DE GRUYTER OPEN

Land Forces Academy Review
Vol. XXIII, No 2(90), 2018

NATIONAL CYBER SECURITY AS THE CORNERSTONE OF NATIONAL SECURITY

László KOVÁCS
National University of Public Service, Budapest, Hungary
kovacs.laszlo@uni-nke.hu

ABSTRACT

The more advanced digital economy and society a country has the more exposed it is to cyber threats. Consequently, countries with advanced digital economy and digital infrastructure naturally need to pay more attention to protecting cyber space. Today it is a national security issue and it can no longer be argued that cyber security is its indispensable part. Accordingly, a national cyber security strategy has to be built on national security strategy. That is the main reason for using the word "cornerstone" in the title of this study. The relation between national security and national cyber security means a specific context, which is one of the subjects of our examination in this study. Today, most countries have a cyber security strategy. However, these strategies are mostly static documents that do not or only partially can handle the dynamism that characterizes cyberspace. This paper focuses on the key issues that are needed for developing a usable cyber security strategy.

KEYWORDS: cyber security, framework, national security, strategy

1. Introduction

States need flexible and dynamic cyber security strategies to react to the cyber threats in a constantly changing and emerging environment such as cyberspace. Although cyberspace has no physical boundaries countries often formulate cyber security strategy independently based on their own ideas and own security perceptions only. This causes very different cyber security strategies to be found in different countries. This is true although many international agencies and research institutions offer suggestions to formulate the main aspects and elements of national cyber security strategy.

When analysing the cyber security strategies of European countries, we can see that in many countries, in the early times, the development of their national cyber security strategy started from the point of view of information society and its security projections, while other countries had different approaches, like critical information infrastructures and their security issues. Today many countries have their second or even third issued and updated strategy for national cyber security, but they are very different.

These are the main reasons why we briefly introduce the main suggested toolboxes for national cyber security strategy from the NATO Co-operative Cyber Defence Centre of Excellence (CCDCOE), the European Union Agency for Network and Information Security Agency (ENISA) and the United Nations' International Telecommunication Unit

DOI: 10.2478/raft-2018-0013

(ITU). These suggested frameworks were made around 2012, and they provide philosophical bases with scientific methods and define a set of recommendations that should preferably be a basis of a national security strategy.

2. NATO Co-operative Cyber Defence Centre of Excellence's Framework Manual for National Cyber Security Strategy

In 2012, the Tallinn (Estonia) based NATO Co-operative Cyber Defence Centre of Excellence issued a study collection titled "National Cyber Security Framework Manual". The main goal of the book is the following: *"it provides detailed background information and theoretical frameworks to help the reader understand the different facets of national cyber security, according to different levels of public policy formulation. The four levels of government – political, strategic, operational and tactical (technical) – each have their own perspectives on national cyber security, and each is addressed in individual sections. Additionally, throughout the Manual there are call-out boxes that give examples of relevant institutions in national cyber security, from top-level policy coordination bodies down to cyber crisis management structures and similar institutions"* (Klimburg, 2012, p. XV.).

The study collection begins with an overview section in which, after terminology, the first part deals with the question of how national security and national cyber security are interrelated in a given country. There are several examples of these contexts, since 2007, many countries have explicitly included cyber threats and their need to address the national security strategy. The book reviews the conceptual architecture of the national cyber security strategy, namely, what the strategic goals should be, who the target audience of the strategy would be, and what the strategy must include in different dimensions on governmental, national and international levels. The study suggests examining five different areas in the national cyber security strategy. These five areas: cyber warfare, cybercrime, cyber espionage, critical infrastructure protection (as a national security interest), and cyber diplomacy with internet governance (Klimburg, 2012).

Regarding national security, the book identifies five dilemmas that influence the discussions on the most fundamental issues of national security strategy. However, only some of these issues belong directly to a country, while some others refer outside the country. In this aspect these dilemmas are international, since a possible development (or its negative change) in the security of a country influences the international environment as well.

The first issue or dilemma is the following: is the increase of the competitiveness of the economy opposed to national security? What may be a major issue, among other things, is that the speed of the development of information technology, which is a basic necessity and in many cases the driving force of economy, is much faster than that of its protection. This involves the risk that rapidly evolving ICT systems will contain a number of vulnerabilities and through them cyber-attacks will not only negatively affect business (or public administration) but the interconnection of these systems, which means high interdependence, will have negative implications for other systems as well. This can cause system failures and malfunctions that pose a very serious national security risk.

The next dilemma: does the rapid modernization of infrastructure involve the growth of vulnerability of critical infrastructures? Regarding this question the study emphasizes that the state is not only a coordinator, but also the highest-level player in the implementation and guarantee of defence. In this meaning, a good

example for that is the national cyber security strategy of the United Kingdom, which emphasizes: *"Government has a clear leadership role, but we will also foster a wider commercial ecosystem, recognising where industry can innovate faster than us. This includes a drive to get the best young minds into cyber security"* (HM Goverment, UK, 2016, p. 7).

The third dilemma is the relation between public and private sectors. It could be stated that public and private sectors should be jointly responsible for the state. Therefore, the connection has to be regulated and it should be a part of the national cyber security strategy. Many countries' national cyber security strategies include this important factor. In 2018 the new National Cyber Security Strategy of the Netherlands formulated this task as follows: *"In recent years, various initiatives have been taken by public, private and public-private sectors to strengthen cyber security in the Netherlands. To monitor that direction, it is needed to follow the approach, but in a higher speed"* (Netherlands, 2018, p. 43).

The next question is the data protection versus information sharing. On this issue citizens have a legitimate interest in living in an open society where the free and limitless flow of information is a fundamental right but at the same time it is a task for the government because this information must be protected by the state and other stakeholders. It is not only a privacy issue because today in anti-cybercrime activities or in the fight against terrorism there is a huge need for the exchange of information that has so far not been a matter of day-to-day interactions between citizens and the state or some of its authorities. Therefore, it is also a national security matter now.

The fifth serious dilemma is the question of the freedom of expression and political stability. Moreover, this question itself includes many sub-questions. Firstly, by using information communication tools, citizens have the opportunity to take part in making political decisions. By using these tools and systems, they can express their sympathy, support, or disagreement on political decisions, additionally they can do it more effectively than ever before. Secondly, for example, is a private enterprise operating a street-monitoring system allowed to transfer pictures and recordings of street protesters to law enforcement or national security organs? These are really serious questions on national security (Klimburg 2012).

The document identifies interested parties in three dimensions when developing their national cyber security strategy. These three dimensions are the dimensions of government, national (social), and international actors. Obviously, of these dimensions the government must be the coordinator and it must coordinate most of the questions between stakeholders and cyber security.

Presenting the most important goals of the national cyber security strategy, the study states the following factors (Klimburg, 2012):

- cyber security and its strategy has to contribute to national security;
- the different approaches of national cyber security strategy (i.e. military and civil) may cause frictions;
- numerous national features should be considered in the development and implementation of national cyber security strategy;
- appropriate resources must be allocated to national cyber security strategy and quantified and measurable goals should be defined;
- the development of human resources needed to create cyber security is often more difficult than anticipated.

Concerning the development of a cyber security organizational system at national level, the study also sets out a number of issues that appear as an important

factor both in the development of the strategy and in its implementation. As we mentioned above, a national cyber security strategy can be divided into five distinct areas: military (i.e. cyber warfare), cybercrime, critical infrastructure protection, crisis management, and cyber diplomacy. These areas need to be mapped on political, strategic, or even operation levels and the organizational framework should be developed accordingly (Klimburg, 2012).

3. The Proposal of the European Union Agency for Network and Information Security for the Elements of National Cyber Security Strategy

ENISA as one of the key organisational players in the cyber security of the EU has identified common the elements in existing national cyber security strategies that can be the basis of a model to build a coherent and responsive cyber security strategy. Based on these analyses the ENISA issued a guidebook titled the National Cyber Security Strategies Practical Guide on Development and Execution in 2012. This book is *"aiming to identify the most common and recurrent elements and practices of national cyber security strategies (NCSSs), in the EU and non-EU countries"* (ENISA, 2012, p. 6).

In this volume ENISA emphasizes the importance of the system of international cooperation. Obviously, one of the basic conditions for international cooperation is that countries must have cyber security policies or strategies and an appropriate organizational system capable of enforcing them, which are set out in comprehensive strategies. At the same time, a comprehensive terminological standardization would be welcomed because, as ENISA pointed out in its guidebook, countries still differ in what is known as the cyber space.

ENISA has taken a step-by-step approach in the collection of the guidelines which as recommendations has been listed, which are the most useful steps to develop a cyber security strategy at national level. Therefore, the document could be described as *How to make a national cyber security strategy*. Additionally, the guidebook cites many examples from existing cyber security strategies, which are presented as good practices in the document.

At the same time, ENISA compares the national cyber security strategy that defines cyber security into a two-phase life cycle in which the first phase is the creation and implementation of the strategy (and then apparently, its operation under the principle, legislative and organizational frameworks), and the second phase is the revision, and based on the conclusions and experience that have been drawn, the necessity of changing the strategy.

In the development of the cyber security strategy, ENISA's recommendation presents numerous logical steps. The first step obviously must be the definition of the most important goals. The second step is risk analysis, and it should be followed by assessing the current situation, including the current regulatory environment, then a clear cyber security organisational system has to be outlined.

However, based on the above-mentioned study, ENISA revised the recommendations and published a new practice guide to design and implement national cyber security strategy just after 4 years that the first guidebook was issued. The new version has been published in late 2016 with the title *NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies* (ENISA, 2016).

In the updated recommendation, ENISA has defined a lifecycle for the cyber security strategy divided into four main phases. The first phase is the development of the strategy. The second life cycle stage is the introduction and operation of the strategy. The third step is the evaluation phase followed by the maintenance phase (ENISA, 2016).

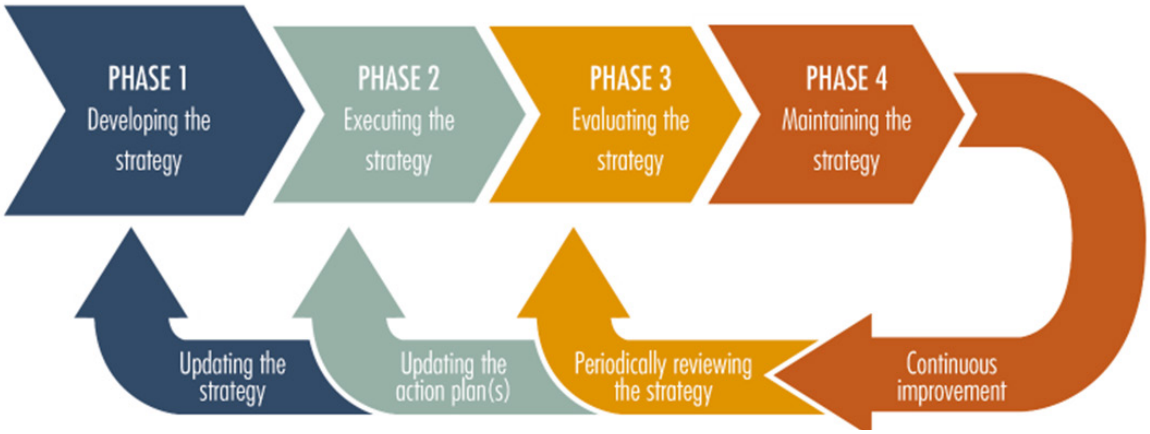

Figure no. 1: The ENISA four-phase recommendation for lifecycle of national cyber security strategy (source: ENISA, 2016)

All phases include feedback sessions, where the continuous development of the strategy is one of the most important priorities. These feedbacks give opportunity to balance and if necessary slightly change the strategy for the responsible organizations, but these feedbacks also mean tasks for them. The strategy needs to be revised at regular intervals, updated action plans, and the strategy itself must be upgraded (ENISA, 2016).

The original recommendation issued in 2012 contained 20 steps to introduce and maintain cyber security strategy, but it focused only on the first two phases of the above mentioned-life cycle. However, the updated edition in 2016 introduces a much clearer and more structured system. In this context, the recommended tasks could guarantee a truly effective and functional national cyber security strategy. Additionally, a very new and very strong regulation has been born in the European Union that is the NIS Directive, whose official title is *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. The ENISA recommendations for national cyber security strategy take into consideration the main questions that are regulated by NIS (NIS Directive, 2016; ENISA, 2016).

One of the best examples of integrating NIS into cyber security strategy is the Polish national cyber security strategy titled National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022, which underlines: *"The most far-reaching changes will result from the obligation to transpose […] the NIS Directive, into Polish law. It contains security and notification requirements for operators of essential services (such as energy or transport) and for digital service providers (e.g. cloud computing, search engines) and establishment of several cooperation or coordination mechanisms"* (Ministry of Digital Affairs, Poland, 2017, p. 8).

As referred earlier, the new guidelines of ENISA and its life cycle elements not only focus on creating and implementing the strategy, but also emphasize assessing and maintaining existing organizations, processes and their effects. In the assessment of the strategy, ENISA proposes the development and introduction of a so-called Key Performance Indicator (KPI). Based on these KPIs, it is possible to assess which of the most important objectives have been achieved and which ones have not been reached or not in the right way. The indicators were divided into 5 large groups by ENISA, which include the main indicators of the area to be measured and evaluated. These

groups are: developing cyber policies and capabilities, achieving cyber resilience which could be reached by developing skills and effective cooperation between the public and private sectors, reducing cybercrime, developing the industrial and technological bases of cyber security, and secure critical information infrastructure. These elements of national cyber security greatly contribute to reaching the main goals of national security; therefore, the national strategy has to include such a kind of elements (ENISA, 2016).

4. International Telecommunication Unit's Recommendations for National Cyber Security Strategy

In 2007, ITU launched the Global Cyber Security Agenda (GCA). The GCA is a framework for international cooperation to enhance the security of information society. The five pillars of the GCA, namely the promotion and enhancement of legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation, aimed at developing an effective information society security based on international cooperation that minimizes overlapping between different areas and activities (ITU, 2007).

Building on the GCA, ITU issued its own manual for national cyber security strategies in 2011. This study *"is a reference model for national cybersecurity strategy elaboration"* (ITU, 2011, p. 5).

ITU's study book, titled *ITU National Cybersecurity Strategy Guide,* begins with a global cyber security situation and information security analysis in which the global and national economic situations, and the cyberspace and its systems and services are analysed. The global situation analysis basically reflects the activities of the United Nations in the area of information society and cyber security.

The document discusses the national cyber strategy with the special focus on the following elements (ITU, 2011):

- cyber security accountability of government: the main decision makers of the country (mostly the Government) are responsible for cyber security, therefore they should be accountable;
- role of national cyber security coordinator: it could be an office or an individual who coordinate most of the cyber activities supporting cyber security;
- centralised national cyber security entity: it is responsible for handling cyber threats;
- legal environment: establishing legal frameworks against cybercrime, to protect critical infrastructure and critical information infrastructure, and legal bases to establish and operate cyber security organisations;
- framework for national cyber strategy: there is a huge need to adapt the most valuable factors from international best practices such as risk management and compliance, which could be the bases of national cyber security;
- computer incident handling: it is a national task for every country to build up capabilities and organisations for computer incident responses;
- cyber awareness, training and education: there should be formulate a cyber security training and education programme on national level which could contribute to the cyber awareness of the society;
- public-private partnership: one of the main tasks of the government should be to create a dependable and functional partnership among the public and private stakeholders regarding on various cyber related fields;
- international cooperation: cyber threats cannot be handled only within the boundaries of a country; therefore, narrow international cooperation is needed to handle the continuously emerging threats and challenges in the cyber space.

This is followed by the presentation of a national cyber security context, with focus on critical infrastructures and critical information infrastructures.

The French national security strategy and national cyber security strategy have been following this approach since 2008. As the new national cyber security strategy of France stated in 2015: *"As was announced in the 2008 French White Paper on Defence and National Security, a national agency was created as of 2009 to address cyberattacks and to protect the State information systems and critical infrastructures"* (Premier Ministre, 2015, p. 8).

The ITU study book contains the recommendation of the national cyber security strategy model based on above-mentioned examinations. The model presents a holistic approach to the proposed structure of cyber security strategy. In this document ITU recommends certain elements for the cyber security programme. The proposed holistic, national cyber security strategy, which integrates as many stakeholders as possible, overlaps with the previously presented and analysed ENISA recommendation (ITU, 2011).

5. Conclusions

When a country develops its cyber security strategies at national or federal level, it is a very difficult question what issues are covered by the specific strategy, how and in what form it is intended to address cyber-challenges.

In accordance with the above-mentioned difficulties it is necessary to take into account the recommendations made by the international organizations, which can serve as a basis for building a country's national cyber security strategy and its key regulatory issues. This enables the possibility that, although the countries at national level form a cyber security strategy, they can still be in line with each other, with the same philosophical background, and thus more or less independent of the strategic ideas that are in the same direction from the interests and values of the given country.

From the comparison of the guidelines of ENISA, ITU and CCDCOE we can conclude that while ENISA proposes quite concrete steps to develop and operate a cyber security strategy at national level, ITU has come up with a more comprehensive, more model-oriented proposal package. At the same time, both documents build on the principles that are formulated in the CCDOE recommendations.

It is also apparent from the above-mentioned considerations that the studies contain a number of carefully thought-out propositions that can really be the basis and may be used as a leader in a nation's decision-making, in developing a cyber security strategy for a particular country, or in revising an existing strategy.

Most of the noted studies emphasize that cyber security strategy is a tool to reach the national security goals, not a solution for everything. That's why a national cyber security strategy must be harmonized with other strategies which are addressed to support the nation's security.

REFERENCES

European Network and Information Security Agency (ENISA). (2012). *National Cyber Security Strategies Practical Guide on Development and Execution,* available at: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport, accessed on: 29 May 2018.

European Network and Information Security Agency (ENISA). (2016). *NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies,* available at: https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport, accessed on: 29 May 2018.

HM Government, United Kingdom (2016). *National Cyber Security Strategy 2016-2021,* available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, accessed on: 29 May 2018.

International Telecommunication Union (ITU). (2007). *Global Cybersecurity Agenda (GCA),* available at: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx, accessed on: 29 May 2018.

International Telecommunication Union (ITU). (2011). *ITU National Cybersecurity Strategy Guide,* available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf, accessed on: 29 May 2018.

Klimburg, A. (ed.). (2012). *National Cyber Security Framework Manual,* available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/NCSFM_0.pdf, accessed on: 29 May 2018.

Ministry of Digital Affairs, Poland. (2017). *National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022,* available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf, accessed on: 29 May 2018.

Netherlands. (2018). *Nederlandse Cybersecurity Agenda Nederland digitaal veilig,* available at: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig/CSAgenda_def_web.pdf, accessed on: 29 May 2018.

NIS Directive (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,* available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN, accessed on: 29 May 2018.

Premier ministre. (2015). *French National Digital Security Strategy,* available at: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf, accessed on: 29 May 2018.