ASPECTS OF POLICIES AND STRATEGIES FOR CYBER SECURITY IN THE EUROPEAN UNION

Ilina ARMENCHEVA

"G. S. Rakovski" National Defense College, Bulgaria

Freedom and prosperity of mankind greatly depend on an innovative, safe and reliable Internet that, of course, will keep evolving. Cyber space must be protected from incidents, misuse and abuse. Handling the increasing number of threats to cyber security is a challenge that national security and the trend in the international environment face. This makes taking fast and adequate measures at national, European and international level a must. Changing national security strategies and adopting new cyber security strategies are a part of these measures.

Key words: *national security, cyber security, national security strategy, cyber security strategy.*

1. CYBER SPACE. A MEANS OF (UN)CERTAINTY

The open Internet space lays the base of globalization, political and social inclusion worldwide and gives opportunities for interaction and sharing of information and ideas. It is a forum for free speech and exercising basic human rights.

Internet, as well as ICT, is turning into a crucial resource for states and national infrastructures. They are a key factor for security, social and economic growth and stability (see **Table 1**).

Table 1. Before, nowadays and in the future [1]

	2010	*Nowadays*	*2020*
Expected population	6.8 bln	7.3 bln	~8 bln
Expected number of Internet users	360 mln (5 % of the world population)	2.5 bln (35 % of the world population are users)	~5 bln (60 % of the world population are users)
Number of devices	-	12.5 bln devices and technologies using Internet (~6 devices per capita)	50 bln devices and technologies using Internet (~10 devices per capita)
ICT contribution to economy	-	~4 % of GDP for G-20 states	~10 % of world GDP

Critical infrastructure, all state government and economy management structures are entirely dependent on networking IT systems. Vulnerability in cyber space is real, considerable and quickly increasing because of this global networking. The key to adequate neutralizing of all threats to cyber security is their prioritization.

2. FROM THEORY TO PRACTICE IN DEFINING NATIONAL CYBER SECURITY STRATEGIES

To guarantee human rights and freedom in the virtual world, regulations must be developed and a consistent policy should be applied. One of the ways to achieve this is each state to adopt a national cyber security strategy (NCSS).

A lot of issues should be considered in order to reach a definition for a cyber security strategy. First, it is to be clarified what meaning is implied in the basic concepts – cyber space, cyber security, cyber attacks, cyber threats, etc. However, a universal, agreed definition of "national cyber security" (NCS) does not exist. Some that are a symbiosis of "cyber security", "national security", etc. can be found in the strategic state documents. That means each country defines these concepts depending on their own vision.

It must be made clear that the national cyber security is not an end itself. It is a tool to reaching the desired wellbeing of the individual, group of people, organizations, nations and world population. Most of the countries find defining a NCSS as a goal that will provide a secure virtual environment which guarantees economic growth, stable development and protection of people from various risks. Such a general strategy should render an account of a number of indicators like:

- Strategy goal;
- Definition of basic concepts in the sphere of cyber security
- The target group;
- Interested parties;
- Division of the cyber domain;
- Setting strategic goals.

Three conceptual tools are applied in the process of defining a strategy. They are called "the three dimensions", "the five mandates" and "the five dilemmas" of the NCS (**Table 2**). Even though this set of instruments provides an option for prioritizing specific components, depending on the particular environment in each country, it has not been applied uniformly in the existing NCSSs.

Table 2. NCS – basic theoretical approaches [1]

National cyber security Definition	Concentrated application of specific governmental instrumentality and the principles for providing information for public, private and relevant international ICT systems, as well as their shared content, where these systems relate directly to the national security.
The 5 mandates [2]	✓ Military cyber space ✓ Giving account of the cyber crime ✓ Intelligence and counterintelligence ✓ Defense of critical infrastructure and crisis management ✓ "Cyber diplomacy" and managing the Internet
The 3 dimensions/interested parties in NCS	✓ Governmental – "coordination" ✓ International – "Collaboration" ✓ National – "cooperation"
The 5 dilemmas *Balance of expenses and NCS benefits*	✓ Stimulating economy vs. developing national security ✓ Modernizing infrastructure vs. Protection of critical infrastructure ✓ Private sector vs. Public sector ✓ Protecting data vs. Sharing information ✓ Freedom of speech vs. Political stability

3. STRATEGIC GOALS AND INTERESTED PARTIES

NCSS should take into account the different categories of interested parties and their specific roles in the two basic activities: defense and attack. These stakeholders are spread in the government, private sector and international organizations. Thus, for the purpose of the NCSS, governments are to coordinate their actions, cooperate among themselves and the interested parties.

Actually, the ability of the government to react to cyber space threats is limited and likely to be doomed to failure if not cooperating with the rest of the involved in the process.

The continuous dialogue, based on coordination, cooperation and collaboration among stakeholders is a key factor for the success of the NCSS.

4. PROTECTION IN THE CYBER SPACE

It is widely known that it is by far easier to attack than to protect. Weak management allows some countries to become a permanent source of attacks [3].

In response to the attacks, defense actions usually fall into four basic types:

- **Protection –** "applying basic rights" (modern antivirus software for the simplest threats, appropriate configuration of firewalls, etc.);
- **Detection –** proofs for a cyber attack are sought, for something irregular happening in the system (typically, proofs for unauthorized access and data export from the system);
- **Response or reaction –** can be done in numerous and various ways (e.g. deleting a file or activating a firewall, closing a network, changing hardware, etc.). Potential situations related to nationwide cyber attacks which, in theory, could require even a complete Internet cutout;
- **Recovery –** starts right after the cyber attack is mitigated. All systems need a set of backup copies or emergency recovery systems which are to substitute the corrupted or lost data (reserve data centers, information storages, etc.).

From the perspective of NCS, cyber defense is a “collective effort”. The concept of “collective cyber defense” can be interpreted as *“operative cooperation of various (international) participants to defend from specific cyber attacks against one or more of the participants“*. Cyber defense uses the methods of physical obstruction or manipulation of the Internet traffic to limit the cyber attacks; sharing and combining intelligence capabilities, human resources and, even, communication infrastructure. In fact, collective defense can not only deal with “detecting” and “responding to”, but it can also undertake active defense operations. Collective cyber defense is predominantly based on the trust at individual and organizational levels. This trust can even substitute the traditional union structures.

Emergency measures – this broad category includes all ICT which facilitate the activities of the incident response services, except those in the sphere of law enforcement. It may vary from better communication and analysis instruments to national crisis management and continuous protection of critical infrastructure and information flow related to them. As a whole, these systems provide a significantly high security level for specific risks.

From all of the above, we could conclude that there are differences between the developed nations with a high level of ambition for integrating cyber security in their general foreign affairs policy and those dealing with NCS as a task included in the scope of the internal security.

5. POSSIBLE CONTRADICTIONS

Basically, NCS has two axes – military/civilians and intelligence/ law enforcement bodies.

Military/civilians: Contradictions arise when roles and responsibilities are assigned in crisis management and critical infrastructure protection.

Law enforcement bodies/ intelligence: interests in the sphere of intelligence are often in direct contradiction with those of the law enforcement bodies. Intelligence/ counterintelligence and cyber crime counter actions are clearly separate activities, but in case of cyber attacks counter actions differ completely in the following: *transparency, motivation, offensive and sharing.*

6. COMMONALITIES AND DIFFERENCES IN THE NATIONAL STRATEGIES FOR CYBER SECURITY

NCSSs aim to guarantee that states are able to face the cyber security challenges and are aware of the consequences, as well as capable of undertaking adequate measures against violations and crime committed in information systems. Many EU and NATO-member states have issued, are developing or updating their NCSSs. Some of them, as it is the case of the Czech Republic, Estonia, The Netherlands and the UK have already updated their initial strategies.

Table 3. NCSS of EU and NATO-member states

State	Title	Issued
The Slovak Republic	Slovak National Strategy for Information Security [4]	2008
Canada	Canada’s Cyber Security Strategy: For a Stronger and More Prosperous Canada [5]	2009
The Czech Republic	Cyber Security Strategy of the Czech Republic for the Period 2011-2015 [6]	2009
Estonia	Cyber Security Strategy [7]	2014
France	Information systems defense and security. France’s Strategy [8]	2011
Germany	Cyber Security Strategy for Germany [9]	2011
Lithuania	Programme for the Development of Electronic Information Society (Cyber-Security) for 2011-2019 [10]	2011
Luxemburg	Not available on-line	2011
The Netherlands	The National Cyber Security Strategy (NCSS). Strength through Cooperation [11]	2011
Romania	Cyber Security Strategy	2011
Spain	Part of Spanish Security Strategy: Everyone’s responsibility [12]	2011
Switzerland	National Strategy for Protection of Switzerland against Cyber Risks [13]	2012
UK	The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world [14]	2012
USA	The National Strategy to Secure Cyberspace [15] (also CNCI, HSPD-7, 60 day Review)	2003

The European Commission supports the concept that there are still flaws within the whole EU, especially regarding the national capabilities, coordination in cases of incidents abroad, as well as in private sector involvement [16]. The European agency for network and information security is to cooperate and support member-states in their attempts to improve the level of resistance of their national cyber security and provide actual directions for assessing the national strategies, published in the good practices and formulations implementation guide [17] (**Figure1**).

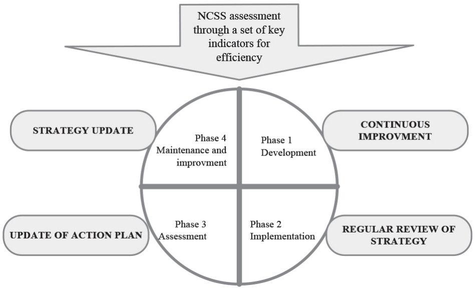
NCSS assessment through a set of key indicators for efficiency
STRATEGY UPDATE
CONTINUOUS IMPROVMENT
Phase 4 Maintenance and improvment
Phase 1 Development
Phase 3 Assessment
Phase 2 Implementation
UPDATE OF ACTION PLAN
REGULAR REVIEW OF STRATEGY

Fig.no.1. Life cycle of NCSS

Because of the lack of a consensus in their understanding, there is not a common definition and universal use of "cyber"-concepts. Reviewing the existing cyber security strategies, it becomes noticeable that a definition of "cyber security" is given in less than the half of them. In some of them the term is looked at descriptively, and in others it is discussed without a particular definition (**Table 3**).

7. GENERAL TRENDS IN FORMULATING A NCSS

Four predominant trends can be observed in analyzing the currently applied national strategies.

- getting closer to a common understanding of key threats and vulnerabilities in cyber space (**Table 4**);
- identifying "new" threats and challenges (climate change, power sources, health risk and cyber security) due to the broader understanding of "security" [18];
- greater awareness of the connection between national and international security;
- admitting the necessity for a full integration of the traditional security policies, economic means and cooperation and development policies.

Table 4. Cyber security in some European strategies [19]

State	Cyber Security
Austria	Cyber security describes the protection of a key legal asset through constitutional means against actor-related, technical, organizational and natural dangers posing a risk to the security of cyber space (including infrastructure and data security) as well as the security of the users in cyber space. Cyber security helps to identify, assess and follow up on threats as well as to strengthen the ability to cope with interferences in or from cyber space, to minimize the effects as well as to restore the capacity to act and functional capabilities of the respective stakeholders, infrastructures and services. [20]
The Czech Republic	Cyber security comprises a sum of organizational, political, legal, technical, and educational measures and tools aiming to provide a secure, protected, and resilient cyberspace [21]
Finland	Desired end state in which the cyber domain is reliable and in which its functioning is ensured... Note 1 ... the cyber domain will not jeopardize, harm or disturb the operation of functions dependent on electronic information (data) processing. Note 2 Reliance on the cyber domain depends on its actors implementing appropriate and sufficient information security procedures ..... Note 3 Cyber security encompasses the measures on the functions vital to society and the critical infrastructure which aim to achieve the capability of predictive management ... [22]
France	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. [23]
Germany	"Cyber security" and "civilian and military cyber security" (Global) cyber security is the desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum. [24]
Hungary	Continuous and planned taking of political, legal, economic, educational, awareness-raising and technical measures to manage risks in cyberspace that transforms the cyberspace into a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risks in cyberspace. [25]
The Netherlands	Cyber security refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred. [26]
Turkey	Protection of information systems that make up the cyber space from attacks, ensuring the confidentiality, integrity and accessibility of the information being processed in this space, detection of attacks and cyber security incidents, putting into force the countermeasures against these incidents and then putting these systems back to their states previous to the cyber security incident. [27]

Table 5. Threats, vulnerabilities and challenges in national strategic documents

State	Document	Year	Key threats/vulnerabilities
France	White book	2008	„Weapons of mass destruction“ (WMD); terrorism;proliferation of ballistic missiles; *cyber attacks*; espionage; criminal networks; health risks; citizens in vulnerable regions abroad.
Germany	White book	2006	International terrorism; proliferation and military buildup; illegal trafficking of weapons; weak state system; transport routes; energy security; uncontrolled migration; epidemics and pandemics.
Hungary	Security strategy	2012	Terrorism; proliferation of WMD; unstable regions/unsuccessful membership; illegal migration; economic instability; challenges to information society; global natural, manmade and medical sources of dangers; regional and internal challenges.
The Netherlands	Security strategy	2007	Violations of international peace and security; CBRN weapons; terrorism; international organized crime; social vulnerability; lack of digital and economic stability; climate changes and natural disasters; infectious and animal diseases.
Poland	Security strategy	2007	Organized international terrorism and crime; power security; illegal migration; weakened transatlantic connections; frozen and regional conflicts; low levels of integration of economic life and financial markets; environmental threats; internal challenges.
Spain	Security strategy	2011	Armed conflicts; terrorism; organized crime; financial and economic instability; power vulnerability; proliferation of WMD; cyber threats; uncontrolled migration flows; disasters and emergencies; critical infrastructure; supplies and services.
UK	Security strategy	2010	International terrorism; hostile attacks in the cyber space; natural disasters and incidents; territorial attacks; risks of high instability; organized crime; disturbances in satellite communications; cutting off basic resources or oil/gas supplies.

8. BASIC TRENDS IN NCSS

A number of basic trends can be observed when analyzing the existing NCSS:

- sustainability of a safe, stable and reliable electronic and operational environment;
- fostering economic and social wellbeing, trust and economic growth;
- overcoming the risk to ICT;
- strengthening infrastructure stability.

In regard with the vision for cyber security, each state has one of their own. They apply different approaches in developing the strategy, reflecting the particular understanding for cyber space and cyber threats. Still, despite the differences, common trends can be observed as follows:

- globalization;
- critical infrastructure;
- economic prosperity;
- national security;
- social wellbeing;
- public trust in ICT.

To apply appropriate protective mechanisms, in the process of research and categorization of the new threats, the threat vector and its characteristics (starter, direction and size) are to be described. It is necessary to clarify what the sources and aims are, as well as what the scope/comprehensiveness is. Accordingly, in regard with these parameters, the following categories can be determined:

- broad scope attacks;
- terrorist attacks;
- foreign threats;
- corporative espionage;
- organized crime;
- political activism against ICT-based services.

In the NCSS developed so far, these categories are partially or fully adopted and, in accordance with the particular security environment, each country supplements the list with others.

Are there common goals? Each NCSS goals are set in a short and long term plan and are implemented through consecutive targeted actions and processes which protect the country from cyber threats and provide for its vital functions. Success indicators are determined for the major part of the goals. They are followed by planned monitoring activities. Some of the goals are shared, as others (e.g. reaching balance between human rights and cyber security in the legislation) are specific for the particular country. Goals are often distributed in topical areas like:

- measures at legislative level and cooperation with stakeholders;
- critical Information Infrastructure Protection (CIIP);
- risk assessment of critical infrastructure;

- security of services in cyber space.

As a whole, activities undertaken in EU-member states are similar. Some of them are typical, and others, like enforcing security standards and good practices, are definitely rarer. The activities are the basic interventions through which the final outcome and goals of the project are achieved (building up capacity, legislative initiatives, risk and threats assessment, increasing awareness). They are usually described through plans for implementing the strategies at a national or institutional level, depending on how much centralized the system is.

9. A SYSTEM VIEW OF NCSS

"INPUT DATA" FOR NCSS

"Input data" state the resources granted for the implementation of a NCSS which, at strategic and program levels, originate from the particular goals in the NCSS. They include financial, human, legislative, institutional, educational, legal, etc. types of goals.

"OUTPUT DATA" FOR NCSS

"Output data" are the actual results of program activities. They generally relate to the key indicators and are able to guarantee good financial management and implementation. Thus, "output data" are the outline for the program implementation reports.

OUTCOME AND EFFECTS

The outcome reflects short- and mid-term implementation of the program, as the effects provide results in a longer term period (10+ years). The short- and mid-term outcome relates to the stability and cooperation and directly derives from the activities stated in the strategy. In turn, the effects are long term goals focused on the cyber space security and are set in the program in their short- and mid- term plans.

INTERESTED PARTIES

Bearing in mind the nature of cyber space, *by default*, *all users are interested parties*. This makes crucial each interested party to be aware of their responsibilities. The role of every interested party varies due to their capabilities and resources.

10. INITIATIVES IN THE SPHERE OF CYBER SECURITY IN BULGARIA

Currently, in Bulgaria, the documents related to cyber security policy and strategy are being developed. Some initiatives and results can be reported.

- In meeting EU and NATO requirements, Computer Emergency Response Team (CERT) Bulgaria is open in November 2008. It is a structure subordinated to the Ministry of transportation. Its mission is to support the users of the services meant to reduce the risks in case of information security incidents and to assist the counteractions when such happen.
- Another initiative is the round table on the topic of *"Cyber space security in Bulgaria - current status and challenges"* held in September 2010.
- In 2010, in accordance with a decision of the State Commission on Information security, a point of contact for Bulgaria is nominated to the EU project "Incident Network Security Management".
- On May 25, 2011, the government approves a Memorandum of understanding for a future cooperation in the sphere of cyber security between NATO cyber security management body and the national cyber security structures.
- In November 2011 a Memorandum is signed, dealing with the information systems of the administrative bodies and classified information networks. It regulates issues of the goals and scope, current legislation, financial conditions on its application, regulations for using shared information, the ways of resolving disputes, means for its amendment or termination.
- In September 2011, an Interagency working group on the issues of cyber security is created. It is tasked to develop a proposal for the composition, powers, mission, functions and tasks of a national authority on cyber security in Bulgaria and prepare a draft Decision of the Ministerial Council for its establishing in the structure of the security system. In the January 2012 report of the group the current cyber security status is analyzed and the following findings are noted:

- Legal-normative regulation of the issues of critical communication and information infrastructure cyber security, as well as a national policy and strategy for cyber security do not exist;
- There is no legal provision establishing a unified coordination of information protection.

- In May 2013, the Prime Minister issues an order that establishes an Interdepartmental Working Group, tasked to prepare a draft Cyber Security Strategy for the Republic of Bulgaria. The Minister for Development of e-government is assigned as a Chairman, and the Minister of Defense is to execute control over the implementation of the order.
- In September 2014, the Minister of Defense appoints a national coordinator for cyber defense and cyber security, with the task of quickly finalizing the strategy for cyber security. The coordinator is equidistant from the various agencies, works in collaboration with industry and academia, and represents the country in the EU, NATO, UN and other bodies concerned with this problem.

Even a quick review of the status of activities in cyberspace in Bulgaria shows that, so far in public life, there is no comprehensive vision on cyber security. There are more sporadic than consistent successive actions in response to specific procedures in the EU or NATO, aimed at achieving an explicit goal. At the same time, as a full EU and NATO-member, Bulgaria has its commitments to the common security and defense policy, which include elements of the joint action in the field of cyber security.

11. CONCLUSION

All governments face the constantly rising level of cyber threats, which requires recognizing these problems, formulating goals and developing a strategy to solve them. The establishment of a national cyber security strategy is a challenge and coordination is needed between the various governmental and non-governmental parties, the public and private sectors.

Since each country has its own priorities and problems, no general framework for national cyber security exists. Each government provides a special individual set of circumstances and the developed strategy meets the particular requirements. It describes the specific governmental instrumentality and the principles of ensuring the security of information in public, private and international ICT systems that directly relate to national security. It is a tool that is beneficial to the government and all stakeholders.

NOTES & REFERENCES

[1] Klimbura, Alexander (Ed), National cyber security Framework manual, NATO Cooperation Cyber Defense Center of Excellence (CCDCOE), Tallinn, Estonia, 2013, p. 234

[2] Ibidem.

[3] Klumburg, Al. and Mirth, Ph."Cyberspace and governance-A primex" (working paper 65), Vienna, 2012.

[4] Edward Snowdon, former NSA contractor, who in 2013 revealed information about American surveillance and tracking telecommunication programs and was granted a 3-year asylum in Russia.

[5] http://www.webcastlive.es/4enise/archivos/T14/T14_Daniel_Olejar_CominiusUniversity.pdf.

[6] Canadian Department for Public Safety, Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada.

[7] Czech Ministry of Interior, Czech Cyber Security Strategy for the Period 2011–2015 (Prague: ENISA, 2011).

[8] Estonian Ministry of Defence, Cyber Security Strategy (Tallinn: Estonian Ministry of Defence, 2008).

[9] French Secretariat-General for National Defence and Security, Information systems defence and security. France's strategy.

[10] German Federal Ministry of the Interior, Cyber Security Strategy for Germany.

[11] Lithuanian Government, Resolution NO 796 on the Approval of the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019 (Vilnius: Information Technology and Communications Department, 2011).

[12] Dutch Ministry of Security and Justice, 'The National Cyber Security Strategy (NCSS). Strength through Cooperation'.

[13] Spanish Government, Spanish Security Strategy. Everyone's responsibility.

[14]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.

[15] UK Cabinet Office, The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.

[16] White House, The National Strategy to Secure Cyberspace

[17] 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-animplementation-guide 6 ENISA. (2012a).

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

[19] Barry Buzan, Ole Wæver, and Jaap de Wilde, Security. A New Framework For Analysis (London: Lynne Rienner Publishers, Inc., 1998)

[20] Cyber Definition, CCDCOE, https://ccdcoe.org/cyber-definitions.html

[21] Austrian Cyber Security Strategy (2013): https://www.bka.gv.at/DocView.axd?CobId=50999.

[22] Czech Republic Draft Act on Cyber Security (2014).

[23] Finland's Cyber Security Strategy Government Resolution (Jan 2013).

[24] nformation Systems and Defence – France's Strategy (2011).

[25] Cyber Security Strategy for Germany (2011).

[26] National Cyber Security Strategy of Hungary (2013).

[27] National Cyber Security Strategy 2 - From Awareness to Capability (2013).

[28] National Cyber Security Strategy and 2013-2014 Action Plan.