the involvement of stakeholders in all its areas.

The most specific guidance on evaluation strategies in NCSS comes from ENISA's good practice guide on formulating strategies[23]. The strategy lifecycle model is illustrated in 1 below. As the figure indicates, the evaluation activities refer to both one-off evaluations and on-going/periodical evaluation.

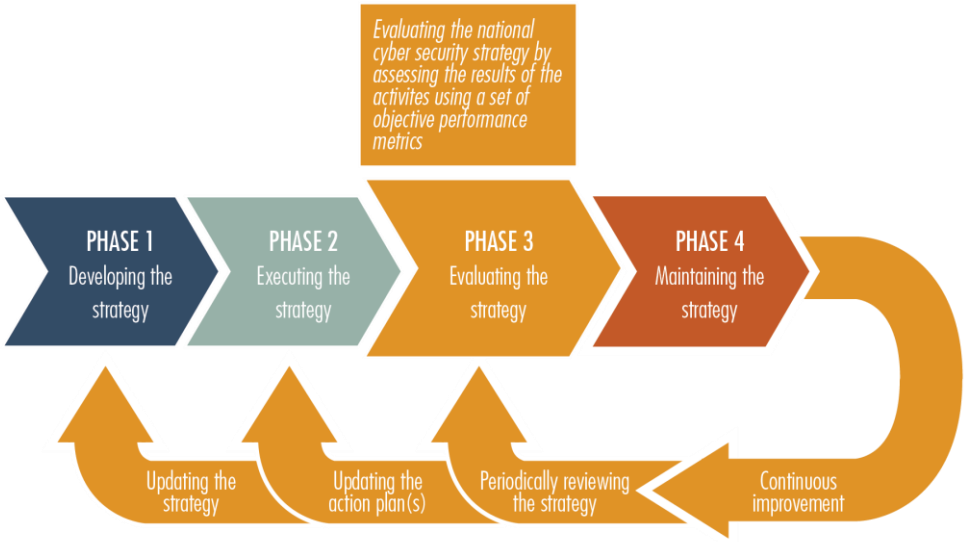

Figure 1 Lifecycle of a national cybersecurity strategy (Source: ENISA, 2012)

[21] Leeuw, F.L., & Leeuw, B. (2012).

[22] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

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

In recent years a number of international organisations emphasised the importance of evaluation in cyber security policymaking, such as the International Telecommunications Union (ITU) in its guidelines on implementing cyber security strategies[24]. The ITU guidance emphasises the importance of SMART objective-setting, the definition of timelines and the adoption of a review mechanism for the framework itself. It also offers a long list of suggested KPIs based on international standards and network and information security indicators or the NATO NCSS framework manual[25]. In the NATO guidance document, evaluation is presented as an instrument to progressively incorporate learning from previous experiences into the policy framework in the light of technological and social change, without weighing down the systems and processes.

Similarly, the Organisation for Economic Co-operation and Development's (OECD) analysis of NCSS published in the past five years has found that these strategies share a number of characteristics[26]. Shared aspects (which could be relevant for evaluation initiatives) include multidisciplinarity, a view encompassing the entirety of society, and a trend towards sharing fundamental assumptions, such as those that cyber threats are increasing and that ICTs are essential for social development. Interestingly, a call for rigorous evaluation processes, risk assessments and data-based planning was made by stakeholders from the communications industry in the consultation process underpinning the research for the report[27].

[24] Wamala, Frederick. (2011). *ITU National Cybersecurity Strategy Guide*. International Telecommunications Union.
[25] Klimburg, Alexander (Ed.). (2012). *National Cyber Security Framework Manual*. NATO CCD COE Publication. Tallinn 2012.
[26] OECD. (2012). *Cybersecurity Policy making at a turning point: Analysing a new generation of national cybersecurity strategies for the Internet economy*. Annex I. OECD.
[27] OECD. (2012).

3 Mapping cyber security strategies to evaluation objectives

As pointed out in the previous chapter, incorporating evaluation in the design and implementation of NCSS can offer significant opportunities for realising the objectives of the strategy. In this chapter, we will survey the current state of evaluation-related aspects in a series of cyber security strategies in Europe and beyond. Moreover, we will look at the contextual factors that can influence the way in which strategies are set up and implemented. This aspect is particularly relevant for the EU due to differences in the institutional setup and administrative cultures of the Member States; it is not optimal to aim at identifying a one-size-fits-all approach to good practices in incorporating evaluation in NCSS. Rather, the evidence-based approaches should be considered according to the particular context of the country. Therefore, the evaluation framework that the present study is supporting will adopt a model that is flexible enough to accomodate these differences.

3.1 Overview of the mapping exercise

One of the goals of the present study is to analyse the approaches taken by European cyber security strategies, with a view towards a NCSS evaluation framework. The first step of the review has been to identify the elements that can be used as part of an evaluation framework based on logic modelling and programme theory. These include Objectives (and focal areas of action), Inputs, Activities, Outputs,Outcomes and Impacts[28].

A review of 18 EU strategies included in the exercise has identified and extracted elements that correspond to each of these categories in the documents. Furthermore, some categories that relate to the specific purpose of the study in assisting Member States in updating, implementing or drafting a strategy, have been added. These summarise provisions related to stakeholder involvement and the review processes.

For the purposes of visual simplification, the maps included do not aim to illustrate the entirety of the elements included in the strategies, but rather to illustrate the multiplicity of approaches across the EU. In the remainder of this section we present a short summary of the analysis based on the mapping[29].

The mapping exercise doesn't aim to compare the countries to a benchmark; rather, to explore the starting point for Member States in implementing and/or enhancing the evaluation aspects of their strategies. Where evaluation exists, it is often limited to spending reviews, although some countries are attempting to approach the effectiveness of expenditure through cost-benefit analysis. From the results of the mapping presented below it emerges that an internal intervention logic is not immediately clear from NCSS and it would have to be reconstructed for the evaluation purpose.

Overall, our review has found that most NCSS articulate objectives and outcomes in broad socioeconomic terms. Action areas, available and projected resources and the processes that need to be put into place while implementing the strategy are often not clearly defined. Outputs are often easier to identify in the strategies; however, their relationship to the objectives is often not clearly

[28] Summary of the terms (see e.g. Kellogg Foundation (2009): The **objectives** of a program relate to the short and long term goals of the strategy which will usually be met by targeted actions and processes. **Inputs** are the resources needed to operate the program (including human resources, financial resources but also others such as facilities and equipment). **Activities** are the actions or clusters of actions that are needed to implement the program. **Outputs** are the direct product of programme activities and are typically tangible and quantifiable. **Outcomes** are the intended and unintended results that are linked to programme objectives. They answer the question "What happened as a result of the programme?" Typically, they can be categorised into short-medium and longer term outcomes. **Impacts** are the fundamental direct and indirect effects of programme activities (on a 7-10 year period) on the wider environment. These include socioeconomic, financial and political effects.

[29] Please note, references to the countries in this chapter always refer to the cybersecurity strategy of the country, which can be found in the References section of the present report.

defined. Although these aspects may be captured in implementation guides, the programmatic approach and agenda-setting that is often the goal of the adoption of the NCSS could be better supported by clearly articulated lines of casuality and intervention logic.

3.1.1 Objectives

The objectives of any NCSS will relate to the short and long term goals of the strategy which will usually be met by targeted actions and processes. While they may be related to the overall outcomes they are usually be more focused and come about as a direct result of an action. However, some objectives as set out in the NCSS are rather generic by stating that a nation can secure their vital functions against cyber threats.

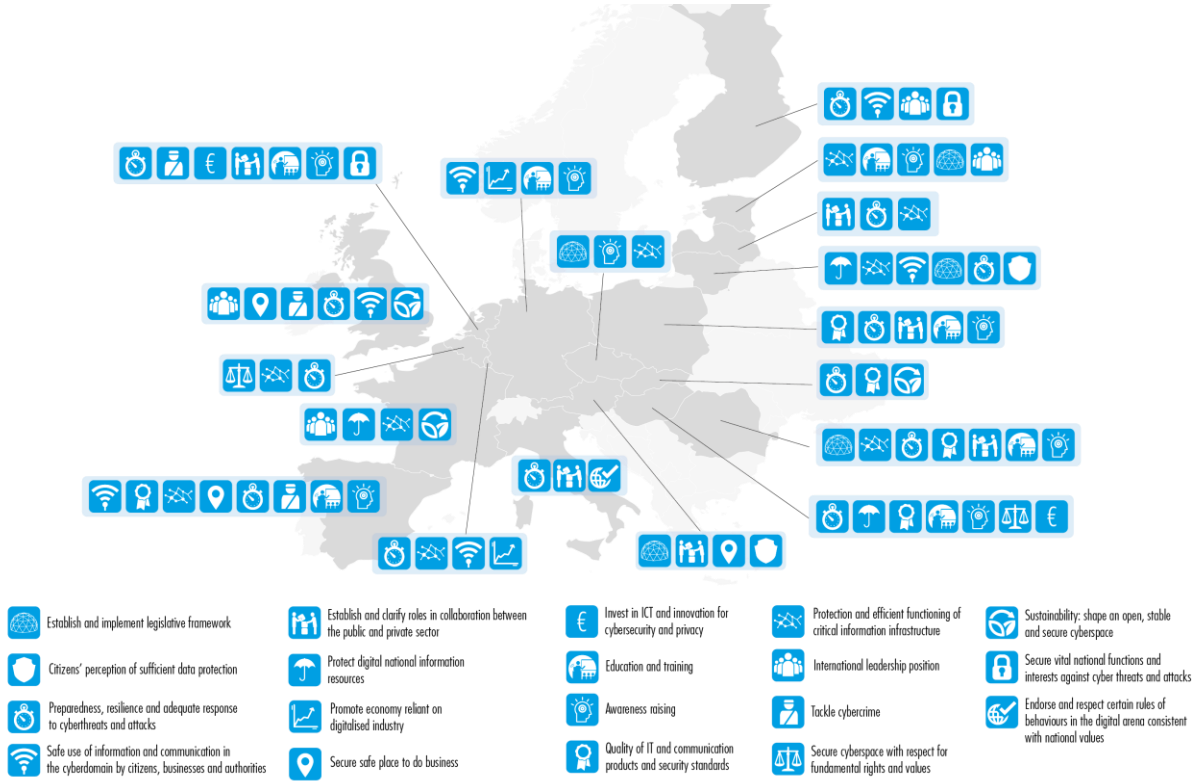

Figure 2 Examples of objectives in NCSS in the EU

The **objectives** as mapped are:

- Establish and implement legislative framework;
- Establish and clarify roles in collaboration between the public and private sector;
- Invest in ICT and innovation for cybersecurity and privacy;
- Protection and efficient functioning of critical information infrastructure;
- Sustainability: shape an open, stable an secure cyberspace;
- Citizens' perception of sufficient data protection ;
- Protect digital national information resources;
- Education and training;
- International leadership position;
- Secure vital national functions and interests against cyber threats and attacks;
- Preparedness, resilience and adequate response to cyberthreats and attacks;
- Promote economy reliant on digitalized industry;

- Awareness raising;
- Tackle cybercrime;
- Endorse and respect certain rules of behaviours in the digital arena consistent with national values;
- Safe use of information and communication in cyberdomain by citizens, business and authorities;
- Secure and safe place to do business;
- Quality of IT and communication products and security standards
- Secure cyber space with respect to fundamental rights and values

While not always the case, many objectives can be measured by defining success indicators and are usually complemented by subsequent projected actions. As illustrated in the map, some of these objectives are shared by a large number of countries (e.g. capability building, the revision of legal frameworks or international cooperation), while others, such as striking a balance between human rights and cybersecurity in legislation, are particular to the Member State. Poland, for instance, wishes to increase the level of security within its ICT infrastructure which could be achieved through running risk assessments and enabling the security of government internet portals. A number of other objectives relate to tackling cyber crime (Netherlands, UK), strengthening or protecting critical infrastructure (France, Romania, Belgium and others), building up a skills base in ICT or e-skills (UK, Netherlands, and others) and enhancing safety standards (Hungary). Some NCSS mention defence objectives by sharing their desire to become a world power in the area of cyber defence (France)[30].

3.1.2 Specific objectives

Programme-level objectives, which tend to be defined at a high level, are often broken down into focal areas of action. The distinction between the objectives and the areas of action serves as an opportunity to present the transversal areas of government and stakeholder activity that need to be coordinated to realise the outputs and outcomes of the strategy. For instance, an objective of international leadership in cyber security markets needs action to be taken at the level of the legislative framework as well as in interactions with the stakeholders. The presentation of specific objectives can support the theory of change and these could serve as a clear vehicle to connect broad objectives with individual actions.

The areas are various: published EU strategies tend to frame these in a broader sense and encompass socioeconomic areas (such as training and promoting a business environment) and put emphasis on international cooperation. Overall, from the mapping it appears that the activity areas show similarity across EU Member States. Some of these, such as critical infrastructure protection or risk assessments occur in a large number of Member States, while others, such as standardisation or capability building in the private sector are more rare.

In a number of the reviewed strategies these areas of action reflect transversal areas where action needs to be taken to reach the objectives (e.g., in the case of Austria or France). In some cases, the areas of action and the objectives of the strategy are not separated (Lithuania). Finland, for instance lists a set of areas that are linked to the implementation process of the strategy i.e. putting into place a review structure for the strategy and defining the division of tasks across stakeholders, and others that are more outcome-related, i.e. improve the resilience of all societal actors.

In a nutshel, the main action points are:

- Develop standards and norms, legislation;

[30] In other Member States military cyberdefence objectives are covered in separate strategic documents which were outside the scope of the present work.

- Enhance strategic collaboration between autorities, business and academicia;
- Invest on international cooperation;
- Protect critical information infrastructure;
- Create a culture of security: inform, educate and raise awareness;
- Research, development and innovation;
- Security of services delivered in cyberspace;
- Support competence and capabilities building in involved actors;
- Counter national and international criminal activities;
- Perform threat tracking, risk assessment and response.

Figure 3 Examples of specific objectives indicated in EU NCSS

3.1.3 Inputs

Inputs indicate the resources that are made available for the implementation of the NCSS at both strategy and programme level, originated from the specific objectives of the NCSS. These include financial, human and relational resources, among others. Only some of the NCSS reviewed for this study listed financial resources among the inputs (examples include the UK, or the projected budgets included in the Slovak strategy). Based on the interviews, it appears as though, at least in a few European Member States, there is not a central funding scheme for the implementation of the strategy. The budget for implementation is part of a departmental or institutional budget. Another approach would be to introduce a national separate budget line for the NCSS, once drafting of the strategy is complete. Acknowledging the need for a dedicated cyber security budget line within budgets could be an important instrument of supporting cyber security policy actions. This view is indirectly supported by the perspective that financial support for the implementation is quite weak since it relies on existing departmental budgets, as observed by another interviewee.

Other often-cited resources include cyber security tools (such as information security tools for the systems of public administrations), educational resources and incentives (such as tax breaks or

procurement rules) for producing safe systems. Several of the documents concentrate on leveraging legal resources to pursue the objectives of the strategy and align it to European and international good practice. Standards are also an important tool in promoting secure practices. In many cases, outputs and inputs interact in a circular manner (the outputs of one action serve as inputs to realising subsequent actions). This is the case for instance of the resources involved in establishing new centres that later exercise function in Critical Information Infrastructure Protection (CIIP) or fight against cybercrime (Luxembourg, Finland). Planned evaluation frameworks will need to find a way to capture this circularity.

Figure 4 Examples of input indicators in EU NCSS

The input indicators:

- Legislative measures;
- Increasing law enforcement and judiciary capabilities;
- Participation in international and regional cooperation;
- Establish/improve processes and coordinating structures;
- Tools and organisational components;
- Support research and development;
- Introduce CS in curicula of education system;
- Feasbility study on separate public and private vital network;
- Incentives and funding for initiatives supporting secure systems;
- Guidelines and internal information on information security.

3.1.4 Activities

Activities are the core interventions through which the outputs and outcomes of the project are pursued. It is fundamental that they are defined in a way that encompasses all inputs and the projected outcomes. At the national level the activities are often described and periodically updated

through the implementation plans of the national strategies, which in turn are usually not published. The country's legislative framework provides for many of the activities (e.g. those involved in creating and revising new legislation). In some cases, such as the UK, where centralised funding is available, central government bodies are more heavily involved in defining the activities. However, in countries with more decentralised systems and where cyber security activities are financed out of the standing budget lines of the entities involved, such as the Netherlands, activities are sometimes designed by the departments themselves.

Capacity building, legislative reviews and assessments of risks and threats are examples of procedural activity which many strategies incorporate (e.g. Spain and the Netherlands). Furthermore, awareness-raising activities are mentioned by all reviewed strategies. Where available, the activities rarely cover all objectives specified in the strategy. Overall, activities are not discussed in detail in the strategies to be identifiable and allow mapping.

3.1.5 Outputs

Outputs are the direct results of programme activities. These are usually linked to key performance indicators as they are relatively easy to measure quantitatively and qualitatively, and can be audited to ensure sound financial management of implementation activities; individual policy units have greater control over outputs or activities than outcomes or impacts. Therefore, outputs form the backbone of separate implementation reports linked to cyber security frameworks and, as a result, they are covered in the main body of the national strategy to a limited extent. Where mentioned, they tend to not be linked to the specific areas of action and scattered throughout the document. Examples of outputs include implementation plans (Lithuania, Slovakia), the legislative frameworks foreseen by the strategy (Czech Republic, Poland, Hungary), the units or task forces that are supposed to be established and the products of the periodic review processes (Slovakia and UK).

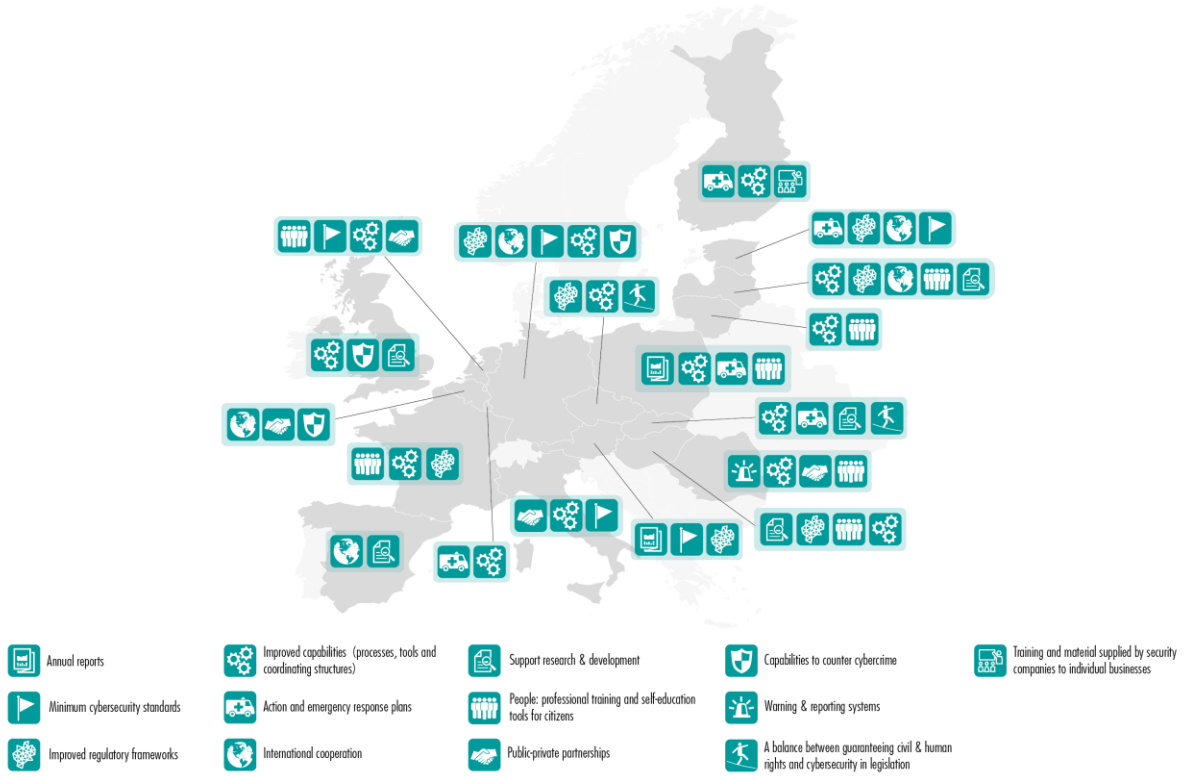

Figure 5 Examples of outputs in EU NCSS

Usual outputs:

- Annual reports;
- Minimum cybersecurity standards;
- Improved regulatory frameworks;
- Improved capabilities (processes, tools and coordinating structures);
- Actions and emergency response plans;
- International cooperation;
- Support research and development (actual investment);
- people: professional training and self-education tools for citizens;
- public private partnership;
- capabilities to counter cybercrime;
- warning and reposting systems;
- Civil and human right in cybersecurity;
- Training and material supplied by security companies to individual business.

Evaluation planning needs to ensure that outputs are linked to outcomes and long-term impact of the programme. Moreover, as several outputs also serve as inputs to subsequent stages of implementation, these relationships need to be reflected in evaluation frameworks.

3.1.6 Outcomes and impacts

Outcomes reflect the short and medium-term results of the programme, while impacts represent the longer term (e.g. 10+ years) results, which are also more broadly defined and take place at the social level. They are usually situated in context with the objectives and the areas of action: for instance, short and medium-term outcomes are incremental changes in resilience and collaboration which directly flow from the activities envisaged in the strategy. Impacts are long-term goals relating to the security of cyberspace as a result of the outcomes realised by the programme in the short- and medium-term. Although this is an important distinction between the types of results that a programme can generate, NCSS reviewed for this study did not distinguish between foreseen outcomes and impacts. Therefore, Figure 6 lists outcomes and impacts together.

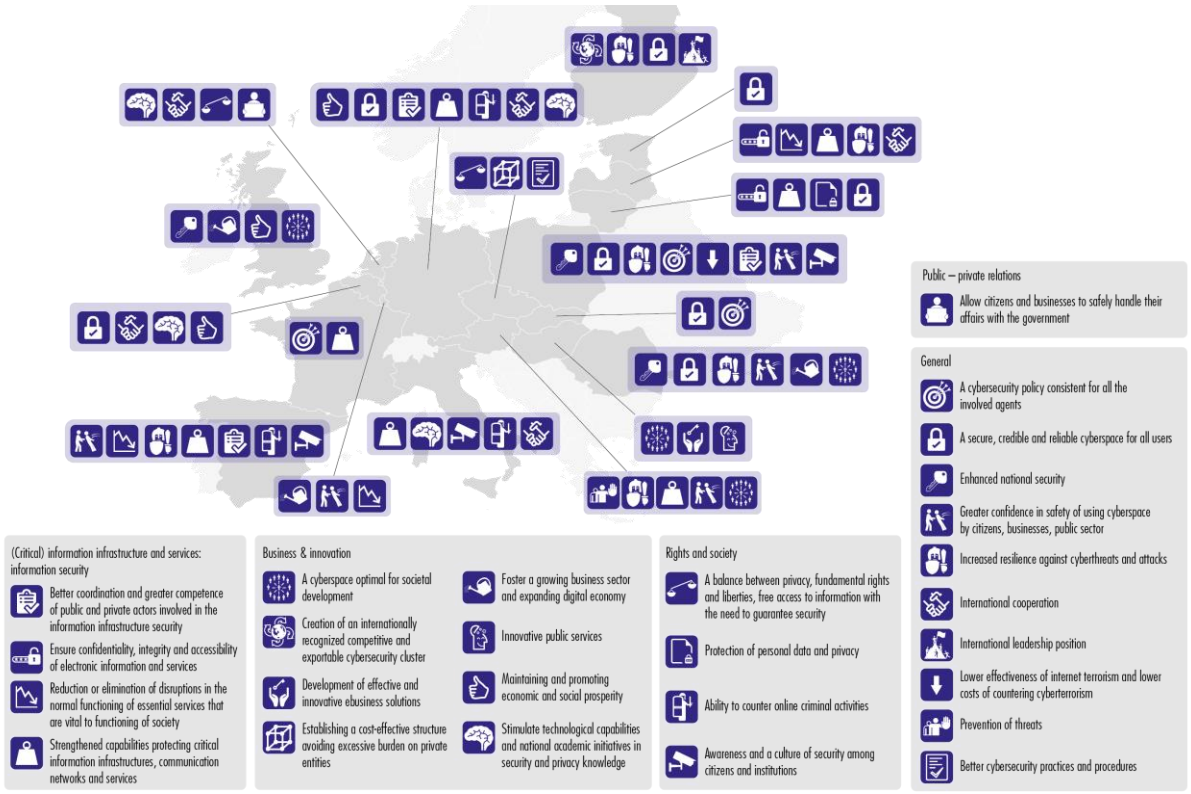

Figure 6 Examples of outcomes in EU NCSS

There are varying projected outcomes and impacts both among the NCSS and within them, the most common of which is to create a safe or secure online environment (France, Romania, Hungary, Belgium and UK). Some NCSS envisage outcomes in wider terms. For example, Estonia wishes to reduce cyberspace vulnerabilities within the nation while the Netherlands expects the Dutch society to understand the safe utilisation of cyberspace as a result of awareness raising on cyber security risks. This study also uncovered a number of desired outcomes relating to the protection of critical infrastructures (Italy), helping businesses to continue their work (UK), preserving their national security (UK, Austria, Romania), protecting individual rights (Czech Republic) and enabling international cooperation (Belgium and Italy).

Since many of these outcomes are defined in complex socioeconomic terms, their measurement can be challenging. However, it is possible to quantify some of the outcomes in terms of a KPI, and set up appropriate measurement methods through the European or national statistics offices. Examples of such indicators are: surveying public trust in online transactions and the level of internationalisation of web commerce. Several such indicators are already monitored at the EU level, allowing a broad grasp of the quality of cyber security, despite the fact that there are methodological limitations to the establishment of cause-consequence relationships between digital strategies and this kind of society-level outcome[31]. Other potential measures (such as the number of breaches and attacks taking place in the country) are often much more challenging to efficiently measure and frame as an outcome of national-level cyber programmes[32].

[31] See e.g., Eurobarometer. (2013). Special report on Cybersecurity, Eurobarometer 404.
[32] See e.g., Robinson and Horvath. (2013).

3.1.7 Evaluation processes

Almost all NCSS reviewed within the scope of the study include provisions on a review and evaluation process for the document (exceptions include e.g., Hungary and Spain). In Finland, ensuring a review and evaluation of the strategy is one of the ten strategic areas of action. In other strategies (UK, Germany, France) the evaluation also serves the purpose of keeping the legislative framework up-to-date with regards to recent developments in the technology landscape. In several strategies, the frequency of the evaluation cycle is established at a yearly (Lithuania, Slovakia, Netherlands) or biannual (Austria) frequency. In all NCSS, however, the details of the evaluation process are included in a separate act or in the implementation plan. Even where the review processes are not specified in the NCSS, the delegated acts and actions foreseen by them are subject to the scrutiny of public audit bodies, depending on the institutional setup of the country. In other strategies the actors involved are also specified (Austria, Estonia, Germany). The review mechanisms that are discussed cover both the programme-level evaluations (i.e. a review on the process of realising the actions foreseen by the framework) and effective reviews on reaching the proposed objectives and outcomes of the strategy. Furthermore, they also extend to reviews at the level of individual projects under the cyber security framework. In Italy, for instance, education and on-the-job cyber security training programmes, two of the action areas of the strategy, are specifically mentioned as being subject to review.

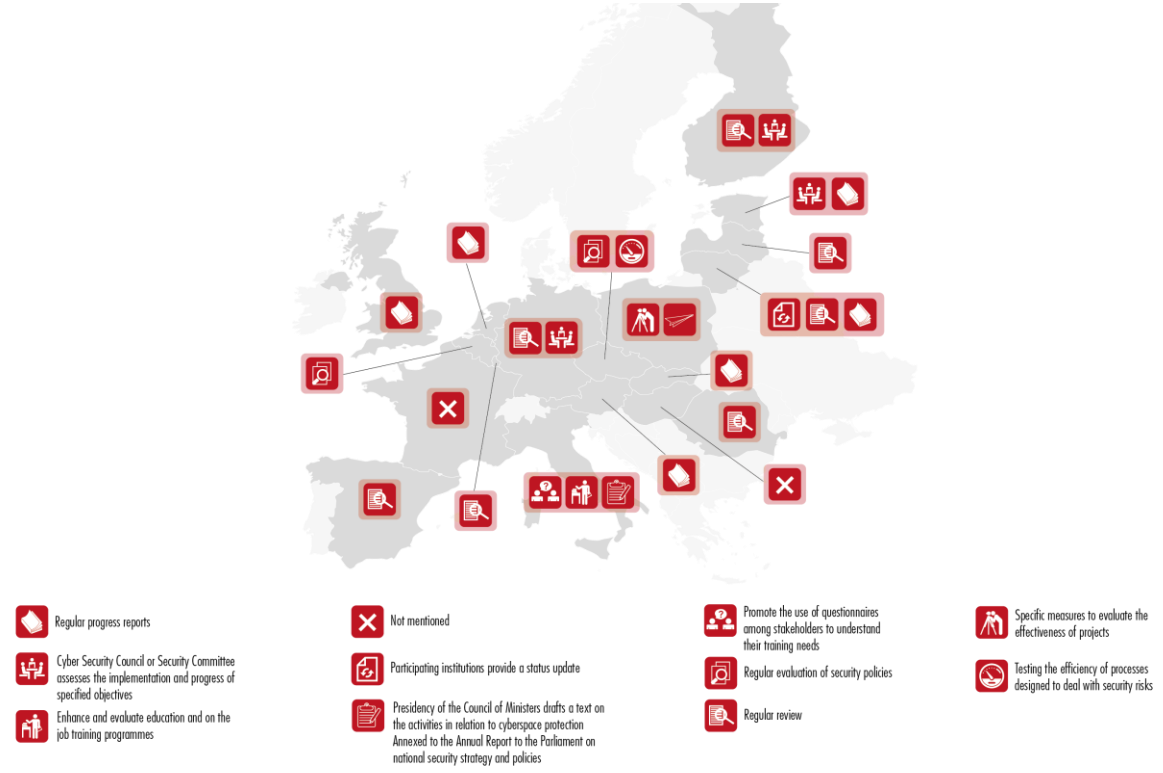

Figure 7 Examples of evaluation processes in EU NCSS

Some evaluation approaches:

- Regular progress reports;
- Cyber Security Council or Security Committee assesses the implementation and progress of specified objectives;
- Participating institutions provide an update;

- Presidency of the council of ministers drafts a text on the activities in relation to cyberspace protection (annexed to annual report to the parliament on national security strategy and policies);
- Promote the use of questionnaires among stakeholders to understand the training needs;
- Regular evaluation of security policies;
- Regular review;
- Specific measures to evaluate the effectiveness of projects;
- Testing the efficiency of processes designed to deal with security risks.

Overall, the description of the evaluation process tends to prioritised in the NCSS. In addition, documents describing the methodologies that are applied to evaluation are often not accessible to the public. As a consequence, the approach taken to define evaluation benchmarks and criteria is difficult to gauge from a review of the strategy itself.

With respect to the entity responsible for the evaluation, the guidelines provided by ENISA with regards to carrying out an evaluation of an NCSS prescribe the identification of an independent entity to ensure segregation of duties. In certain Member States, a National Cyber Security Council is responsible for the evaluation of the implementation of the strategy. In other Member States, the government auditing body is responsible for the evaluation. Either way, this is an important indication that the entity responsible for the evaluation is independent of the entity responsible of the execution of the strategy in order to guarantee an impartial evaluation.

3.1.7.1 Computer Emergency Response Teams - CERTs

In the evaluation process in the majority of the cases CERTs play a vital role. CERTs, due to their critical placement with respect to incident response, can provide unique input about cyber security progress. In one Member State, for example, the monitoring of KPIs depends on the National CERT since the team is responsible for measuring information security. A similar structure is available in the Netherlands, where the National Cyber Security Centre, which includes the CERT capacity for the Dutch government, leads the Cyber Security Assessment, which is published several times per year. CERTs have overview on a number of aspects which can feed into KPIs, such as number of advisories about vulnerabilities, as well as potential malware infections and developments, and, as previously mentioned, cyber security incidents. Particularly, the latter could be an indicator that CERTs could contribute to measure the level of information security across various years. This is, however, subject to a number of other influential variables, such as a potential increase in sophistication due to the introduction of breach notification obligations across different sectors.

An important issue that must be taken into account when considering the involvement of CERTs in the evaluation process is the sharp contrast between their usual informal working practices, which rely on a trust model among an informal network of contacts and the professionalisation and formalisation of the cyber security landscape. The right balance should maintain the benefits of the informal manner of working in CERTs. This is particularly important as the landscape evolved and CERTs became part of a National Cyber Security Centre, as occurred in, for example, the Netherlands. One interviewee noted how the questions related to CERTs should also focus on National Cyber Security Centres. This is probably due to the close connection between the roles of National Cyber Security Centres and CERTs.

3.1.7.2 Critical Infrastructure Protection (CIP)

Critical infrastructure protection deserves special attention when discussing cyber security in general as well as government strategies. This is due to two factors. First, critical infrastructure concerns the protection of vital services for society to function and, as such, receives a higher priority and often more stringent security requirements due to their sensitive or delicate nature. Therefore, the mapping

and identifying of services to be part of CIP is essential. One Member State interviewed used a variety of indicators, including legal definitions, but also the potential impact of an interruption measured through how many people would be affected within a given timeframe, including a potential number of casualties in the event that services became unavailabe. These metrics assisted in the mapping and idenfitication of vital services.

The second factor concerns the lack of direct government control in the majority of Member States over the critical infrastructure sector, since most critical infrastructure are in the hands of private actors. In one Member State, CIP was dealt with in a separate document, which focused more on crisis management. In other Member States, CIP was a key area of action or a key objective included in the strategy. For one Member State, the separate department responsible for CIP provided a yearly report on the progress made in the area. As such, CIP may and can be hosted elsewhere in the governmental landscape but still maintains a connection to cyber security evaluation.

3.1.7.3 National regulatory authorities

Even though not all the national regulatory authorities (NRA) have a mandate on cyber security, their role remains important in the improvement of resilience at the national level. Starting with the implementation of incident reporting in the telecoms sector (Article 13a of the Telecoms Act[33]) or the data breach notification (Article 4 of the Privacy Directive[34]), the NRAs are becoming the national hub of information on cyber incidents. In the proposed NIS Directive[35], in which the incident reporting provision would apply to the critical sectors (energy, water, transport, health, finance etc), the NRAs have again an important role. It is evident that their responsibilities will increase turning them into an important actor also in the evaluation of the national strategy as they will have all indications to measure the level of resilience and cyber security in the different sectors in a national level.

3.2 Stakeholder involvement

Given the borderless nature of cyberspace, all that use it are stakeholders by default. Some NCSS call for participation of the private sector on a taskforce (Netherlands, SMEs in Germany), the establishment of working groups for sectorial issues (Spain, Czech Republic) or public-private partnerships[36] (Italy). A couple of interviewees noted how stakeholders also play a key role in the review process, especially during consultation sessions. For others, the private sector receives a more prominent role due to external developments such as the proposed NIS Directive. Since the NIS Directive is perceived to have a significant impact on the cyber security landscape, the public sector is presently involved in an ongoing public discussion on the Directive. As a result, private sector stakeholders are presently very involved on a practical level. Once roles and approaches are defined it is then key to determine the directional nature of ensuring stakeholder involvement: do stakeholders have almost equal contribution to defining actions (horizontal structure) or is one stakeholder more authoritative than the other (top-down structure)?

Finland, for example, follows a top-down approach whereby the state outlines roles and approaches applicable to different groups operating within society. The UK appears to have a more horizontal structure in which it allows for the private sector to seek business-driven solutions and Slovakia calls on the private sector to contribute financial resources. Each case utilises the public-private partnership in different ways. In the UK and Slovakia, the private sector contributes substantial resources

[33] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting
[34] http://ec.europa.eu/justice/data-protection/
[35] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf
[36] Public private partnerships or PPPs are important scheme for information sharing (like ISACs etc) ENISA has been working on the topics offering an overview of the EU PPPs currently developed http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps (to be updated in 2014)

(expertise, use of its infrastructure, finance) and the Finnish private sector takes its lead from the state.

The added value of the development of a national strategy has been often found by interviewees to include externalities such as the potential of the framework created to encourage dialogue between levels of government and different stakeholders. For instance, the cooperation between levels of government can take the form of periodical reports to Parliament by the organisation responsible for overseeing the implementation of the strategy, on a yearly or biannual basis (UK, Austria). Such network-building processes are further reinforced by the multidisciplinary nature of cyber security, central funding where applicable and the consequent need for government departments and stakeholder organisations to act in a coordinated manner. This is an aspect that, while often contributing to the setup of policymaking processes, is frequently not captured in the evaluation of the strategy. Review mechanisms must be tailored specifically to each case in both the evaluation of stakeholders and involving stakeholders, ensuring the highest level of transparency. According to the findings of a preliminary scoping study conducted for the present study, the value of stakeholder involvement is often absent from evaluations.

Figure 8 Examples of stakeholder involvement mechanisms in EU NCSS

Several NCSS which discuss mechanisms for the review or evaluation concentrate on practices involving releasing reports (Estonia, Netherlands, Austria, Lithuania and Slovakia). However not all of these include a clear definition of their measures for success or how they are to obtain the information required to successfully evaluate stakeholders. Focus groups (working groups, taskforces, etc.) envisaged under the strategy would guarantee a certain level of evaluation of self-examination, yet it is unclear as to how these will be operated.

In collaborating with the government or competent authority for the implementation of a cyber security strategy, stakeholders are investing in their interests (commercial, personal, data related, etc.). It is important that stakeholders understand their responsibilities and what is required of them.

The role of each stakeholder differs depending on their capacities and their resources. For example, Slovakia expects the private sector to fund some activities within the paradigm of cyber security and the UK looks to business driven solutions to the cyber security question. The Italian state assumes responsibility as one of the key stakeholders but invites the private sector to collaborate as they also have a lot to gain from a secure cyberspace. The majority of other NCSS rely on the public and private sector and individuals to work on implementing some activities within their strategies while other countries, such as Japan, call more specifically on those controlling critical infrastructure to play a part in securing their interests. Individuals, for their part, are expected to become aware of threats and vulnerabilities across the board and responsibility can then fall to the government to conduct awareness raising campaigns and promote educational programmes.

	Area of action	Coordination of activities
Individual users	▪ Education and training. ▪ Building trust in law enforcement.	- Integration of innovation, technology and cyberspace and security teaching into school curricula (Italy) or into scientific and technical training (France). - Self-learning opportunities on cyber security website (Lithuania).
Business/private sector	▪ Public-private partnerships. ▪ Education. ▪ Investment in creating a secure cyber environment.	- Creation of consultation groups/taskforce (Netherlands) and working groups for sectorial issues (Czech Republic). - Collaboration with the public sector on processes and structures for political coordination (Austria). - Protecting SMEs through sector specific platforms in developing cyber security in relation to businesses (Austria). - Investing financial resources (UK) and other resources such as expertise, training capabilities, etc.
Critical infrastructure	▪ Building a robust critical infrastructure. ▪ Partnerships with other sectors.	- Testing critical infrastructures (Estonia). - Cross-sectorial collaboration - Information sharing within the industry (Netherlands).
CERT	▪ Collaboration with the public and private sector. ▪ Building a CERT network.	- Establishment of CERT entities in the public and private sector (Romania).
Public bodies	▪ Awareness raising campaigns. ▪ Education and training. ▪ Establish a culture of cyber security and resilience.	- Creation of training programmes and outreach activities (Lithuania). - Establishment of minimum standards of security (Austria, Czech Republic, Romania).

Table 2 Examples of stakeholder involvement in NCSS in the EU

4 Evaluation Framework for NCSS

As earlier chapters have shown, the approach taken to the evaluation of NCSS differs largely among European Member States. From several interviews it also transpired that the policy departments that are responsible for overseeing the implementation of the programme are often not utilising systematic program-level evaluation frameworks. This part of the deliverable presents elements of a framework for national cyber security strategies, describing three tools that could help Member States enhance their programme-level evaluation work[37]. The framework has been designed drawing on the insights gained through the systematic review of existing cyber security strategies, interviews with Member States, feedback from Member States on the draft logic model, and academic and grey literature on policy evaluation. It also draws on the principles listed in Chapter 3 of the 2012 ENISA guide on cyber security[38].

The proposed evaluation framework consists of the following elements:

a) A blueprint logic model presenting conceptual building blocks and a structure;

b) A list of possible key performance indicators (KPIs);

While the present chapter offers a brief overview on the suggested tools, it is by no means a comprehensive guide to their implementation. Annex B offers further resources for policymakers wishing to know more about the details of these approaches and detailed advice on applying them. In this section we provide a short summary of the methodologies included in the evaluation framework and the rationale behind their inclusion. Depending on the legal obligations and review practices which are currently in place in the individual Member States, the policymakers responsible for the NCSS may benefit from drawing on some or all of these tools in planning and understanding the impact of their activities.

4.1 Logic Modelling

Logic modelling is an evaluation tool which is useful to deploy in order to understand the logic of the NCSS and its implementation. In brief, Logic Modelling permits the mapping of all the different ingredients of the initiative. Given the complexity of cross organisational strategies like NCSS, a degree of simplification is necessary to apply in order to show the connections between the different elements. A Logic Model associated with a programme must be kept updated to ensure that it is relevant to the programme as time progresses. Reference information on Logic Modelling can be found in annex B.

Based on the review of the national strategies as well as the literature and an internal working session, we have identified the elements that are present in the reviewed strategies and the policy and academic literature. Subsequently, we mapped these components out in a comprehensive logic model that reflects the architecture of the EU Cyber Security Strategy. The following figures illustrate the outcomes of this exercise. These models illustrate the underlying logic behind recurring components of national cyber security strategies, even though their own intervention logic may not be made explicit in the individual documents.

[37] While below we present a compendium of tools, a complete evaluation framework would have to rely on a conceptual framework that defines how these tools are applied in the national context and how the results of these exercises are interpreted.
[38] ENISA. (2012b).

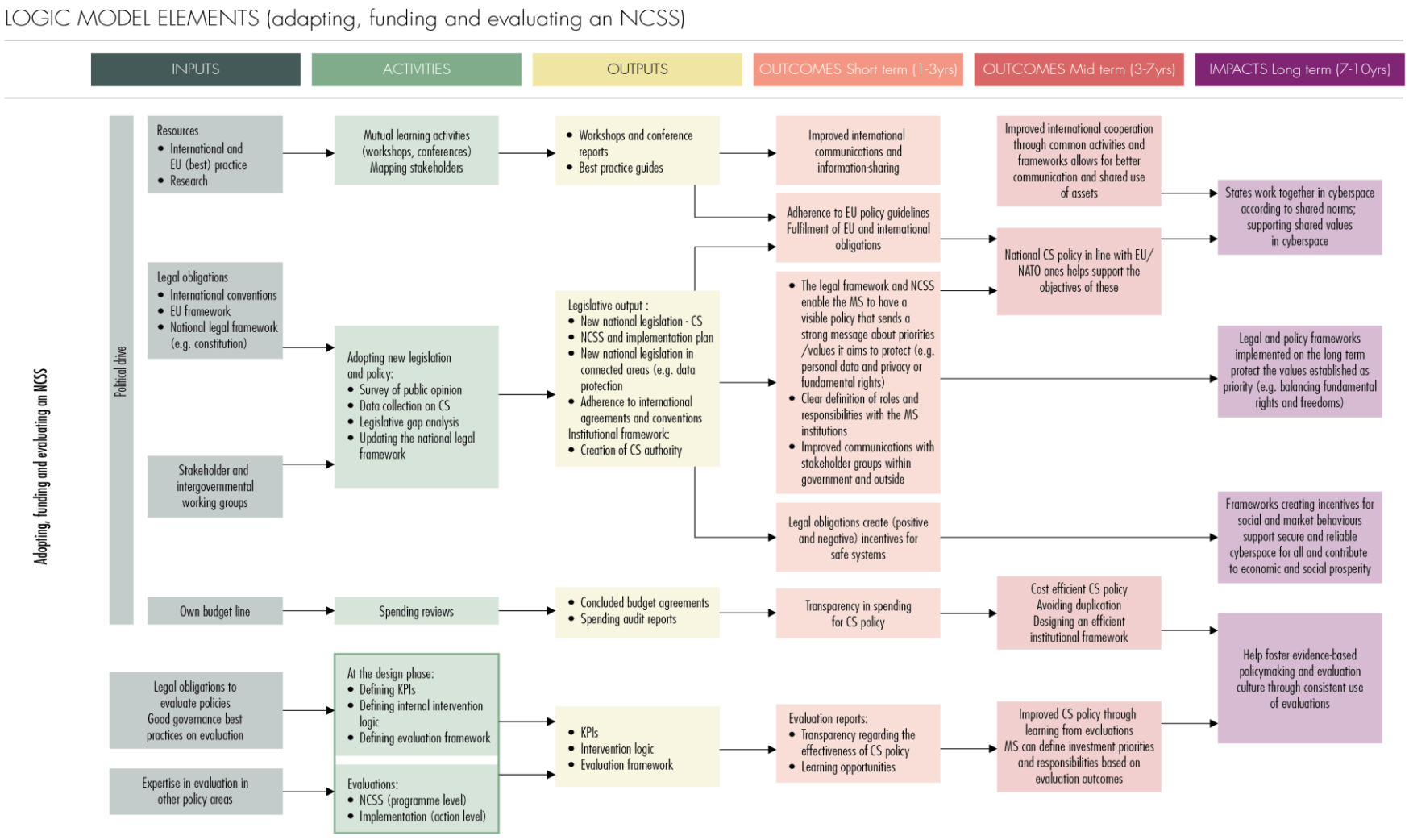

Figure 9 Logic model elements from the review I.

LOGIC MODEL ELEMENTS FOR NCSS

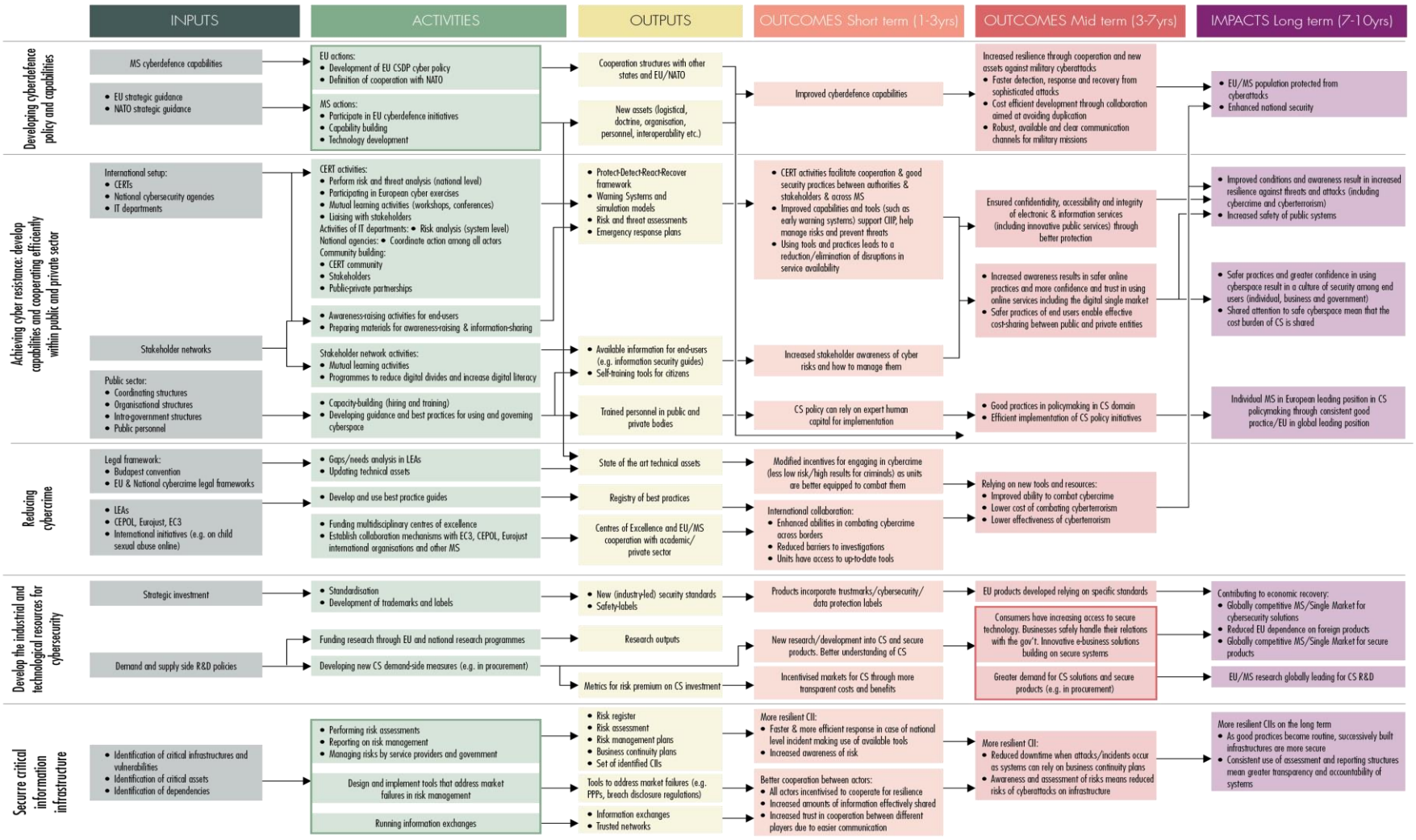

Figure 10 Logic model elements from the review II.

The blueprint logic model illustrates the building blocks that can be used to map the "logic" behind the actions taken and how these support the goals of the NCSS. This tool can be used to detect and summarise the relationship between the inputs, processes, outputs and outcomes involved in the strategy. The streams of activity in the blueprint logic model have been defined in a manner that allows Member States to align the articulation of their strategy to the overall goals of the European Cybersecurity Strategy. However, national contexts vary greatly across Member States. Therefore, the structure contains only suggestions for potential elements and clusters to take into account without prescribing in detail what these areas of activity should contain and what kind of relationship should persist between the individual elements. These elements in more detail:

Developping cyber defence policies and capabilities

The activities are based on the EU strategic guidance and/or NATO strategic guidance (and other policy documents that give guidelines on cyber defence) and include:

- Participation in EU cyber defence initiatives
- Capability building
- Technology development

The outcome would be to have improved cyber defence capabilities, in mid term to have improved resilience through cooperation and new assets against cyber attacks and in long term to have the level of cyber attack protection higly increased.

Achieving cyber resilience: developing capabilities and cooperating efficiently within public and private sector

The inputs are the feedback provided by the different stakeholders, CERTs, National Security (or cyber security) agencies, NRAs etc. From the public sector the information received depends on the coordination structures, on the organisational structures and on the intra-government.The specific activities include:

- Perform risk and threat analysis in national level
- Participating in national and international cyber exercises
- Invest time on mutual learning activities (trainings, workshops)
- Enhance community building

The results should be to facilitate cooperation in CERT activities and enhance good security practices between authorities, to improve capabilities and tools and to eliminate discruption of service availability. In the mid term the confidentiality, availability and integrity of electronic and information services should be ensured; and in the long term the improved conditions and awareness result in increased resilience against threats and attacks. In parallel, increased awareness results in safer online practices and trust in online services including the digital market and more good practice on policy making in the cyber security domain.

Reducing cyber crime

The input to achieve this goal should include the EU and national cybercrime legal frameworks existing already. The specific activities would be to identify the needs and gaps in law enforcement agencies (LEAs), to update the national technical assets, to develop and use best practice guides, to create and invest in centers of excellence and to establish collaboration mechanisms with national and international organisations. The immediate results would be a list of the state of the art technical assets of a national range, a registry of best practices and the creation of centers of excellence and

cooperation with the private sector and academia. In international collaboration aspect more specifically the results should be:

- To enhance the capabilities of dealing with cross border incidents (related to cybercrime);
- To reduce barriers in forensics investigations (multi jurisdictional issues that are difficult to overcome);
- To gain access to state of the art tools.

Develop the industrial and technological resources for cybersecurity

In order to develop industrial and technological recources on cyber security the country should invest from a finance and resources perspective; and put effort on R&D projects and demand-side procurement. The immediate goals would be to develop industry related standards (of national range) and to diffuse the results of the research projects in the market. In a long term perspective this will provide grounds for the creation of competitive European products (and support the EU market on secure solutions) and will introduce them to the international market secure products.

Secure critical information infrastructure

On the CIIP perspective by having as input the identification of critical infrastructures and vulnerabilities (a 'must do' in all countries at national and regional level), the identification of critical assets and their interdependencies, some very useful results would emerge:

- Risk registry ands risk assessment results;
- Risk management plans and business continuity plans;
- List of identified CIIs and their interdependencies;
- Trusted information sharing mechanisms (ISACs, PPPs).

In a long term vision this would result to more resilient CIIs (faster and more efficient response mechanisms) and into better cooperation between actors.

4.2 Key Performance Indicators

Key performance indicators (KPIs) are important criteria which may be selected to measure performance or progress of a policy initiative such as NCSS. On the other hand, output indicators[39] measure mostly the quantity of goods and services produced after a plan was followed; in this study, we focus more on the qualitative criteria, which is why we focus on key performance indicators. Key performance indicator can also be quantitative, but our focus is more on the long term outlook, so the qualitative measures. Defining key performance indicators at the design phase of an NCSS allows policymakers to track progress towards the objectives of the strategy during its implementation. They can also be used in evaluation and supporting the revision of objectives during the lifecycle of the program.
KPIs can be mapped for the planning and evaluation process using a matrix of characteristics.
However, it might be challenging to identify KPIs for NCSS given the difficulties of obtaining data and the fact that outcomes for an NCSS are often highly influenced by other factors. As KPIs are often difficult to create, we outline some illustrative examples. The examples of KPIs are categorised per objective and according to the phase of the process they are addressed (inputs, activities, outputs etc.). As a result some KPIs are binary because based on the feedback received from the MSs there is not enough maturity at the moment to go one step further that the typical binary indicators. This study raises awareness on the specific issue.

[39] http://www.hfrp.org/publications-resources/browse-our-publications/indicators-definition-and-use-in-a-results-based-accountability-system

The first table presents KPIs on developing capabilities on cyber security; part of this are awareness raising, training and CERT activities. The collaboration between public and private sector is also important but KPIs on this topic will be included in the next tables as well, as it is a horizontal aspect of cyber security. The KPIs are categorized per objective to achieve in the strategy; this way the evaluation is more focused and results into more concrete actions.

Key objective 1: Developing cyberdefence policy and capabilities

The first objective to be achieved after the implementation of a national strategy is the development of cyberdefence policy and capabilities.

Key Performance Indicator	Evidence (what we should measure)
Existence of a strategic national plan on cyber defence (doctrine, concepts, stakeholders involved, specific responsibilities)	Existence and status of such a plan, activity reports, action plan and responsibilities
Degree of participation in EU cyberdefence initiatives (capability building)	Indication of participation, level of participation
Identification and structure of military CERT (mili CERT, military policy level)	Capability assessments; Policy documents; internal operational documents
Existence of training (for required types of personnel) and level of influence	Capability assessments; Policy documents; internal operational documents
Interoperability (extent to which CD capabilities interact with others outside mil area)	Capability assessments; Policy documents; internal operational documents
Increased resilience through cooperation and new assets against military cyberattacks (Faster detection, response and recovery from sophisticated attacks, Cost efficient development through collaboration, robust, available and clear communication channels)	Capability assessments, Incident reports, Activity reports

Table 3 KPIs on developing cyberdefence policies and capabilities

Key objective 2: Achieving cyber resilience: develop capabilities and efficient cooperation within public and private sector

The key notion for this objective is the collaboration between sector and the later development of cyber security capabilities in joint actions. Raising awareness is also part of this key objective. Some key performance indicators could be:

Key Performance Indicator	Evidence (what we should measure)
Setup of CERTs and/or National Security Agencies	Existence and mandate of the institutional actors (mission scope, agencies/ bodies mandate)
Existence or setup of public private partnerships on cyber security	Identification and structure of those partnerships, bodies involved and their role, activity reports
Identified risk and threats landscape	Risk analysis, threat analysis (conducted by CERTs or National Security Agencies)
Existence of organised national cyber security exercises	Activity reports

Enhanced capabilities: organised trainings for the public and private sector, mutual learning activities (workshops and conference).	Activity reports, event title, companies/stakeholders participated
Awareness raising activities for end-users (material, campaigns, events)	Material disseminated, campaigns/event organised, survey on citizens perception
National coordination actions among all actors in the national cyber security field (National Security Agencies)	Activity reports, mandates, collaborative activities
Existence of developed response capabilities (react-recovery plans, early warning systems etc)	protect-detect-react-recover plan, early warning systems and simulation models, activity report
Increase safety of public IT systems	Vulnerabilities detection (report-CERTs or National Security Agencies), document the frequency of software upgrades/patches and make procedures, adopt security standards for ICT systems.

Table 4 KPIs on achieving cyber resilience

Key objective 3: Reduce cybercrime

In part we provide a set of KPIs to measure the activities to reduce cybercrime first in a national level and then in international. These KPIs are focused more on the operation of law enforcement agencies (LEAs) and national security agencies.

Key Performance Indicator	Evidence (what we should measure)
National institutional framework for cyber crime reduction (LEAs, CERTs etc)	Structured and documented framework
Enforcement of LEA (gap analysis, identification of needs, state of art technical assets, use of best practices)	Documentation on gaps identified and on mitigation actions to support LEAs with mandate on cyber crime reduction, capability assessment, registry of best practices, pprocedures documentation
Existence of collaboration mechanisms with EC3, CEPOL, Eurojust , international organisations & other MS	Activity reports and common actions
National cybercrime cases resolution	Statistics from LEAs on cases of cyber crimes (investigations solved, prosecutions etc)
International collaboration: • Enhanced abilities in combating cybercrime across borders • reduced barriers to investigations • access to up-to-date tools • lower cost for combating cybercrimes	Procedures for cross border cooperation between authorities (LEAs, CERTs etc), statistics of investigations and resolutions, budgetary reports
Safer cyberspace for all users (users are protected from cybercrime)	Statistics (Law enforcement agencies, Surveys, National statistical offices)

Table 5 KPIs on reducing cybercrime

Key Objective 4: Develop the industrial and technological resources for cybersecurity

The concept of this key objective is tha industry and technological advancements (through academia etc) would support the level of national cyber security in the market products. Some KPIs to measure this:

Key Performance Indicator	Evidence (what we should measure)
Support standardisation and development of trustmarks & safety labels	Compliance with security standards, audits and certification mechanisms in place by the regularoty authorities, adoption rate of standards and safety labels
Funding research through EU and national research programmes	EU databases on research project, Science funding agencies.
Developing new national CS demand-side measures (e.g., in procurement)	Policy documnents, governemtnal ICT requirements documents, new policies
Support innovation in e-business (and cost effeciveness)	Eype and uptake of innovative e-business solutions
Consumers more access to secure technology	Market research reports

Table 6 KPIs on industrial and technologican support for cyber security

Key objective 5: Secure critical information infrastructure

Under the key objective on critican information infrastructures protection we notice that notions like incident reporting, identification of ciritical inftastructures, international cooperation and information sharing are included. The KPIs that cover them are described below:

Key Performance Indicator	Evidence (what we should measure)
Identification of critical information infrastructures i.e. critical assets, vulnerabilities, dependencies, risks	List of CIIs (in national level), list of national critical assets and dependencies, risks and vulnerability registries (CERTs, governmental agency, National security authority)
Risk assessment and risk management prcedures/plans	Division of responsibilities and procedure to be followed (including frequency of updates)
Setup incident reporting and breach notification procedures	Description of procedure, roles and responsibilities, bodies involved, cooperation between countries
Design and implement tools that address market failures (PPPs, breach disclosure regulations)	Strategic program documents; implementation guides
Business recovery and continuity plans for critical infrastructures	Strategic documents, implementation guides, bodies involved, responsabilites and roles of different bodies
Successful information sharing and trusted cooperation between different players	Trusted channels for communication , regular meetings, engagement of stakeholders
Faster and more efficient response in case of national level incident (less downtime in case of attacks/incidents)	Reduction in speed of response; reduction in uncertainty of response
Transparency and accountability of systems	Number and type of documentation available to the public, measure people's awareness

Table 7 KPIs for securing CIIs

General evaluation objectives

In this section we describe high level evaluation indicators that should also be taken into account when discussing the overall cyber security level reached by the national strategy and the action plan.

Key Evaluation Indicator	Evidence (what we should measure)
Evaluations of NCSS (programme level)	KPIs and metrics, complete results (Policy unit responsible for program, Audit bodies)
Evaluations of implementation (action level)	KPIs and metrics, complete results (Policy unit responsible for program, Audit bodies)
International & national legal obligations	Implementation percentage of the obligations (transpositions of european laws, or national legislation)
Budget (level of transparency in spending for th CSC policy)	Financial audit with specifc scope on the activities of the cyber security action plan
States work together in cyberspace according to shared norms; supporting shared values in cyberspace	Level of collaboration and common actions

Table 8 Key perormance indicators for measuring the evaluation of a NCSS

5 Pitfalls to avoid when implementing an evaluation framework

In this chapter we offer some potential challenges which might confront those seeking to apply the guidance described above. These are not meant as an exhaustive list but rather a selection of issues which we consider might have the potential to adversely affect the implementation of an evaluation framework for NCSS.

5.1 Human Capacity

Recruiting the right human resources, skilling and retaining them is critical to any policy implementation, none more so than in a complex area like cyber security strategies where there is a high demand for coordination across different organisations. Failing to recruit the right people and to implement an engagement strategy, alongside any programme, would not bode well for its eventual success. As evaluation is newly introduced, additional resources that would be dedicated in monitoring the process of the strategy would be a rare action to take.

5.2 Budgetary support

Adequate budgets, whilst related to the question of human resources (personnel) is distinct in so far as it provides resources for critical activities such as studies, reports, conferences and workshops that help to achieve the ultimate impacts of an NCSS as set out in our blueprint. Without budgetary support, there is a risk that those establishing and maintaining an NCSS and any associated programme might become side-lined, lose visibility or have their efforts hampered by internal struggles between administrative departments. A good evaluation (and a adjustment) framework would require an annually set budget to fulfil all the objectives.

5.3 Communications and engagement

A third potential challenge of an evaluation framework relates to communications and engagement. Cyber security, like other forms of complex security challenges that characterise the risky, uncertain world we live in, requires a joined up or “comprehensive” approach. In practice, this means that government bodies and agencies, previously able to work within clear mandates and boundaries, must be encouraged to work across their institutional remits, for benefits that might not directly accrue to their efforts but to society and government as a whole. This is even more the case with the private sector, which must recognise that in certain domains (e.g., CII) they must better balance security and business rationales.

5.4 Transparency and public accountability

As NCSS is an example of a public policy intervention, that is using public money to benefit the society and economy, it is vitally important to engage citizens in an accessible way in relation to the rationale for the intervention, the expected benefits, levels of spending on the intervention and what practical steps would be involved (subject of course to specific rules regarding classified Action Plans). Given the current deficiency in public accountability and low levels of public trust in governments[40], being seen to be accountable for efforts in a complex and intangible domain as cyber security will no doubt be challenging. In trying to do so, it will be critical to illustrate the rationale for NCSS which might have budgetary consequences (such as additional spending) and its expected benefits for the average

[40] Eurobarometer Standard 79 Spring 2013; Public Opinion in the European Union available at: http://ec.europa.eu/public_opinion/archives/eb/eb79/eb79_first_en.pdf

citizen. So the evaluation of the strategy should take into account this very delicate matter and express the final results in a way that invests on this transparency of the government to the citizens.

5.5 Developing a lessons learned culture

As outlined in Chapter 3, part of the benefits of implementing an evaluation framework is being able to create and sustain a culture of identifying and learning lessons. This is important to create a continuous positive feedback loop, where mistakes can be identified and resolutions offered and implemented. This requires a step-change in behaviour, however.

- Firstly, it requires encouraging the mind-set of evaluation amongst policy practitioners charged with designing, implementing and evaluating an NCSS (e.g. so that they ask themselves the question: "How would I measure the impact of this or that element of our NCSS?");
- Secondly, the organisational and human capacity is needed to identify and learn lessons in a constructive environment and have been embedded into practice.

5.6 Dealing with uncertainty

Finally, a potential pitfall of evaluation of an action plan/strategy which cannot be avoided is uncertainty and what to do when things do not work out as planned (what if the evaluation results are not so good as expected). The 'building block' approach outlined in this report does not preclude the possibility that despite the design and implementation of all the elements identified in this report, cyber-security goals might not necessarily be reached. This is due to the inherent nature of uncertainty of cyber security, where sudden systemic emergent risks can upset even the most carefully planned NCSS. In this case, policy practitioners should be equipped to deal with adverse political and public reaction (in addition to the usual consequence management, business continuity practices), as well as having capacities to implement sound crisis management to enable them to manage risks as and when they arise. This requires strong capacity for crisis communication skills.

6 Concluding summary

In this report, we have outlined, in the context of the main themes of the 2013 EU Cyber Security Strategy (namely resilience, tackling cybercrime, national security capabilities, cyber defence, critical information infrastructures protection and as horizontal themes education and international co-operation) two empirically based methods that can be used to evaluation of an NCSS. The evaluation activities we have described can be classified according to whether they apply to the content or to the processes of the design or implementation of an NCSS.

We have identified that from those NCSS reviewed, there is a somewhat fragmented approach to the ultimate impacts that a NCSS is expected to provide. To a certain extent this is understandable, because each country will have its own priorities and issues. Indeed, in cyber security, there is no policy prescription that fits every situation. However, this inconsistency and fragmented approach belies a need for the application of broad framework through which NCSS can be evaluated, both in the practical sense of effectiveness, but also in the broader and more important sense of whether the extensive investments of time and effort are worthwhile in reaching stated goals.

After a presentation of empirical evidence, this report offered a number of suggestions and advice in the form of practical tools to assist policy practitioners in evaluating NCSS. The main objective of this reports is to offer:

A generic framework, classified along the themes of the EU Cyber Security Strategy, for evaluation in NCSS, and a set of practical advice in the form of a roadmap, covering:

1. A consolidated logic model consistent with the headlines of the EUCSS;
2. Suggested advice on possible key performance indicators (which would allow progress against the objectives set out in the logic model to be measured).

The roadmap in particular provides practical advice and tips aimed to support the practitioner in translating the good practice identified from the desk research into their own particular contexts. It is hoped that this roadmap will be of use across the broadest user base as it aims to be a flexible pragmatic tool based on principles rather than prescriptive checklists. Finally, in a similar vein, this report has identified some pitfalls that policy practitioners must be aware of when evaluating the strategy.

This report completes the ENISA doctrine on the lifecycle of cyber security strategies (together with the practical guide on development and execution-2012), namely the last steps of evaluation and adjustment of a cybersecurity strategy. This way it addressed both the countries that are now new in the field of the cyber security strategy but also the ones that have a certain level of maturity and would like to enrich it. ENISA offers the complete set of recommendations and tools to the EU Member States to draft and implement a sustainable and efficient strategy that will indeed increase the level of cyber security in the country. The next step would be to offer an automated tool to perform this evaluation, to show different maturity stages and to combine different criteria in the final result.

References

Barbier, J. C., & Hawkins, P. (Eds.). (2012). *Evaluation CulturesSense-making in Complex Times* (Vol. 1). Transaction Publishers.

Boyle, R., McNamara, G., & O'Hara, J. (2012). Riding the Celtic Tiger: Forces Shaping Evaluation Culture in Ireland in Good Times and Bad. In *Evaluation CulturesSense-making in Complex Times*, *1*, 45.

Communities and Local Government (2009) Multi-criteria analysis: a manual. Department for Communities and Local Government.

ENISA. (2012a). "National Cyber Security Strategies: Practical Guide on Development and Execution". December 2012. ENISA.

ENISA. (2012b). National Cyber Security Strategies: An Implementation Guide. ENISA.

European Commission. (2014). 'Digital Agenda for Europe: A Europe 2020 Initiative'. As of 23/05/2014: http://ec.europa.eu/digital-agenda/

European Commission. (2013). *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*. COM(2013) 48 final. 2013/0027 (COD). Available online at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

Furubo, J. E. (2003). The Role of Evaluations in Political and Administrative Learning and the Role of Learning in Evaluation Praxis. OECD Journal on Budgeting, 3(3), 67-86.

High Representative of the European Union for Foreign Affairs and Security Policy. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. JOIN(2013) 1 final - 7/2/2013. Available online at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

Hofstede, G.H. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. Sage Publications.

House, R.J., Dorfman, P.W., de Luque, M.F.S., Javidan, M., & Hanges, P.J. (2013). *Strategic Leadership Across Cultures*. Sage Publications.

Jensen, M.C. (2010). 'Value Maximization, Stakeholder Theory, and the Corporate Objective Function.' *Journal of Applied Corporate Finance*. 22(1): 32 -42.

Klimburg, Alexander (Ed.). (2012). *National Cyber Security Framework Manual*. NATO CCD COE Publication. Tallinn 2012. Available online at: http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

Knill, C. (1998). European policies: the impact of national administrative traditions. *Journal of Public Policy*, *18*(1), 1-28.

Lawrence, John E.S., and Thomas J. Cook. (1982). 'Designing Useful Evaluation: The Stakeholder Survey.' *Evaluation and Program Planning*. 5: 327-336.

Leeuw, F.L., & Leeuw, B. (2012). Cyber society and digital policies: Challenges to evaluation? *Evaluation*, *18*(1), 111-127.

Luijf, E. , Bessleing, K. & Graaf, P.D. (2013). Nineteen national cyber security strategies. *International journal of critical infrastructures*, 9, 3-3.

Marques, G., Gourc, D., & Lauras, M. (2011). Multi-criteria performance analysis for decision making in project management. *International Journal of Project Management,* 29(8), 1057-1069.

Microsoft. (2013). Linking Cybersecurity Policy and Performance. Microsoft White Paper.

Mustajoki, J. et al (2013) Comparison of Multi-Criteria Decision Analytical Software, Searching for ideas for developing a new EIA-specific multi-criteria software, IMPERIA project deliverable, Finnish Institute for Environmental Studies, available at: http://imperia.jyu.fi/tuotokset/Annex7.5.13ComparisonofMultiCriteriaDecisionAnalyticalSoftware.pdf

National Audit Office (NAO). (2013). *The UK cyber security strategy: Landscape review.* London: The Stationery Office. Available online at: http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf

OECD. (2012). *Cybersecurity Policy making at a turning point: Analysing a new generation of national cybersecurity strategies for the Internet economy*. OECD.

Rabinovich, L. (2009). ' Stakeholder engagement.' In *Performance Audit Handbook: Routes to Effective Evaluation*, edited by Tom Ling and Lidia Villalba Van Dijk, 184 – 189. Cambridge, UK: RAND Europe.

Reineke, R.A. (1991). 'Stakeholder Involvement in Evaluation: Suggestions for Practice.' *American Journal of Evaluation*. 12(1): 39 – 44.

Robinson, N. & Horvath, V. (2013). *Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts.* Report prepared for the European Parliament. Directorate General for Internal Policies. 2013.

Shulha, L.M. & Cousins J.B. (1997). 'Evaluation Use: Theory, Research, and Practice Since 1986.' *American Journal of Evaluation*. 18(3):195-208.

Speer, S. (2012). Sectoral Evaluation Cultures: A Comparison of the Education and Labor Market Sectors in Germany. In *Evaluation CulturesSense-making in Complex Times*, *1*, 65.

Toulemonde, J. (2000). Evaluation culture (s) in Europe: differences and convergence between national practices. *Vierteljahrshefte zur Wirtschaftsforschung/Quarterly Journal of Economic Research*, *69*(3), 350-357.

Triantaphyllou, E., & Sánchez, A. (1997). A Sensitivity Analysis Approach for Some Deterministic Multi‐Criteria Decision‐Making Methods. *Decision Sciences*, 28(1), 151-194.

United Nations (2001) Multi-Criteria analysis.Methodologies for Assessment. United Nations Framework Convention on Climate Change.

United States Government Accountability Office (GAO). (2009). *Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats- Statement on the evaluation of cybersecurity actions in the US.* GAO-10-230T. Available online at : http://www.defense.gov/home/features/2010/0410_cybersec/docs/d10230t.pdf

United States Government Accountability Office GAO. (2011). Cybersecurity: *Continued Attention Needed to Protect Our Nation's Critical Infrastructure* GAO-11-865T: Published: Jul 26, 2011. Available online at : http://www.gao.gov/assets/130/126702.pdf

Veleva, V., & Ellenbecker, M. (2001). Indicators of sustainable production: framework and methodology. *Journal of Cleaner Production*, 9(6), 519-549.

Veleva, V., & Ellenbecker, M. (2000). A proposal for measuring business sustainability. *Greener Management International*, 2000(31), 101-120.

Wamala, Frederick. (2011). *ITU National Cybersecurity Strategy Guide*. International Telecommunications Union. Available online at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

WEF. (2013). *World Economic Forum Global Competitiveness Report*. World Economic Forum. Geneva.

Weiss, C.H. (1999). The interface between evaluation and public policy.*Evaluation*, 5(4), 468-486.

National Cyber Security Strategies:

Cabinet Office, United Kingdom. (2011). *The UK cyber Security Strategy: Protecting and promoting the UK in a digital world*. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/UK_NCSS.pdf

Department of Communications, Republic of South Africa. (2010). *Draft cybersecurity Policy of South Africa*. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/southafricancss.pdf

Department of Electronics and Information Technology, Ministry of Communications & Information Technology, Government of India. (2013). As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NationalCyberSecurityPolicyINDIA.pdf

Federal Department of Defence, Civil Protection and Sport DDPS, Swiss Confederation. (2012). *National strategy for the protection of Switzerland against cyber risks.* As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf

Federal Republic of Germany. (2011). Cyber Security Strategy for Germany. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Germancybersecuritystrategy20111.pdf

Government of Australia. (2009). *Cyber Security Strategy*. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/AGCyberSecurityStrategyforwebsite.pdf

Government of Belgium. (2012). Cyber Security Strategy. As of 5 May, 2014: https://www.b-ccentre.be/wp-content/uploads/2013/03/cybersecustra_fr.pdf

Government of Canada. (2010). *Canada's Cyber Security Strategy: For a stronger and more prosperous Canada*. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/canadaNCSS.pdf

Government of the Czech Republic. (2011). *Cyber Security Strategy of the Czech Republic for the 2011 – 2015 Period.* As of 5 May, 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CzechRepublic_Cyber_Security_Strategy.pdf

Gobierno de España. (2013). *National Cyber Security Strategy*. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS_ESen.pdf

Government of France. (2011). Information systems Defence and Security: France's Strategy. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/France_Cyber_Security_Strategy.pdf

Government of Finland. (2013). *Finland's Cyber Security Strategy.* As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/FinlandsCyberSecurityStrategy.pdf

Government of Hungary. (2013). *National Cyber Security Strategy of Hungary, Government Decision no. 1139/2013*. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/HU_NCSS.pdf

Government of New Zealand. (2011). New Zealand's Cyber Security Strategy. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/nzcybersecuritystrategyjune2011_0.pdf

Government of the Republic of Lithuania. (2011). *Resolution no. 796*. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Lithuania_Cyber_Security_Strategy.pdf

Government of Romania. (2013). *STRATEGIA de securitate cibernetică a României.* As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/StrategiaDeSecuritateCiberneticaARomaniei.pdf

Government of the Slovak Republic. (2008). *National Strategy for Information Security in the Slovak Republic.* As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Slovakia_National_Strategy_for_ISEC.pdf

Government of the United States. (2011). International Strategy for Cyberspace: Prosperity, security and Openness in a Networked World. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/international_strategy_for_cyberspace_US.pdf

Gouvernement du Grand-Duché de Luxembourg. (2011). *Stratégie nationale en matière de cyber sécurité*. As of 5 May 2014 : http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Luxembourg_Cyber_Security_strategy.pdf

Information Security Policy Council, Japan. (2013). *Cybersecurity Strategy: towards a world-leading, resilient and vigorous cyberspace.* As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/JAP_NCSS2.pdf

Ministry of Adminisrtation and Digitation, Internal Security Agency, Republic of Poland. (2013). *Cyberspace Protection Policy of the Republic of Poland*. Warsaw. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_PO_NCSS.pdf

Ministry of Defence, Government of Estonia. (2008). *Cyber Security Strategy*. Tallinn. As of 5 May, 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf

Ministry of Security and Justice, Government of the Netherlands. (2013). *National Cyber Security Strategy 2: From Awareness to Capability*. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf

Republik Österreich. (2013). *Austrian Cyber Security Strategy*. Vienna. As of 5 May, 2014: https://www.bka.gv.at/DocView.axd?CobId=50999

Presidency of the Council of Ministers (Italy). (2013). *National Strategic Framework for Cyberspace Security*. As of 5 May 2014: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/IT_NCSS.pdf

TP-07-14-017-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

ISBN: 978-92-9204-109-0
DOI: 10.2824/3903

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu