Source: **Jozef Vyskoc**
CEPIS LSI SIN

Version: v1.1 /9.3.2018

Document for:

Decision	
Discussion	
Information	x
Publication	

Best practices for a journey towards secure cyberspace

Preamble

This statement collects and comments on official documents aiming towards a secure cyberspace. Its aim is to be a backgrounder for the statements on good or bad practice with regard to cybersecurity that can be derived from its “Conclusion” section.

1. Introduction

Though individual initiatives for some time tried to achieve some order in cyberspace, the publication of the Cybersecurity Strategy of the European Union[1] in 2013 can be regarded as main push towards the systematic effort to ensure cybersecurity in national and international contexts. Nowadays all EU Member States as well as many others have adopted their national cybersecurity strategies (NCSS) – their list is maintained by the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE)[2].

However, the complexity, variability, borderless nature and other characteristics of cyberspace make a path towards the creation of a secure cyberspace for businesses, communities and individuals long and demanding. As countries are still in early phases of their march towards the goal, it is important to ensure they are well prepared and equipped for a journey in such largely unexplored and changing terrain. The very existence of NCSS represents just a first step of the journey.

2. The ENISA Guidance on NCSS implementation and the need to go beyond it

A peek at the NCSS implementations is offered by the European Union Agency for Network and

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667

[2] Cyber Security Strategy Documents https://ccdcoe.org/cyber-security-strategy-documents.html

Information Security (ENISA) in its National Cyber Security Strategy Good Practice Guide[3] (first published in 2012, updated in November 2016). There (Chapter 4), 15 objectives for the implementation of „National cyber security strategies (NCSS)" are suggested. Also (Chapter 6) a list of possible key performance indicators (KPIs) for the objectives is presented and subsequently used to examine status of their implementation for 16 EU Member States plus Switzerland (who participated in the study). A low degree of implementation (meaning fewer than 10 countries have largely implemented the objective) was found for 4 objectives, a medium degree of implementation (10 to 16 countries have largely implemented the objective) was concluded for 6 objectives while for only 5 objectives the study claims a high degree of implementation (meaning more than 16 countries have largely implemented the objective).

The approach of the NCSS Good Practice Guide has some serious limitations, though. One should not forget that the study is aimed to just examine the pace of implementation of NCSS while silently assuming that all NCSS provide an appropriate and holistic guide to achieve the overall goal, i.e. a secure cyberspace. It should be clear, however, that a weak or incomplete NCSS may lead the whole effort to a dead end, thus the quality of a cybersecurity strategy is at least as important as the pace of its implementation.

A closer examination shows that ENISA in its study focused on operational issues like incident management, education and awareness raising, sharing of information, protection of critical (information) infrastructure. While such objectives have their value, the focus on managing individual incidents (be it real or just potential) does not improve the high-level decision-making capacity needed for long-term success in reducing cybersecurity risks over time[4].

A nice example of a high-level decision to reduce cybersecurity risks has been provided by the Singapore government who decided that all computers used officially by public servants have to be cut from the Internet[5]. Such a move is beyond the set of objectives considered by ENISA's NCSS Good Practice Guide. In other words, ENISA's study lacks examining NCSS from the point of view of their capability to introduce and support political-strategic decision-making aimed at achieving an open, safe and secure cyberspace. We believe a study aimed at this guiding how to achieve a secure cyberspace may help in early identification of potential weaknesses in NCSS and related important documents.

3. NCSS and political-strategic aspects of a journey towards a secure cyberspace

There is no single way how to prepare a national cybersecurity strategy and it shows – examined national cybersecurity strategies represent a mixture of documents of different size, scope, priorities and other characteristics. In order to analyze whether and to what extent NCSS address

[3] NCSS Good Practice Guide – Designing and Implementing National Cyber Security Strategies, November 2016 (update of the first version of the guide in 2012) https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[4] J.Whitsitt: The trap of information security & escalating cyber risk. In: European Cybersecurity Journal Vol. 2 (2016) Issue 3, pp.47-52 https://cybersecforum.eu/files/2016/12/ecj_vol2_issue3_j.whitsitt_the_trap_of_information_security_and_escalating_cyber_risk.pdf

[5] Singapore public servants' computers to have no Internet access from May next year. http://www.straitstimes.com/singapore/singapore-public-servants-computers-to-have-no-internet-access-from-may-next-year

political-strategic aspects of achieving the overall goal we need a basic framework enabling the evaluation of just this part of the individual national strategies. Hopefully by comparing (key domains of) such a framework with individual NCSS a sort of "best practices" to deal with political-strategic aspects can be determined.

The political-strategic level of cyber-related activities may be achieved simply by a call for establishing a specific body explicitly tasked with coordination of cybersecurity efforts at the political-strategic level. Another possibility is to achieve the goal indirectly by specifying priorities which are of strategic nature, hence impossible to be achieved by operational measures only. For example, the Cybersecurity Strategy of the European Union states 5 strategic priorities, namely:

1. Achieving cyber resilience,
2. Drastically reducing cybercrime,
3. Developing a cyberdefence policy and capabilities related to the Common Security and Defence policy (CSDP),
4. Developing the industrial and technological resources for cybersecurity,
5. Establishing a coherent international cyberspace policy for the European Union and promote core EU values

Of these priorities the first one (achieving cyber resilience) is closely related to the so-called NIS Directive[6] which itself represents a collection of operational best practices, thus clearly belongs to the operational level, while the rest of the priorities is of a more strategic nature.

As the Cybersecurity Strategy of the European Union is not related to a particular country, we consider it to be an appropriate inspiration for a common framework to evaluate individual national strategies. That is what follows: individual NCSS[7] will be examined as whether and to what extent they cover the following domains:

1. SBS: Creation of a ***s***pecific ***b***ody explicitly tasked with the coordination of cyber***s***ecurity efforts at the political-strategic level;
2. TNC: Active cooperation with the international community to address ***t***rans***n***ational ***c***ybersecurity issues, cyber norms and legislation;
3. ITPI: Development of ***i***ndustrial and ***t***echnological resources for the national or international cybersecurity ecosystem, towards e.g. highly secure ***p***roducts or ***i***nnovative approaches towards cybersecurity;
4. RCC: ***R***eduction of ***c***yber***c***rime to create a safer cyberspace.

Of course individual NCSS likely do not use the same wording and some effort is needed to recognize whether the NCSS touches in a significant manner one or more of these domains. Moreover, one has to distinguish between just superficial mentioning and a documented intent to achieve the goal or to devote time and resources to deal with the respective domain. We suggest the simple rule of thumb for the domains above:

1. SBS: The body in question has to be explicitly tasked with coordination at the political-strategic level and so different from the one tasked with operational issues, that resources for the coordination are not used up in day-to-day operations.

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems accross the Union http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

[7] more precisely their English language version

2. TNC: The cooperation has to be active and address transnational cybersecurity issues, ordinary participation on cybersecurity exercises or cooperation of CERT-like bodies belong to operational level.
3. ITPI: Measures considered as a minimum have the potential to stimulate the demand for highly secure products, innovative approaches towards cybersecurity, etc.
4. RCC: Both strong and effective legislation as well as measures to enhance capabilities to combat cybercrimes have to be considered.

4. The common framework applied to individual NCSS

According to our understanding of (the English language version of) a sample of NCSS the framework domains are covered there as follows:

Legend: ● – covered, Blank – not covered, ○ – partially/superficially covered

Framework domain	**AT**	**CY**	**CZ**	**DE**	**DK**	**EE**	**ES**	**FI**	**FR**	**HR**	**HU**	**IE**	**IS**	**IT**	**LT**	**LU**	**LV**
1 SBS	●			○		●	●		○	○	○			○			○
2 TNC	●	○	●	●	●	●	●	●	●	●	○	●	○	●		●	●
3 ITPI	○	○	●	●		○	●	○	●	○	○			●			
4 RCC	○		●	●	●	●	●	●	●	●		●	●			●	●

Framework domain	**NO**	**PL**	**SK**	**UK**				**JP**	**SG**							
1 SBS	●	○		●				●								
2 TNC			○	●				●	●							
3 ITPI	○		○	●				●	●							
4 RCC	●			●				●	●							

5. Conclusion

A quick examination of evaluation of individual NCSS shows that cybersecurity strategies more or less fit into the proposed framework thus confirming its applicability. However, few countries seem to be quite off of it. Particularly, Lithuania (no domain covered), Poland (one domain partially/superficially covered, three domains not covered), Slovakia and Cyprus (two domains partially/superficially covered, two domains not covered). **In other words, the cybersecurity-related thinking of these countries seem to be focused almost exclusively on the operational level while the political-strategic level is either omitted or only superficially touched**.

Focusing on individual domains of the proposed framework offers more conclusions. Our evaluation indicates that **the needed coordination at the political-strategic level is rarely explicitly called for** (six/five times out of 23/(21 European) NCSS examined). Moreover, even if this aspect is taken into account, the problem of ensuring reliable data for respective decision making – as pointed out by the CEPIS Statement "Supporting High-level decision Making on Cyber

Security and Privacy protection with reliable Data"[8] – is disregarded; at least no evidence for coverage is visible, the only exception seems to be Croatian NCSS with its explicit call for collection and analysis of data and reporting trends about security incidents.

On the other hand, some form of international cybersecurity cooperation is envisaged in almost all examined NCSS. The level of involvement varies, though, as some NCSS explicitly call for active role of the respective country while the others just settle for participation within the framework of existing international organizations.

Besides the lack of inclusion of political-strategic level for most NCSS, we feel it necessary to remind that a **considerable portion (38 %) of the analyzed 21 European NCSS fail to represent a holistic approach to cybersecurity on the national level, i.e. they cover less than 3 of the 4 areas.**

With regard to uncovered areas it is worthwhile to note, that measures for reduction of cybercrime, as well as development of industrial and technological resources for the cybersecurity ecosystem are not mentioned at all by 11 countries' NCSS (Cyprus, Hungary, Italy, Lithuania, Poland, Slovakia for cybercrime reduction and Denmark, Ireland, Iceland, Lithuania, Luxembourg, Latvia, Poland for industrial and technological resources).

An important and delicate aspect, that does not seem to be covered sufficiently in the strategy documents, is an assessment of the required qualities of the entities dealing with cybersecurity, both on a strategic and operational level.

The status of these entities does not seem to be discussed and/or reflected explicitly. At least no document is pointing the need for independence or even ways to implement such an independence. Practically the entities dealing with cybersecurity are dependent on state institutions, e.g. ministries. This is problematic as state institutions are stakeholders themselves with regard to cybersecurity.

So far, mainly two examples exist, where the tensions between the respective tasks and the state stakeholders have created difficulties for optimal solutions for cybersecurity challenges:

1. Collecting information on (potential) weaknesses in ICT systems and especially critical infrastructures: Often state institutions are involved with the enforcement of penalization against operators of (critical infrastructure) ICT systems, e.g. for the neglect of security measures. Obviously, operators of such infrastructures are not keen to report any information beyond what they are clearly obliged to, as they always expose themselves to potential penalization.
2. Responsible collection, administration and publication of ICT security weaknesses: State institutions are not neutral but stakeholders with regard to the collection, administration and publication of ICT security weaknesses. As e.g. the WannaCry event showed, often state institutions are collecting or even harnessing or buying ICT security weaknesses to exploit them for e.g. intelligence purposes (and the access to other parties' ICT systems). So, the respective information is not (always) transferred in the fasted possible way to those, who are to repair the weaknesses and those who can suffer damages from the weaknesses (e.g. from break-ins). The responsible collection, administration and publication of ICT security weaknesses is a very delicate matter and requires a set of impartial institutions, that are not impaired by any interests of institutions close to them.

[8] CEPIS Statement on Supporting High-level decision Making on Cyber Security and Privacy protection with reliable Data, 2014 https://www.cepis.org/index.jsp?p=942&n=963&a=5231