CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

National Cyber Security Strategy Guidelines

Tallinn 2013

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

www.ccdcoe.org
publications@ccdcoe.org

Prepared by Anna-Maria Osula and Kadri Kaska

About NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a "Centre of Excellence". Located in Tallinn, Estonia, the Centre is currently supported by the Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, the United Kingdom and the USA as Sponsoring Nations and Austria as a Contributing Participant. The Centre is neither part of NATO's command or force structure, nor is it funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements.

NATO CCD COE's mission is to enhance capability, cooperation and information sharing between NATO, NATO member states and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-oriented interdisciplinary approach to its key activities, including academic research on selected topics relevant to the cyber domain from the legal, policy, strategic, doctrinal and/or technical perspectives, providing education and training, organising conferences, workshops and cyber defence exercises, and offering consultations upon request.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

Table of Contents

ACKNOWLEDGEMENT

This document is the public version of *National Cyber Security Strategy Guidelines*, prepared by Anna-Maria Osula and Kadri Kaska, developed by NATO CCD COE upon the request of NATO Emerging Security Challenges Division and published in 2013.

EXECUTIVE SUMMARY

The aim of the National Cyber Security Strategy Guidelines is to assist national policy planners in drafting, improving, implementing and evaluating their national cyber security strategies (NCSS) and other related documents, thereby achieving a higher level of protection against rapidly evolving cyber threats. The Guidelines take a comprehensive approach to cyber security, reaching out to a broad range of relevant actors and aspects in order to support the development of a national cyber security strategy that would benefit the overall protection of national communication and information systems, and national security.

Similarly to any national strategy, a national cyber security strategy should enable government entities to identify strategic objectives, to translate this vision into coherent and implementable policies, to pinpoint the resources necessary for achieving such objectives and provide guidance for the use of these resources, and distinguish how the NCSS is linked to other, related strategies. To support this, the Guidelines propose a generalised structure for a national cyber security strategy that can be further tailored by the nations according to the characteristics of their political, strategic, legal and organisational frameworks as well as national vulnerabilities and existing capabilities.

The Guidelines are divided into three chapters. Chapter I describes the necessity and aim for a national cyber security strategy, explains the main terms and concepts, and identifies a few nationally relevant considerations that determine the scope and content of the national strategy. Chapter III focuses on assessment of nationally relevant cyber threats and vulnerabilities in the strategy. Finally, Chapter IV takes a more detailed look into the main aspects that require attention for action in order to attain an adequate level of protection against cyber risks. Throughout the document, recurring elements and best practices in a selection of published NCSSs are brought out as examples and points of reference.

The Guidelines are supplemented by two annexes. Annex I provides a comprehensive checklist that identifies the diverse aspects and possibilities to be examined in the course of developing or reviewing national cyber security strategies. Annex II lists selected NCSSs from which recurring elements of NCSSs, examples and best practices have been derived.

Chapter I. GENERAL PRINCIPLES AND CONSIDERATIONS

1.1. Rationale for Developing a National Cyber Security Strategy

The dependence on well-functioning critical communication and information systems (CIS) points at both the opportunities and vulnerabilities related to the growing use of information and communication technologies (ICT). Nations are increasingly facing the need to both stimulate ICT-enabled economies as well as ensure the reliability and security of cyber space, especially when it comes to the protection of critical infrastructure. Since the availability, integrity, confidentiality and resilience of CIS and response to asymmetric cyber threats have emerged as national priorities for all developed nations, policy-makers need to address cyber security on a national level and integrate the respective concepts of cyber security and national security.

The aim of a national cyber security strategy therefore is to identify, based on an assessment of national security relevant cyber threats and existing national capabilities, gaps in the existing national framework that have a detrimental effect on the desired level of cyber security in the nation, and to define a set of concrete lines of action to overcome these gaps. The purpose is attaining a coherent and holistic strategy that would encompass all relevant stakeholders and areas of activity having a role in securing a nation's cyberspace.

Due to the interconnectedness of ICT systems into global networks across national boundaries, the level of cyber security of a particular nation affects also that of other nations. Therefore, the existence of a national cyber security strategy to manage cyber threats and improve CIS security is not only significant for the particular nation, but also from the viewpoint of collective and international security.

The development, implementation and review of a national cyber security strategy are influenced by a range of elements and played out by various stakeholders. The scope, principles and content outlined in a national cyber security strategy can be addressed in greater detail in political strategic documents, national and international laws, regulations, organisational and administrative measures, such as communication and crisis management procedures within a State, but also in purely technical protection standards.

The specific national characteristics (such as national values and interests, the legal framework, historical and political contexts, governmental and organisational structures, crisis management processes) and vulnerabilities makes it unfeasible to propose a uniform structure for a national cyber security strategy. Instead, it is the combination of the above-mentioned aspects that determines the national approach to cyber security.

1.2. Main Terms and Concepts

The diversity of aspects and possibilities to be considered in the process of drafting a national cyber security strategy is reflected in the lack of a universal definition of "cyber security" or "national cyber security". Due to domestic and organisational specifics, national strategies and policy documents use diverging terms for cyber-related concepts; while the proposed definitions in the NCSSs tend to be descriptive (i.e. referring to certain characteristics and expectations) rather than normative (i.e. implying or expressing an existing or ideal standard or norm) in nature.

Not all existing NCSSs explicitly define terms such as *cyberspace*, *cyber security* and *cyber defence*. Below is a list of examples of the terms that are used by some of the NCSSs:

a. *Information and Communications Technology*[1] *and Information and Communications Systems*[2], which is defined by the components of digital data and information infrastructure as well as their interaction and functionality;

b. *Cyberspace*[3]*,* which is defined as the virtual space of interconnected ICT systems globally;

c. *Cyber security*[4], which is defined by freedom from danger or damage to ICT systems, reducing risks to an acceptable minimum, or the ability of an ICT system to resist events from cyberspace likely to compromise the availability, integrity or confidentiality of systems or data.

d. *National Cyber Security*[5], which is defined by aspects of electronic data and services that affect a country's interests and wellbeing, or as the sum of suitable and appropriate measures to reduce the risks of the national cyberspace to an acceptable minimum.

e. *Cyber Defence*[6], which is defined as a set of technical and non-technical measures allowing a nation to defend in cyberspace information systems that it considers to be critical.

[1] *Netherlands*: The National Cyber Security Strategy (NCSS). Strength through cooperation. Ministry of Security and Justice, 2011

> "an umbrella term referring to digital information, information infrastructures, computers, systems, applications, plus the interaction between information technology and the physical world that is the subject of communications and information exchange."

[2] *France:* Information systems defence and security - France's strategy, 2011

> "organised set of resources (hardware, software, personnel, data and procedures) used to process and circulate information".

[3] *Netherlands*: The Defence Cyber Strategy. Ministry of Defence, 2012

> "[u]nderstood to cover all entities that are or may potentially be connected digitally. The domain includes permanent connections as well as temporary or local connections, and in all cases relates in some way to the data (source code, information, etc) present in this domain."

Germany: Cyber Security Strategy for Germany. Federal Ministry of the Interior, 2011.

> "[t]he virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace."

France: Information systems defence and security - France's strategy, 2011

> "The communication space created by the worldwide interconnection of automated digital data processing equipment."

[4] *Netherlands*: The National Cyber Security Strategy (NCSS). Strength through cooperation. Ministry of Security and Justice, 2011.

> "[f]reedom from danger or damage due to the disruption, breakdown, or misuse of ICT. The danger or damage resulting from disruption, breakdown, or misuse may consist of limitations to the availability or reliability of ICT, breaches of the confidentiality of information stored on ICT media, or damage to the integrity of that information."

Germany: Cyber Security Strategy for Germany. Federal Ministry of the Interior, 2011.

> "[t]he desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum".

France: Information systems defence and security - France's strategy, 2011.

> **"**'The desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cybersecurity makes use of information systems security techniques and is based on fighting cybercrime and establishing cyberdefence."

[5] *Estonia*: Cyber Security Strategy. Cyber Security Strategy Committee/Ministry of Defence, 2008.

> "*National cyber security* is a broad term encompassing many aspects of electronic information, data, and media services that affect a country's interests and wellbeing."

Germany: Cyber Security Strategy for Germany. Federal Ministry of the Interior, 2011.

> "[…] cyber security in Germany is the desired objective of the IT security situation, in which the risks of the German cyberspace have been reduced to an acceptable minimum. Cyber security (in Germany) is the sum of suitable and appropriate measures. *Civilian cyber security* focuses on all IT systems for civilian use in German cyberspace. *Military cyber security* focuses on all IT systems for military use in German cyberspace."

[6] *France:* Information systems defence and security - France's strategy, 2011.

For the purposes of the NCSS, in order to avoid miscommunication and lack of coordination in both strategic planning and implementation of the strategy, attention should be paid to the clarity of key concepts such as “cyber security”, “Internet security”, “ICT security” and their interrelationship, possibly considering defining relevant terms either explicitly or via describing the national context in order to facilitate uniform understanding.

Throughout these Guidelines, the following terms are to be understood as follows:

a. *Cyberspace* – the global domain created by the interconnection of communication and information systems;[7]

a. *Cyber security* – the desired condition by which CIS are adequately secured within cyberspace;

b. *Cyber defence* – the operationalisation of CIS Security to deter, prevent, detect, withstand and recover from a cyber attack;

c. *Communication and Information Systems* – The ability to adequately protect the confidentiality, integrity, and availability of CIS and the information processed, stored or transmitted;

d. *Communications and information systems security* - The application of security measures for the protection of communication, information and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation;

e. *National cyber security* – “the focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security”[8]

f. *National cyber security strategy* – “a tool by which policymakers identify strategic objectives (ideally consistent with national values and interests), pinpoint the resources available and provide a guide on how such resources are to be applied to reach strategic objectives”;[9]

g. *Cyber attack* – “A CIS Security incident initiated in cyberspace to cause harm by compromising communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems”.

1.3. National Considerations

1.3.1. Purpose of a National Cyber Security Strategy

National cyber security strategies are used to provide guidance to policy-makers and other stakeholders regarding national cyber security policy priorities. Thus, as with any national strategy, a NCSS should enable government departments to identify strategic objectives; translate this vision into coherent and implementable policies; pinpoint the resources for such objectives and how these resources are to be used; clarify how the nation might act in international affairs and within the context of relevant international organisations; and how they are to be linked to other, related strategies.

Despite the diverging perception of key concepts and national goals, the following common objectives are addressed in most of the NCSSs:

“Cyberdefence - The set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical.”

[7] Definitions in items (a)-(d) have been aligned with those recognised by NATO Cyber Defence Taxonomy, NATO Security Policy C-M(2002)49 and other relevant NATO documents.

[8] Alexander Klimburg (Ed.), *National Cyber Security Framework Manual*, NATO CCD COE Publications, 2012, 29.

[9] Ibid, 46.

- Maintaining a secure, resilient and trusted electronic operating environment,
- Promoting economic and social prosperity,
- Promoting trust and enabling business and economic growth,
- Overcoming the risk of information and communication technologies,
- Strengthening the resilience of infrastructures.

1.3.2. Relation of Cyber Security to Other National Strategies

The NCSS should be consistent with the existing and projected national strategies, policies, and development plans, specifically those addressing the development and functioning of information society and digital economy, critical information system-dependent sectors such as energy supply; crime and terrorism prevention, crisis management, and national security and defence. Where it is foreseen that the NCSS will need to diverge from the existing policy documents, concrete proposals should be prepared to overcome those conflicting principles in order to avoid complications in implementation. When integrating the positions of the different stakeholders, care should be taken to balance their interests so that the NCSS would not disproportionately favour the position of one player at the cost of another.

Since there is growing convergence across various national security strategies with respect to identified threats and challenges (e.g., proliferation of weapons of mass destruction, terrorism, state failure, cyber attacks, etc.), special attention should be paid to the relationship between the national security strategy and NCSS. In most recent national security strategies, cyber security is given the highest priority compared to other risks. In addition, the cyber dimension is frequently recognised as cross-cutting a variety of critical infrastructure sectors and other sectors important to society (e.g., energy security) and can therefore be part of the overall national security strategy not only as a distinct element but also as a horizontal issue that crosses a number of other national security strategy goals.

1.3.3. Determining the Scope

Depending on national interests and values, and most of all on the national view on cyber space and the necessary scope of regulation, the objectives for nations in adopting a NCSS can be very different. Some nations take a broad view of cyber space that includes infrastructures while others take a much more narrow approach, equating it more closely to the Internet. To illustrate, the United States is an example of one end of the spectrum with a broad definition of cyberspace, even implicitly acknowledging the importance of social networks. The same approach is followed in the Dutch 2011 NCSS, in which cyberspace is so broadly defined as to include chip cards and in-car systems. On the other side of the spectrum, nations like Australia, Canada, Germany, New Zealand and Spain place an emphasis on the Internet and Internet-connected information technologies.

There are several options in determining the *scope* of the NCSS, ranging from a comprehensive strategy that includes all subject areas and governmental, national and international actors to a more limited sub-strategy addressing a concrete group of actors or a specific part of the wider domain of cyber security. An example of the latter is the Dutch "Defence Cyber Strategy," which supplements the broader NCSS and outlines focal points on the bases of which the Dutch Defence organisation will aim to realise its objectives in cyber space.

The scope of the NCSS depends on several variables. The most common of them are:

a. **Actors**

Although a NCSS almost always focuses most on governmental activities, it is central to address the roles and responsibilities among other stakeholders in cyber security as the governmental, national and international actors need to work together in order to succeed. Pros and cons of the top-down and bottom-up approaches to developing a strategy should also be weighed, keeping in mind the role of bottom-up companies, non-state groups and citizens that build the networks and add the content.

b. **Target groups**

National cyber security strategies may target a number of stakeholders, among them explicitly mentioned in recent strategies: government/national security officials, critical infrastructure operators, and citizens. Depending on the focus of the strategy, other targeted groups may include large organisations and small- and medium-sized enterprises as well as Internet Service Providers.

Comprehensive national cyber security strategies take an effort to follow an inclusive approach, considering the full range of relevant target groups from the user to governmental level and from the service provider to critical information infrastructure owners.

c. **Subject areas**

Besides different actors (governmental, national, international), there are a number of subject areas of cyber security that may be included in the NCSS. These include but are not limited to military, counter cyber crime, intelligence and counterintelligence, critical infrastructure protection and national crisis management, education, cyber diplomacy and Internet governance; each of which could be addressed by different governmental departments. The most comprehensive strategies will cover the political aims, strategic goals and organizations of all of the above.

Independent of the final choice of subject areas to be covered within the NCSS, there are aspects such as research and development, coordination, and information sharing and data protection that should be incorporated into all.

d. **Balancing contradictory needs**

In addition to the subject areas, the scope of a NCSS is determined by the choice of whether or to what extent to express the national approach to balancing various contradictory needs. These include the inherent tension between the openness required for innovation and the requirements of public security; the careful balancing of economic gains through adoption of new technologies and possible increases in security risks; choice between private or public sector on deciding on either a “regulatory” (mandated) or “voluntary” approach to critical infrastructure protection; weighing requirements for data protection and information sharing; and ascertaining to what extent, if any, the curtailment of “Internet freedoms” is justifiable for public safety.

Chapter II. IDENTIFYING THREATS AND VULNERABILITIES

2.1. Purpose and Aim of a NCSS Cyber Risk Assessment

A NCSS results from the recognition of cyber threats and vulnerabilities that are relevant to the nation and can potentially have a detrimental effect on the desired state of functioning of the society.

The majority of current national security strategies acknowledge cyber threats as a new security challenge bearing relevance for national security, especially as other sectors such as energy, health and environment are dependent on the cyber domain. The inclusion of cyber threats as potential threats to national security is often accompanied by the recognition of the increasing complexity, far-reaching implications and specific vulnerabilities related to cyber threats and malicious cyber activities.

For this reason, a NCSS should undertake a national cyber risk assessment (cyber threat and vulnerability assessment) that would determine the dependence of the society on the functioning of communication and information systems, identify general and specific cyber threats, define assets or interests that require protection, and analyse the identified vulnerabilities. The identification of cyber-dependent assets and interests, including their nature, functionality and specific vulnerabilities, is significant for determining the relevance of a particular cyber threat to national security, thereby shaping both the scope and implementation of a NCSS. In addition, such assessment enables the definition of an optimal course of action for the mitigation of cyber threats and ensures that the proposed lines of action are appropriate, effective, and cost-efficient.

2.2. Cyber Risk Assessment

A comprehensive national cyber risk picture should assess national characteristics by taking into account factors such as dependence on CIS; sources, motivation and nature of cyber threats; and the scale, sophistication and organisation of such threats. However, it is important to recognise that traditional categorisations of threats, sources and motivation are becoming growingly blurred. Clear distinctions among them are often not possible, and therefore the complexity of the task of national risk analyses and assessment should be given proper recognition, especially by avoiding simplified and finite judgements. Also, even the most current NCSSs will still reflect the *status quo* of a certain period and be limited by it, which is why it is vital that a NCSS recognise the evolving nature of cyber threats, including the evolvement of methods and actors involved.

2.2.1. Sources of Threats

There is a wide range of possible sources of threats. Individuals and groups related to organised crime and motivated by economic and/or political interests are the traditional sources of cyber threats recognised by most nations. Potential terrorist use of cyberspace has gained attention as a threat source, and increasingly, NCSSs consider state as potential sources of cyber threats.

The different sources are combined with various motivations for carrying out malicious cyber activities, related to either criminal aims, terrorist purposes, espionage or economic and social/political interests. In addition to the more traditional financial interests, the recent years have witnessed an increase of the presence of political motivation behind cyber attacks. Neither type of motivation is limited to private or national players only.

Due to the Internet's structure and nature of communications, precise attribution to a specific source of threat of even a certain type of malicious actor is often complicated. Multiple motivations are also recurrent, which further complicates source identification.

There is a general recognition of a significant increase in the level of organisation and sophistication of threat sources over the recent years. This applies to all major sources of cyber threats, including individuals, (criminal) groups, and states, all of which have grown increasingly innovative and skilled in their actions.

2.2.2. Nature of Threats

Cyber threats are typically categorised as threats affecting the availability, integrity and confidentiality of data and systems. For the purposes of threat definition, the focus of NCSSs leans towards *intentional* activities of malicious actors rather than *accidental* (including *force majeure*-type) incidents arising from natural causes or system/software malfunctions, even though both aspects are typically acknowledged.

Types of cyber threats recognised in the NCSSs include intrusion into CIS with the purpose of obtaining information such as personal data, confidential data (commercial secrets, national security, diplomatic or other national interests), theft of identity, and breach of intellectual property. Cyber attacks can also take the form of vandalism, which is more typical to private actors. In terms of frequency, large-scale distributed denial of service (DDoS) attacks have been a main type of cyber attack during recent years, and have targeted both state and private CIS. In terms of severity, the cyber threats viewed as the most critical by nations include the disruption of critical infrastructures, and cyber espionage against governments and critical parts of private sector.[10]

A cyber attack is normally not limited to one type of method only: for example, a typical organised hacker attack may consist of several phases, involving penetration of vulnerable systems of the target and a following coordinated DDoS or defacement attack. However, nations mostly refrain from describing threat methods in specific terms, recognising their quickly evolving nature, and focus instead on the estimated and potential effect of cyber threats on vital societal interests.

Some nations take a wider approach to threat identification, including activities carried out in cyber space, but not necessarily against "cyber" targets. In this regard, threats originating from cyberspace may include the spread of terrorist propaganda, terrorist recruitment, communication, planning and fundraising.

2.2.3. General and Specific Vulnerabilities

While national reliance on ICT infrastructure is generally viewed as a source of vulnerability in itself, national strategies also recognise specific vulnerabilities that expose certain strategic interests of the nation to cyber threats. Vulnerabilities of critical infrastructures to cyber threats are commonly discussed in this category; some nations also mention national defence structures/functions, societal well-being and economic prosperity. New and evolving cyber-dependent services (such as mobile data transmission or the growing use of social networking services) are also addressed as a specific vulnerability by some strategies.

Various factors contribute to the inherent vulnerability of cyber infrastructure; among those, NCSSs identify aspects such as the global and largely commercially owned nature of cyberspace, the vast array of components that form cyberspace and that come from diverse range of suppliers, the high pace of innovation and change, and the largely reactive nature of defences and responses.

Chapter III. DEFINING LINES OF ACTION

3.1. Aim of Identifying National Cyber Security Lines of Action

As recognised in Chapter II, the aim of a NCSS is to identify, based on an assessment of national security relevant cyber threats and existing national capabilities, gaps in the existing national framework that have a detrimental effect on the desired level of cyber security in the Nation, and to define a set of concrete lines of action to overcome these gaps.

A comprehensive set of lines of action should cover policy, legal and regulatory as well as organisational capabilities and stakeholders, including tasking and responsibilities for particular activities. Again, the national context, which is conditioned by historical, cultural, legal, organisational and political factors, as well as the national choices in balancing the dilemmas inherent to cyber security (see Chapter II), are likely to lend to significant national differences in approaching relevant issues in a NCSS.

The number and extent of issues to be tackled in a NCSS necessitates a certain amount of political guidance with regard to prioritised areas and activities. Therefore, a NCSS normally identifies a set of strategic and political objectives of central importance, strategic areas where coherent action is foreseen, together with

[10] "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", OECD Digital Economy Papers, No. 211, OECD Publishing, 2012, 16-17.

prioritised activities. In most strategies, these quote items such as improving cooperation between stakeholders in the public and private sectors, strengthening the protection of critical information infrastructure, and raising cyber security awareness. Such lines of action follow the general objectives of the NCSS, but are defined in more concrete terms with a focus on clearly identifying prioritised areas and activities.

The typical approach of NCSSs is to define the lines of action in rather general terms, leaving detailed description of the tasks, authority and procedure to a consequent document, such as an Action Plan, which serves as the main tool for the implementation of the NCSS by encompassing all relevant stakeholders and areas of activity having a role in securing a nation's cyberspace.

The following structure reflects essential aspects to be considered in the drafting of a NCSS; it does not necessarily propose any particular structure for a NCSS. Also, the measures described in this section of the Guidelines relate to a number of different domains involved in cyber security, which causes a certain extent of overlap in discussion, but also illustrates that no measure can or should be viewed as isolated to one domain only.

3.2. Legal and Regulatory Measures

3.2.1. Assessment and Revision of Existing Legal Obligations in Relevant Domains

The national and international legal environment defines a large set of commitments that shape potential domestic cyber security approaches. This means that the objectives and activities of a NCSS must be appropriately coordinated with the principles, regulatory mechanisms and procedures foreseen in cyber security-related national legal instruments, as well as other legal commitments made by the nation.

The assessment of legal and regulatory measures, with the purpose of identifying vulnerabilities and remedying them, will need to include existing legal obligations in the domains of government/public sector responsibilities, responsibilities of the private industry (including service providers), and CIS user responsibilities. The cyber security legal framework is determined by both international and national legal instruments in various areas of law.

3.2.1.1. International Obligations

A NCSS and the envisioned updates in policy and legal instruments will need to be consistent with the nation's obligations under international law, including commitments arising from national membership in international and regional organisations.

Since no uniform international law instrument exists that would apply to cyber security in general and be binding on all countries nations should consider mapping their participation in international and regional organisations as well as international treaties, and identifying any consequent commitments that have an effect on national law relevant to cyber security. In terms of international treaty obligations, the applicability and extent of such commitments should be analysed with due attention to any treaty exemptions (e.g. in relation to national security) and national reservations or derogations to the treaty that affect the application of the particular obligation in the nation generally or from a national (cyber) security perspective.

An example of an international treaty applicable to cyberspace is the Council of Europe Convention on Cybercrime. It is the only binding international instrument focusing on crime committed via the Internet and other computer networks, regulating such aspects as copyright, computer-related fraud, child pornography, violations of network security, international cooperation and procedures. The convention's goal is to pursue a "common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation".[11] Since a harmonised approach to cybercrime criminalisation is highly recommended and international cooperation a key for fighting cyber threats, signing and ratifying the convention is strongly encouraged.

The mapping of international treaty obligations should also have consideration for international treaties or organisations to which the nation is not currently party but where accession would be desirable to ensure more efficient protection from general or particular cyber threats or to further the nation's political objectives with regard to cyber security.

3.2.1.2. National Law Affecting Cyber Security

Aspects that need to be taken into account on the national level include identifying the gaps in national law that affect a coherent, comprehensive and efficient response to cyber threats, developing legal measures necessary to overcome those gaps, as well as a careful balancing of such proposals with other legitimate interests of the society and individual stakeholders.

Since a number of legal domains touch upon various cyber security subject areas, nations rarely adopt a single overarching national cyber security law.[12] Instead, aspects relevant to cyber security may be addressed in various legal instruments by subject area, organisational structure and authority, or other considerations.

The following list of areas of law that affect or are employed to address cyber security is indicative; a NCSS does not necessarily have to address each of these items or each area of law.

a. *Privacy and Personal Data Processing Law*, including principles for operational information sharing in the event of a cyber incident;[13]
b. *Telecommunications Law*, including obligations of data communications service providers in ensuring CIS infrastructure and service continuity; mechanisms for service providers to intervene in case of a threat against the security or integrity of communications networks;[14]
c. *Cyber Crime and Criminal Procedural Law*, including penalisation of malicious cyber activities (offences against the availability, integrity and confidentiality of computer data and systems); adequacy of criminal sanctions for cybercrime (taking into account varying motivations for cyber crime and various potential economic or social consequences); and aspects related to criminal proceedings, including procedural aspects of collection of evidence characteristic of cyber crime and international cooperation and legal assistance in cyber crime matters;[15]

[11] Council of Europe Convention on Cybercrime, ETS 185. 2001.

[12] An example is Latvia, who adopted an IT Security Law on October 2010 (in force from 1 January 2011). The act defines responsibilities for the public sector, Internet Service Providers, and critical IT infrastructure owners as well as the national Computer Emergency Response Team (CERT-LV) in prevention of and response to cyber threats.

[13] For Member States of the European Union, these are commonly affected by the provisions of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which are to be transposed into national law of Member States. (A major reform of the EU legal framework on the protection of personal data has been proposed in 2012).

[14] For Members States of the European Union, these extensively derive from the Framework Directive (Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services), with its subsequent amendments, as well as the four Specific Directives of the Telecommunications Regulatory Package.

[15] An example of a review of the cyber crime regulation is the proposed European Union Directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)). Also, some nations have chosen to adopt a separate strategy document for the fight against syber crime such as the "UK Cyber Security Strategy: Protecting and promoting the UK in a digital world", 2011.

d. *Critical Information Infrastructure Protection and Crisis Management Law*, including the arrangement, procedure and responsibilities for defining critical services and critical information infrastructure, conducting national risk assessments, and drawing up (sector-specific) protection plans.[16]

3.3. Organisational Measures

3.3.1. Assessment of Existing Organisational Capabilities

National organisational capabilities and structures may follow various models but a generic distinction of policy and strategic level functions and operational and tactical level functions should exist. A strict functional separation is normally not possible, nor is it necessary; the actual scope of activities of institutions responsible in this area varies in different national contexts. These functional levels may however be additionally divided sectorally by various spheres of competence of the government, involving actors with tasks and responsibilities in specific fields such as the government information systems, economic environment, law enforcement, or national defence. The degree of communication and coordination among those institutions with regard to cyber security varies vastly in national practices. A main aim of a NCSS therefore is to improve coherence by establishing mechanisms for interagency communication and coordination.

3.3.2. Organisational Measures for Improving National Cyber Security

The identification of organisational measures for improving national cyber security involves reviewing the current organisational structures, appointing responsible entities on strategic and operational levels as well as the description of their tasks and responsibilities. It also involves assigning coordination points and defining principles for coordination, cooperation and collaboration.

a. *Defining a coordination mechanism and appointing a coordinating body/bodies on the strategic level.* Establishing an effective national cyber security organisational framework has a clear relation to the scope and objectives identified in a NCSS. However, while the definition of specific organisational functions, tasks and responsibilities is mostly divided among the different spheres of competence of the government (i.e. ministries/departments) for efficiency reasons, it is advisable to avoid distinct narrowly defined sectoral mandates, terminology and policy objectives as this is likely to result in a policy or regulatory vacuum, conflicting legal requirements, and organisational frictions.

In order to avoid such fractioned approach to cyber security, a prime defined objective of most NCSSs is to identify mechanisms for political and strategic top and mid-level interagency coordination. To that end, a number of NCSSs appoint a body for coordinating cyber security activities by the different entities. The function may be allocated to an existing governmental or inter-ministerial body, which will need to be given a sufficient mandate and tasking. A specialised body, such as a National (Cyber) Security Council, may also be formed to carry out the overall cyber security coordination. The purpose of such a body is to maintain coherence in activities and developments of the governmental agencies that have an effect on national cyber security. This body may also be tasked with ensuring an integrated approach by public and private parties.

A strategic and political level coordination mechanism should also be defined for the purposes of crisis management, including for the coordinated response to major cyber incidents.

[16] An example of a national approach for crises management can be seen in Estonia’s Emergency Act (RT I 2009, 39, 262) that provides the legal bases for crisis management, including preparing for and responding to emergencies as well as ensuring the continuous operation of vital services. The act obliges the provider of a vital service to ensure “the constant application of security measures in regards to the information systems used for the provision of the vital service and the related information assets.”

b. *Establishing incident management mechanisms and bodies on the operational level*. The task of handling immediate cyber incident response and response coordination on the operational level is normally allocated to a Computer Emergency Response Team (CERT)/Computer Security Incident Response Team (CSIRT). The CERT is a coordination body that oversees response to major ICT disruptions and cyber attacks; obligations related to the application of security measures in the affected CIS remain with the owners and operators of those CIS, who will handle incident management in cooperation with the CERT. The CERT may also be given functions related to cyber threat awareness aimed at improving the detection, analysis, mitigation and response to sophisticated cyber threats.

The establishment and empowerment of a CERT involves defining responsibilities, incident handling mechanisms, information sharing and coordination mechanisms with CIS service providers, other national/governmental entities, and with similarly tasked organisations in other nations. While the tasks and responsibilities of the CERT are often specifically focused on government CIS and the critical infrastructure, there is no exclusion of other CIS that are relevant for national interest.

The NCSS should also consider operational level responsibilities for cyber incident response in crisis management, including establishing connections between the bodies involved in cyber incident response, reviewing crisis organisations and processes at a public and private levels, and establishing appropriate crisis organisations and processes if necessary.

c. *Public-private sector cyber security cooperation.* With regard to the private sector bodies bearing a role in national cyber security, such as CIS service providers, the focus of organisational measures is on establishing and improving coordination, cooperation and collaboration, including communications channels and frameworks for information exchange. With regard to owners and operators of critical (information) infrastructure, the establishment of protection mechanisms will typically require also some form of incentivisation or regulatory measures.

d. International cooperation. Due to the cross-border nature of cyber threats, it is essential that a NCSS have consideration for the centrality of international cooperation and coordination of activities, including cooperation in international and regional organisations with a cyber security agenda, organisations whose agenda affects national, regional or international cyber security, as well as relevant bilateral collaboration in cyber security matters.

3.4. Awareness Raising Measures and Education

3.4.1. Identifying the Audience for Awareness Measures

The lines of action identified in a NCSS will need to consider the necessity of bringing the relevant information, understanding and competence of cyber security to all levels of society. This requires defining target groups, identifying the minimal level of awareness and competence required, and suitable measures directed at each group to achieve a satisfactory level of cyber security awareness and competence in the society as a whole.

The target groups are defined by their functions or tasks with regard to the use and operation of cyber resources, particularly the public CIS. These may include users of communications services, communications network and service providers, critical infrastructure owners and administrators, policy-making and legislative system, law enforcement, cyber incident and emergency management, and others, as determined by the national circumstances and needs. Functionally, sub-groups may exist under the target groups identified above (such as children or users of e-commerce services under the user group). Where relevant, such sub-groups should receive attention appropriate to the nature of their activities in cyberspace.

3.4.2. Measures for Raising Cyber Security Awareness

Awareness measures should consider the need for ensuring generic awareness of secure behaviour as well as ensuring situational awareness of current cyber security vulnerabilities and threats appropriate to the relevant target groups. Any existing awareness and competence measures should also be assessed with these criteria in mind.

Awareness measures for the abovementioned target groups comprise programmes and activities aimed at strengthening both the general ICT security culture in the nation as well as improving cyber security awareness of professionals active in the various fields directly related to or affecting cyber security. These may include publicly available and/or targeted information materials, online awareness and learning environment and tools, and basic education programs to confront cyber illiteracy. On a more advanced level, specialised training curricula and programmes in information and network security should be available. Cyber defence exercises involving technical/operational aspects, strategic/political decision-making procedures, or both, have an important role in the assessment of the suitability and effectiveness of awareness measures.

3.4.3. Education

Integration of cyber security aspects into education and research are important measures of improving national cyber security and ensuring its sustainability in the longer perspective. In many NCSSs, cyber security education focuses mainly at professionals by means of formal education and professional training in information and network security. The former can take several forms:

a. incorporating cyber security courses into computer science curricula,
b. teaching aspects of cyber security in other relevant curricula (such as education for professions related to the management of critical infrastructure, teacher profession),
c. developing full cyber security professional curricula.

Some nations also include education in ICT security throughout the public education system, beginning with elementary education.

3.5. Technological Tools and Measures

Due to the non-static nature of the cyber threat environment, the technological tools and measures should be focused on both the aspect of protection and defence as well as on the continued improvement of prevention and resilience. Therefore, a NCSS should address the development of the technological measures in order to increase national preparedness, risk mitigation focusing on limiting disruptions and their consequences, and measures aimed at facilitating rapid recovery in the aftermath of an incident.

More practically, the technological measures aimed at improving prevention, resilience and defence in NCSSs may include:

a. establishing (sectoral) *fundamental security requirements* for communication and information systems, based on existing security standards, good practices widely recognised by the industry, or other equivalent frameworks. A fundamental level of CIS security should be implemented in existing infrastructure; furthermore, fundamental security requirements should also serve as a criterion in the acquisition of new systems;
b. keeping up technically with *threat evolvement*; investing in keeping technical capabilities for analysis, monitoring, resilience and response to cyber incidents up-do-date; furthering cyber security standardisation (including the incorporation of concepts such as “secure by design” and “privacy by design”);

c. *supporting Research and Development* in information systems security, also in fields related to the implementation of security technology (such as law, economy, policy); promoting relations between information security academic environments and the industry.

3.6. Critical Infrastructure Protection

Critical infrastructure comprises those public or private infrastructures which are essential for maintaining vital societal functions and whose disruption or destruction would have a significant impact on the safety and wellbeing of residents or the functioning of state institutions. Considering the common dependence of critical infrastructures on specialised CIS (usually referred to as *critical information infrastructures*), critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP) together with national crises management form an indispensable part of cyber defence and are among vital topics addressed in NCSSs.

CIP-related measures and activities in NCSSs are primarily related to the need to address malicious cyber activities, especially cyber crime and cyber espionage, but also accidental cyber incidents such as natural disasters and malware dysfunctions. Essential components in achieving the objective of ensuring the resilience of critical infrastructures from cyber threats include the identification of critical infrastructures and their dependency on information infrastructure, and supporting CIP by relevant legal regulations as well as organisational and technical measures ensuring the continuity of providing critical services.

Whereas the majority of NCSSs consider CIP and CIIP as a specific subject area within a NCSS, the more detailed approach is commonly outlined in a comprehensive national crises management policy and related legal acts. The crises management policy would typically establish a basis for sectoral identification of critical service providers as well as address the arrangement, procedure and responsibilities for conducting national threat and risk assessments and for drawing up and maintaining (sector-specific) protection plans. The role of the NCSS, in practice, is to extend or update the national crisis management arrangement by addressing core functions for the mitigation of cyber threats in critical infrastructure, specifically with regard to strengthening cooperation and information exchange between the public and the private sector both nationally and internationally, supplemented by a stable crises communication network and an applicable legal framework.

3.6.1. Roles and Responsibilities in CIP

In the context of cyber-induced national emergencies, the existing NCSSs identify individual and collective responsibilities for various parties, including suppliers and users. Minimum requirements for ensuring the continuity of services may be considered, addressing both technical security and procedural aspects. These may be defined by law or by standard in accordance with the specifics of the sector. In order to ensure the proper implementation of information security practices, a compliance monitoring body may be appointed and a supervision mechanism established. Measures for improving the capability to withstand cyber attacks against critical infrastructure, such as national cyber risk assessment and contingency planning as well as exercises, may also be foreseen in the NCSS. Considering the primarily private ownership and management of critical infrastructures, the need for a cooperative effort by public institutions and relevant private sector service providers is commonly emphasised.

Beside responsibilities related to the protection of their own vital CIS, the government plays additional roles in providing support to the public and private sector actors in fulfilling their responsibilities, including sharing information on joint risk analysis, models for risk assessment and accreditation of risk management methods, harmonisation of training measures as well as technology assessment analyses. Organisational measures for the inclusion of cyber crisis management capability in the national crisis management system should also be taken (see Chapter IV, *Organisational Measures*).

3.6.2. Information Exchange

NCSS may also address specific mechanisms to strengthen public-private information sharing and ensuring the reciprocity of information flow, with the goal of improving the situation awareness of different actors. Measures may include reporting mechanisms on disruption or breakdown of services, the right of competent authorities to obtain information necessary for preparing an emergency response plans, and mechanisms to benefit the critical service providers from the information gathered by the State on threat analysis. To ensure effective and confidential communication in crisis management, secure means of communication may also be considered in the NCSS.

3.7. Financial Considerations

Besides conducting an economic impact assessment for the NCSS, which may be required to be carried out under national procedural rules, a number of financial considerations should be addressed as being relevant for the development and implementation of the NCSS.

The text of NCSS will typically not detail the allocation of resources and their prioritisation, leaving that for separate budget documents, but serves as a general guideline for financial considerations. These considerations touch both public and private sector budgets since successful NCSS development and implementation depend on financial resources from both. Essentially, it is not of primary importance whether the NCSS budget is reprogrammed from existing budgets or constitutes additional funds to carry out the intended activities.

As a rule, the NCSS should provide sufficient guidance concerning key objectives to enable identification of resources required from different entities for the coherent implementation of the strategy. Without clearly assigned resources for the measures and activities foreseen in the NCSS, the strategy may remain declarative and incapable of achieving the declared objectives. Clear and coherent guidance can also help to avoid overly focusing resources on narrow organisational goals at the cost of others and prevent situations where reductions in funding certain activities will be done without regard to related or dependent activities which could be adversely affected.

During the NCSS development process, the advantages of engaging a wide range of public and private sector stakeholders and their expertise in NCSS development should not be outweighed by the related costs for the strategy development process, which may condition a certain amount of optimisation in the range of actors that could potentially be involved. Stakeholder engagement will also help ensure that the measures and activities defined for achieving the strategic objectives of the NCSS are financially realistic.

As discussed in Chapter III, the NCSS development phase also includes national risk assessment. Since this should serve as a basis for defining the NCSS lines of action, it will also ensure a direct connection of NCSS measures and activities to the nationally relevant cyber risk picture. Such approach will facilitate having regard for limited national resources and provide a sound, fact-based foundation for actions as well as prioritisation, thereby ensuring overall cost efficiency.

The implementation of the NCSS will produce costs for both the public and private sectors, induced by upgrading hardware and software as well as adapting internal and external procedures, e.g. those for coordination and information sharing. Labour costs related to the increase of administrative burden are also to be considered. For this reason it is important that any planned cyber security measures are both necessary and proportionate to the desired NCSS objectives. It is advisable to involve the private sector in the decision-making process to ensure a transparent and proportionate solution, considering alternative and less costly options of regulation (incl. self-regulation) where possible. Cost-sharing principles between the public and private sectors in the case of additional legal or regulatory obligations intended for the latter could also be considered.

Also, resource allocation should be consistent with other existing and projected national strategies, policies, and development plans (see section 2.3.2.). Additionally, it is relevant to consider that all long-term measures planned in the NCSS should be financially sustainable.

3.8. Implementation Measures

3.8.1 Establishing an Action Plan

The implementation of the main lines of action identified in a NCSS requires the development of an Action Plan, which would detail the concrete activities needed to achieve the objectives of the NCSS in accordance with the defined strategic priorities and measures. An Action Plan should address in particular the distribution of tasks and responsibilities, timeline, evaluation, and allocation of resources.

As a NCSS Action Plan is integrally linked to a NCSS, an Action Plan should likewise be developed with the participation of the different stakeholders and working groups involved in the development of a NCSS.

While a NCSS is usually a public document, an Action Plan containing detailed implementation arrangements are variedly limited to official use only.

3.8.2. Responsibilities and Coordination

Cyber security is a collective effort and the responsibility for the implementation of the identified lines of action is divided among multiple stakeholders. Therefore, special attention must be paid to the overall coordination of the envisaged actions. In addition to assigning the responsibility for creating the Action Plan, a NCSS should appoint a body responsible for implementing the proposed actions or for coordinating and overseeing the implementation if the task is distributed between several stakeholders. Such a body should have the mandate to task different national agencies and should thus be either relatively high-level or collective in nature. It is advisable for accountability and transparency purposes that such coordinating body and the implementing bodies in particular report periodically on the progress of implementation. To facilitate progress monitoring, evaluation criteria together with the responsible entity should be identified in an Action Plan.

3.8.3. Timeline

For the purposes of effective and focused implementation of a NCSS, an Action Plan should define concrete deadlines for rolling out particular measures and activities. Detailed planning may be developed for shorter periods (one or two years), or a periodic review and update of an Action Plan may be foreseen to take targeted corrective action, with a body appointed to direct and supervise the updating of an Action Plan.

3.8.4. Finances

The limited availability of resources normally requires at least some prioritisation of the activities laid down in an Action Plan. Both the cost of implementing the foreseen cyber security measures and the potential loss arising from abstaining from implementing these measures should be considered. The Action Plan should ensure balanced development across sectors and lines of action, taking into account that neglect of lower priority areas could lead to lack of coherence, ineffectiveness or gaps in the implementation of the NCSS as a whole or in critical parts.

The development of a NCSS Action Plan should take into account the resources available and define a clear picture of additional budgetary funding needed for the various tasks and activities.

3.9. Evaluation and Review of a NCSS

The constantly evolving nature of cyber threats and the resulting need to continuously develop up-to-date responses, as well as the involvement of various stakeholders and subject areas in cyber security requires that a NCSS be periodically evaluated, and if necessary, reviewed. Evaluation is necessary to gain insight to the *status quo* of the existing initiatives and to measure the implementation and overall efficiency of the strategy in meeting its stated objectives. By evaluating the achieved results of the proposed activities it is possible to move forward with suitable additional actions in order to align with or amend the objectives of the strategy, where necessary.

Methodologies in evaluating the effectiveness of the NCSS or its implementation may vary, but the principal steps in the assessment process can be divided into the following categories:[17]

a. **Defining variables.** Define the scope, objectives, methodology, timeline or frequency, actors involved, and resources of the evaluation.

b. **Assigning responsibility.** It is important to assign the responsibility for the evaluation process to an independent entity (an existing governmental body, an interagency body, or other) with an appropriate mandate, roles and responsibilities (e.g. to whom should such an entity report back to). The body appointed to carry out the assessment of the efficiency of a NCSS in meeting its objectives may be different from the body coordinating the implementation or review of a NCSS. In addition to the leading entity in charge of the evaluation, other stakeholders should also be encouraged to take part in the evaluation process.

c. **Review.** The reassessment of NCSS objectives and corresponding Action Plan items can be undertaken through a periodic review. The review process includes having a clear overview of the implementation of a NCSS as well as ensuring coherence with other national strategies, initiatives and legal instruments**.** Appropriate performance measurement mechanisms could be considered to facilitate rational and well-directed use of resources.

d. **Reporting on the outcome.** The outcome of the evaluation may be in a format of a report on the status of affairs and a list of future actions that should be implemented. In addition, the evaluation may include lessons learned, good practices, achieved results, the evaluation of the progress of implementation of each activity as well as the expectations for the next evaluation.

[17] National Cyber Security Strategies: Practical Guide on Development and Execution. ENISA 2012.

ANNEX I. CHECKLIST FOR NCSS DEVELOPMENT

The checklist for NCSS development is complementing the Guidelines by offering a condensed list of aspects to be taken into account during drafting, reviewing and evaluation of a NCSS.

GENERAL PRINCIPLES AND CONSIDERATIONS

- ✓ Defining the rationale for developing national cyber security strategies
- ✓ Defining the purpose, aim and objectives of a NCSS
- ✓ Defining main terms, concepts and their interrelationship
- ✓ Identifying the relation of cyber security to other national strategies, such as the national security strategy
- ✓ Reviewing other relevant national policies, laws, regulations, decision-making processes and other aspects regarding national cyber security
- ✓ Balancing different aspects related to national cyber security such openness for innovation and requirements for public security; data protection and information sharing; and Internet freedoms and public safety
- ✓ Determining the scope of a NCSS by:
    - o Identifying governmental, national, international and other actors involved in national cyber security
    - o Weighing different approaches to developing a strategy
    - o Identifying target groups for a NCSS
    - o Outlining the subject areas to be addressed
- ✓ Determining the principles for a NCSS
- ✓ Outlining the national position regarding cyber in international affairs and in the context of relevant international organisations
- ✓ Balancing the interests of different stakeholders

IDENTIFYING THREATS AND VULNERABILITIES

NCSS Cyber Risk Assessment

- ✓ Recognising the role of national cyber risk assessment as starting point for the scope and implementation of NCSS
- ✓ Identifying the components of NCSS cyber risk assessment following national characteristics (e.g. dependence on ICT; sources, motivation and nature of cyber threats; specific national interests)
- ✓ Recognising the evolving nature of cyber threats and the ambiguity of cyber threat environment
- ✓ Avoiding simplified and finite judgements

Sources and Nature of Threats

- ✓ Recognising different sources of cyber threats such as:
    - o Accidental cyber security incidents arising from natural causes or system/software malfunctions
    - o Intentional activities of malicious actors, including:
        - ▪ Individuals and groups related to organised crime
        - ▪ Terrorist groups
        - ▪ State or state-supported actors

- ✓ Recognising various actor motivations
- ✓ Acknowledging the nature of threats, including:
  - o Affecting CIS availability (e.g. distributed denial of service (DDoS))
  - o Affecting CIS integrity
  - o Affecting CIS confidentiality (e.g. cyber espionage against governments and critical parts of private sector)
- ✓ Identifying critical threat targets, including:
  - o Governmental CIS
  - o Important private sector CIS, including critical information infrastructure
- ✓ Acknowledging specific concerns such as complication of precise attribution to specific source of threat and the increased organisation and sophistication of threats

General and Specific Vulnerabilities

- ✓ Identifying the degree of dependence of society on CIS and the resulting level of general vulnerability to cyber threats
- ✓ Recognising specific vulnerabilities related to strategic interests of the nation
- ✓ Identifying inherent contributors to cyber infrastructure vulnerability in order to facilitate optimal course of action and the appropriateness, effectiveness, and proportionality of measures planned

DEFINING LINES OF ACTION

General, Legal and Organisational Measures

- ✓ Identifying and prioritising national cyber security lines of action
- ✓ Identifying tasking and responsibilities for particular activities
- ✓ Assessing and revising existing legal obligations in relevant domains in international and national law (e.g. privacy and personal data processing law, telecommunication law, cyber crime and criminal procedural law, critical infrastructure protection and crises management law)
- ✓ Mapping participation and commitments related to international organisations and treaties
- ✓ Assessing existing organisational capabilities
- ✓ Keeping in mind the objective of more efficient communication and coordination among all involved entities
- ✓ Identifying organisational measures for improving national cyber security by:
  - o Reviewing current organisational structures
  - o Defining principles for coordination, cooperation and collaboration
  - o Outlining mechanisms for strategic and political level coordination
  - o Appointing responsible entities on strategic and operational levels as well as the description of their mandate, tasks and responsibilities
  - o Assigning coordination points of contact
  - o Establishing and empowering incident management mechanisms and bodies on the operational level such as CERT
  - o Establishing and improving coordination, cooperation and collaboration, including communications channels and frameworks for information exchange
- ✓ Identifying relevant actors for international cooperation

Awareness Raising Measures and Education

- ✓ Considering the necessity of awareness raising
- ✓ Identifying the audience for awareness measures

- ✓ Determining measures for raising cyber security awareness
- ✓ Considering adding cyber security aspects to education and research

Technological Tools and Measures

- ✓ Developing technological tools in order to increase national preparedness, risk mitigation and measures aimed at facilitating rapid recovery
- ✓ Considering establishing fundamental security requirements, underlining the importance of keeping up with evolving threat environment and supporting cyber security related research and development

Identifying the Scope of CIP Issues in NCSS

- ✓ Outlining the source scope of CIP-related measures and activities to be addressed in NCSSs
- ✓ Identifying the essential components in ensuring resilience of critical infrastructures from cyber threats and ensuring the continuity of vital services, including:
    - o identification of critical infrastructures and their dependency on information infrastructure
    - o supporting CIP by relevant legal regulations
    - o supporting CIP by organisational and technical measures
- ✓ Extending/updating the national crisis management arrangement by core functions for mitigation of cyber threats in critical infrastructure

Roles and Responsibilities in CIP

- ✓ Establishing minimum technical security and procedural requirements for service continuity
- ✓ Establishing a compliance monitoring body and a supervision mechanism to ensure implementation
- ✓ Implement measures for improving the capability to withstand cyber attacks against critical infrastructure (including national cyber risk assessment and contingency planning and exercises)
- ✓ Strengthening cooperation mechanisms between public and private sector stakeholders
- ✓ Defining governmental support to public and private sector responsibilities to ensure integrated approach
- ✓ Inclusion of cyber crisis management capability in the national crisis management system

Information Exchange

- ✓ Strengthening public-private information sharing
- ✓ Ensuring reciprocal information flow between government and private sector
- ✓ Establishing communication in crisis management

Financial Considerations

- ✓ Pinpointing the resources and their allocation for the identified objectives and how these resources are to be used
- ✓ Engaging stakeholders in evaluating the financial aspects of the NCSS measures and activities
- ✓ Involving mechanisms to ensure overall cost efficiency
- ✓ Considering cost-sharing principles between public and private sectors
- ✓ Making sure that resource allocation is consistent with other existing and projected national strategies, policies, and development plans

Implementation Measures

- ✓ Developing and implementing the activities set forward in an Action Plan

- ✓ Defining a coordinating body to oversee implementation
- ✓ Including the NCSS evaluation criteria in the Action Plan
- ✓ Defining the timeline for the implementation

Evaluation and Review of a NCSS

- ✓ Consider periodic review and updating of the NCSS and Action Plan
- ✓ Identify mechanisms for periodic evaluation and review including:
  - Defining variables
  - Assigning responsibility
  - Reviewing and reassessing the NCSS objectives
  - Reporting on the outcome

ANNEX II. LIST OF NATIONAL CYBER SECURITY STRATEGIES

Below is the list of national cyber security strategies that have been used for the development of these Guidelines.

Austria: National ICT Security Strategy Austria. Federal Chancellery, 2012 Australia

Canada: Canada's Cyber Security Strategy: For a stronger and more prosperous Canada. Government of Canada, 2010.

Czech Republic: Cyber Security Strategy of the Czech Republic for the 2011 – 2015 Period. 2011.

Estonia: Cyber Security Strategy. Cyber Security Strategy Committee/Ministry of Defence, 2008.

Finland: Finland's Cyber security Strategy. Government Resolution 24.1.2013

France: Information systems defence and security - France's strategy, 2011.

Germany: Cyber Security Strategy for Germany. Federal Ministry of the Interior, 2011.

Netherlands: The Defence Cyber Strategy. Ministry of Defence, 2012

Netherlands: The National Cyber Security Strategy (NCSS). Strength through cooperation. Ministry of Security and Justice, 2011.

Spain: Spanish Security Strategy: Everyone's responsibility. Gobierno De Espańa, 2011.

United Kingdom: The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. Cabinet Office, 2011.