CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Torsten Corall, Katriina Härma, Ann Väljataga

Enhancing international collaboration in cyber defence through national cyber security strategy development

Tallinn 2018

www.ccdcoe.org

publications@ccdcoe.org

Prepared by Torsten Corall, Katriina Härma and Ann Väljataga

1. Contents

2. Abbreviations

C(I)I	Critical (information) infrastructure
C(I)IP	Critical (information) infrastructure protection
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
ECI	European Critical Infrastructure
ENISA	European Union Agency for Network and Information Security
EPCIP	European Program for Critical Infrastructure Protection
EU	European Union
ICT	information and communication technology
ISO	International Organisation for Standardisatiojn
ITU	International Telecommunications Union
MOD	Ministry of Defence
MOFA	Ministry of Foreign Affairs
MOI	Ministry of Interior
NCSS	National Cyber Security Strategy
UN GGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

2.1 Introduction. Cyber security as a public good and shared burden in the Allies' National Cyber Security Strategies

In July 2016 at the Warsaw Summit, NATO declared cyberspace to be the fourth operational domain. Although the possibility of cyberwar and the national and international obligations arising from it had been heatedly debated for almost three decades, the event marked a milestone in the legal and political conceptualisation of cyberspace. In addition to the foregoing, the international community has long recognised that international law applies to cyber operations. These two developments give a new, more clearly outlined and formulated meaning to collective cyber defence. This raises questions as to how to promote international collaboration and what would be the role of states, governments, the ICT industry, civil society and international organisations in doing so. In many facets, the cyber domain is challenging and expanding the traditional views on collective defence and international collaboration.

Firstly, although state practice speaks strongly for recognising sovereignty in cyberspace, the actual control that states exercise over the activities in this domain is considerably weaker than in other domains and the role of non-state actors is unprecedentedly strong. Secondly, the very underpinnings of cyberspace dictate an interconnectivity and shared vulnerability not paralleled in any of the other domains. To address the urgency and particularities of cyber defence, NATO adopted its Cyber Defence Policy in 2011, meanwhile between 2003 and 2017, around 80 states around the world have adopted a national cyber security strategy (NCSS). This includes all NATO Allies. The following study looks into the NCSS-s of NATO Allies that have been published as of January 2018 and are available in English.

NATO Country	Year of publication
Canada	2010
Croatia	2015
Czech Republic	2015
Denmark	2014
Estonia	2014
France	2015
Germany	2011
Greece	2017
Hungary	2013
Iceland	2015
Italy	2013
Latvia	2014
Lithuania	2011
Montenegro	2013
The Netherlands	2013

Norway	2012
Poland	2013
Portugal	2015
Slovakia	2015
Slovenia	2016
Spain	2013
Turkey	2013
UK	2017
USA	2011

Just as with national security strategies in general, NCSS are characterised by diversity shaped by digital capacity, network dependency, socio-economic factors and domineering political platforms. This diversity per se is not however a destabilising factor or threat, nor are any collective efforts which aim to eliminate the divergence realistic or feasible. The necessity of international cooperation seems to be one of the aspects that all states deem worthy of emphasising in their strategies. Virtually no NCSS document ignores the international dimension. However, some strategic elements lay the grounds for valuable cooperation while others might turn out to be hindrances in the longer perspective. Therefore, while uniformity is not likely to be considered a reasonable aim to pursue, diverse points of view can be valuable from the defence perspective, as long as they are complimentary.

Although versatile in their ICT penetration, dependency and literacy, each and every member state has introduced a NCSS, and furthermore allies who are also members of the EU are obliged to do so by the Directive on security of network and information systems[1]. Additionally, the critical relevance of cyber defence is further highlighted in many national security strategies hence, ideally, a NCSS should be conceptually linked to, and coherent with other strategic documents.[2] This, however, should not be the only point of connection. Purely inward-looking strategies are rare, both globally and among the allies; the latter, however, does not automatically imply that all national cyber security strategies understand and interpret the role and function of international collaboration in a uniform manner. Therefore, even in a climate where international collaboration is a generally recognised value, it is possible to perceive differences as to whether or not the declaration is followed by a set of concrete lines and points of action or left at a merely programmatic stage.

Although international collaboration and collective defence can be perceived from a variety of viewpoints, some lines of action / activities that send a strong signal of openness and willingness to cooperate internationally include:

- Participation in the work of international organisations in addition to NATO, as well as EU, OECD, ITU etc.;
- Joint exercises;

[1] 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, OJ L 194, 19.7.2016, p. 1–30.

- Full compliance with international standards (ICo, PMM, ISO);
- Development of MLATs and memoranda of understanding;
- Full compliance with international law, both the general instruments of PIL and cyber-specific legislation (Budapest Convention, EU instruments - NIS, E-Privacy etc); and
- Willingness to comply with international standards.

The spectrum along which the collaborative tools are located covers technical, political and legal spheres to an equal extent, but sometimes mere intergovernmental collaboration is not sufficient, and the collaborative bonds should reach across the lines between public and private entities. Similarly, often the lines between the military and civilian spheres are to be obfuscated. Therefore, while declaring international collaboration as one of the key aims and guiding principles, a strategy that at the same time allows for a fragmented or strictly state-centric approach renders any actual collaboration unfeasible. An example of the latter tendency would be the approach taken by France in its first NCSS (published in 2011) in which it states its ambition to become a world power in cyber security and to maintain information superiority in the national part of cyberspace.[3] France's second generation NCSS is however much more cooperative-minded.[4]

As a general tendency, the strategies adopted during the last two years are more clear-cut when it comes to the particular activities and metrics. The current fragmented landscape is hence almost unequivocally recognising the relevance of international collaboration, while sometimes still shifting the focus disproportionately onto domestic cyber issues that are viewed as being divorced from broader global trends. Another trend that might prove counter-productive in the longer run is taking an excessively government-focused approach and overlooking the essential role of the private sector, civil society and end-users. Therefore, any strategy that aims to count for an efficient Whole-of-System[5] collaboration should at first ensure the affluence of the strategy on Whole-of-Government[6] and Whole-of-Nation [7] level. This paper looks at the national cyber security strategies of NATO allies published as of January 2018 while giving an overview of current approaches in the following frameworks:

1. Law and norm creation
2. Combating cyber crime;
3. Harmonised standards for information security;
4. Critical information infrastructure protection as a cooperative aim;
5. International collaboration within the private sector
6. Preventive military cooperation

[3] France 2011, p.16. (note: hereinafter all references to states signify their most recent NCSS)

[4] See, e.g. Prime Minister´s foreword to the NCSS, France 2015, p.1.

[5] Also known as networked government, an approach where different government departments act jointly in planning, implementation and evaluation national strategies, action plans and public services (Klimburg, Alexander,ed., National cyber security framework manual, NATO CCD COE, 2012.)

[6] A governance model that, in addition to government departments, includes non-state actors such as NGOs and industry on an international level (Klimburg, 2012, 95).

[7] A governance model that includes like-minded non-governmental actors such as civil society and industry on a national level (Klimburg, 2012, 96).

7. CERT cooperation

While exploring the latter aspects, the authors pay particular attention to whether the strategy has declared international collaboration as a guiding principle/key objective, and if so whether the declaration is followed by definite action points

As a result of mapping 19 NCSS in 2013. Luijif *et al.* pointed out that international collaboration is listed among the key action lines of the majority of the reviewed strategies either explicitly ('active international engagement', 'closely cooperate with international organisations and other means', or as a part of wider cooperative aspect ('responsible interdependence' (ESP), 'working in partnership' (UK), 'transfer of information, expertise and good practices to protect the cyber infrastructure')).[8] However, only four strategies directly addressed stakeholders on the global infrastructure level.[9]

As a general rule, the NCSS of a NATO member state starts with highlighting the importance of the cyber domain from the perspective of national security, global and national economic prosperity, development, and fundamental rights and freedoms. The vast majority of the studied strategies acknowledge the importance of critical information infrastructure protection and combating cybercrime, while in the other aspects the priorities and focal points differ. However, in its most basic form, a strategy limits itself to the first two elements, and currently less than half NCSS-s are accompanied by a specific and publicly available action plan. Also, the strategies vary to a wide extent in the level of abstraction, which is why comparable data is not always available. However, the political, legal and societal consensus seems to be that cyber security, if it is to be of any relevance and efficacy, cannot be viewed as isolated national issues but does rely on international multi-stakeholder collaboration.

This view was also expressed in NATO CCD COE's National Cyber Security Framework Manual, where different models of stakeholder engagement are applied to national cyber security strategies. Pursuant to commonly accepted public policy theory, policies can be delivered either via Whole of Government (WoG), Whole of System (WoS) or Whole of Nation (WoN) approach. While the cyber domain poses multiple specific challenges, the general objective is common to all 21st century security efforts – to inspire a wide range of different actors to work together on an even wider range of security-related themes.

In its essence, every effort to promote collective cyber security is a Whole of System project, with states acting primarily as goal-setters and regulators, but nevertheless depending on the more specific actions of the private sector, end-users, researchers and international actors responsible for standard creation and internet governance to name a few. However, any such effort is unlikely to succeed without a strong foundation at both WoG and WoN levels. An example of a successful implementation of the WoG approach would be a transparent and clear national cyber security management structure that is characterised by unambiguous and practical subordination schemes, roles and responsibilities. Moreover, collective cyber defence is built upon WoN elements such as public-private partnerships (especially in the context of CIIP) and the education and training of

[8] Luiijf, Eric, Kim Besseling, and De Graaf, Patrick, „Nineteen national cyber security strategies," *International Journal of Critical Infrastructures* 6-9, no. 1-2 (2013): 3-31. This paper analyses and compares 19 NCSS of 18 nations: Australia (AUS), Canada (CAN),Czech Republic (CZE), Estonia (EST), France (FRA), Germany (DEU), India (IND), Japan (JPN), Lithuania (LTU), and Luxembourg (LUX). Romania (ROU), The Netherlands (NLD), New Zealand (NZL), South Africa (ZAF), Spain (ESP), Uganda (UGA), the United Kingdom (GBR; 2009 and 2011 versions), and the United States (USA), of which three (CZE, IND, ROU) were drafts at the time of publication.

[9] Ibid, 19.

cyber security specialists. Therefore, while exploring an issue that is best dealt with through the WoS approach, the present study also aims to assess whether or not the studied national strategies have laid down the necessary technical, legal, political, military and industrial grounds for international collaboration between the allies.

The vast majority of NATO allies do mention international collaboration among the strategic objectives or guiding principles of NCSS, and it is one of the most common lines of action presented in the strategy. The extent of detail on how to take action toward promoting collaboration is again varied, ranging from a simple declaration[10] to an elaborate list of steps to be taken.[11] The following table illustrates how the NCSSs of NATO allies address the importance of international cooperation:

[10] e.g. Hungary.

[11] e.g. UK.

Table 1. **International cooperation in NCSS-s**

NATO Country	Strategic objectives	Guiding principles	Tactical lines of action
Canada	X	X	
Croatia		X	
Czech Republic	X	X	X
Denmark			
Estonia	X	X	
France		X	
Germany	X	X	
Greece	X	X	
Hungary	X	X	X
Iceland	(x)		
Italy	X	X	X
Latvia	(x)	X	X
Lithuania	(x)	X	X
Luxembourg	X	(x)	X
Montenegro	X		
The Netherlands	X	X	X
Norway	X	X	
Poland	X	X	X
Portugal	X	X	X
Slovakia	X	X	X
Slovenia	X		
Spain	X	X	X
Turkey			
UK	X	X	X
USA	X	X	X

X- addressed (x) – implicitly addressed

3. Law and norm creation

3.1 International cooperation

Cyber security requires the cooperation of many stakeholders both nationally and internationally. Because of the very fundamental crossborder nature of cyber related threats, international cooperation cannot be completely forgotten. National cyber security strategy gives guidance for future developments in legislation, policies and other recommendations. International cyber norms and laws emerge under the auspices of various international organisations, which conjoin experts in order to bring clarity to existing state practice and *opinio juris* and make proposals for future norms; therefore it is important to also map all relevant collaboration possibilities.

As mentioned, the nature and substance of international cyber security cooperation has not usually been described in great detail in NCSSs, nor do they include specific action plans in this regard. The most common way to address this question is to describe cooperation as *engagement in discussions* in international organisations or just *active participation* in different forums. Participation in international cooperation can lead to new commitments for states that can be either binding or voluntary. These commitments can be either political or legal in nature, or can have elements of both aspects.[12]

A common way to address this international aspect in NCSSs is to list the organisations or other actors that the nation cooperates with. International cooperation can be in general be conducted in different levels and forums; between states regionally or bilaterally, pursued in the context of the European Union or by participating in the work of international organisations such as NATO, the OSCE, and the UN.

EU and NATO are the organisations that are mentioned in most in national cyber security strategies and they seem to have most importance in the field of cyber security.

The EU implemented its own cyber security strategy in 2013. The strategy includes a vision for cybersecurity, clarifies roles and sets out the action plan to make the EU's cyberspace the safest worldwide. In its work, the EU has implemented guidelines and directives e.g. on cyber crime prevention, protection of critical IT infrastructure, data security and data protection.

The work of the Organisation for Security and Co-operation in Europe (OSCE) aims to develop confidence-building measures (CBMs) for the prevention of cyber conflicts. The goal of this cooperation is to complement the efforts of other international organisations. Decisions are taken by consensus and are by nature politically, but not legally, binding.

ITU is the United Nations' specialised agency for information and communication technologies. It has implemented the Global Cybersecurity Agenda (CGA) for a framework that promotes the international cooperation in the field of cyber security culture. ITU has also drafted a national cyber security strategy that can be used as a reference model when creating national cyber security strategies.

The Organisation for Economic Co-operation and Development (OECD) is an expert organisation that supports its member states' decision-making in economic and social policy. The organisation aims to develop or harmonise

[12] Klimburg, 2012, 149.

the policies of its member states in various sectors of the economy or society. The OECD completed a comparative study related to ten member states' national cyber security strategies in 2012.[13]

Apart from listing appropriate organisations or participants, one way to describe the cooperation options is to emphasise the field or specific area of interest the cooperation is expected to happen: e.g. foreign and security politics or discussions.

The purpose of cooperation is often explained as a need for *information sharing*, *knowledge exchange* or *benchmarking* the best *practices*. Some states see that information sharing and cooperating with less developed nations is also a way to enhance their own security, because it helps to secure the possible loopholes and hinder the adversaries that use the weak links in global networks. The building of weaker states' cyber abilities will protect nations' own interests as well.[14] In that sense the cooperation can be seen as improving global security.

One part of collaborating is to prepare for crisis situations. When advance planning is done together, it is much easier to respond in crisis situations.[15] Skills and contacts are important, and these can be improved; e.g. through joint exercises.

Some states do not stick to seeking partners only from governmental levels, but expresses willingness to work with private parties internationally as well.[16] The methods or means are not described in detail, but usually by listing possible partners (non-governmental institutions, public and private parties, universities, industry). States also tend to give emphasis to certain values of possible partners. This is one way to enable future bilateral cooperation with partners that are not necessary named or specifically pointed out in the strategy. This effort can be expressed using phrases as 'like-minded' or 'similar minded' countries, or as 'nations sharing identical values'. Hungary, for example, 'strives to establish and maintain cooperation based on mutual trust with all public and non-public actors of the global cyberspace representing similar values'.

3.2 International legal framework

To date, there is no uniform international law instrument that deals with all cyber related matters. The need for one has been repeatedly raised by SCO and contested by the majority of Western states on the grounds that existing international law applies in cyberspace just as it does in other domains. The UN Charter regulates use of force in state relations. Use of force is forbidden except when justified by self-defence in the event of an armed attack or when certain military action is mandated by the Security Council.[17] The legal debates concerning cyber incidents at the moment include whether and in what circumstances cyber attacks can rise above the level of an armed attack threshold defined in UN Charter, and thus justify a military response by the state that was the

[13] The Organisation for Economic Co-operation and Development, Cybersecurity "Policy-Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy," 2012 http://oe.cd/cybersecuritystrategies, last accessed May 14, 2018.

[14] UK, Canada, France.

[15] Iceland.

[16] The Netherlands, Poland.

[17] United Nations, Charter of the United Nations, art 2(4) and 51.

victim.[18] Other legal discussions[19] in this field include sovereignty and *due diligence*. States are obliged to a certain extent to ensure that their territories are not used by third parties to cause serious harm to other states.[20]

The interpretations concerning international law may lead to new assessment of cyber incidents in the work of international organisations. But the states as subjects of international law give the real substance to the norms when (or if) implementing them in state practise.

United Nations Group of governmental experts (UN GGE) is a UN mandated working group in the field of information security. In 2013 it published a report which found that international law, and in particular the Charter of the United Nations, is applicable in cyberspace. The report also confirmed the appropriateness of the law of sovereignty and of state responsibility in the context of cyber security.

NCSSs will have to reflect a nation's contemporary position on international law discussions, while remaining flexible enough to evolve as understanding continues to grow.[21]

Some states explicitly restate the UN-recognised applicability of international law in cyberspace or that human rights apply online as they do offline.[22]

This example, taken from the Croatian NCSS, is perhaps the most comprehensive way to describe the legal framework while regarding all the important aspects of norm hierarchy in one sentence:

> 'National interest and all the necessary activities will be pursued according to the principles, values and obligations based on the Croatian Constitution, the Charter of the United Nations, international law, international humanitarian law and the relevant legal and strategic frameworks of Croatia and the EU, as well as other international obligations arising from the membership in the United Nations, NATO, Council of Europe, Organisation for Security and Cooperation in Europe and other multilateral platforms and initiatives'.

Cyber-related matters can often be approached in a fragmented manner and scattered throughout legislation. Relevant articles can be found concerning privacy and personal data processing law, telecommunications law, cyber crime and criminal procedural law. Strategies in the national legal framework are seldom described in detail. That gives some space to create new legislation that will take into account future technical developments.

When there is completely new or very recently drafted cyber legislation, it is usually mentioned in the strategy. That serves the informational purposes of a strategy. States inform their own citizens and also other governments of their future developments through strategies. For example, Slovakia describes in its NCSS the solution for cyber issues and the creation and adoption of a legal framework for cyber security, which includes also adoption of the Cyber Security Act.[23]

[18] See for example: Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press, 2017, Rule 71, 339, (Short title) Tallinn Manual 2.0.

[19] UN General Assembly. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.", *A/68/98* 24, 2013, paras 20, 27, 28; Tallinn Manual 2.0 Rule 1, 11.

[20] See for example: Tallinn Manual 2.0, Rule 6, 30.

[21] Klimburg, 2012, 152.

[22] Estonia, France, UK.

[23] Slovakia.

The interpretation and discussions relating to international law will most probably result in the need to harmonise the legal doctrines of individual states. It is not enough to only assess existing domestic legislation. It must also be compatible with international legal and technical developments. The cyber security legislation is seen as a continuous process that needs regular updating and harmonising national legal norm with international obligations.[24]

What comes to technical developments legislation must also keep up with the current global cyber security trends. That applies also to strategies. National legislation must not include any loopholes that might attract criminals and it must also be able to create a good environment for private enterprise.[25]

An international approach is usually adopted concerning cyber crime. The 2001 Convention on Cybercrime of the Council of Europe (the Budapest Convention) lays the groundwork for the prevention of all cyber crime.[26] This also requires harmonisation in national legislation.

Among the EU member states the EU level legal and regulatory provisions require harmonisation. The EU's focus has been recently on cyber crime prevention, protection of critical IT infrastructure as well as legislative work on electronic communications, data security and data protection.

3.2.1 Human rights[27]

Although international cooperation and the openness of networks are considered important in national strategies, many countries stress the importance of human rights in the digital environment. There can be a general statement that individual rights are applicable both online and offline.[28]In regard to basic rights and human rights, the rights to privacy and confidentiality of communications have been seen essential in cyber context.[29]

Networks can promote freedom of expression and opinion. Well executed cyber security can also guarantee the protection of property of users in networks:

'Individual rights are applicable in the same way «on-line» and «off-line». Cyberspace should therefore remain a place of free expression for all citizens, where abuses can only be prevented within the limits set by the law and in line with our international agreements' (France).[30]

[24] Czech Republic.

[25] Iceland.

[26] See Chapter 3.

[27] Tallinn Manual 2.0, Rule 34, p.182.

[28] France, UK.

[29] Slovakia.

[30] The European Convention on Human Rights (ECHR) is a European initiative. All member states of the Council of Europe are parties to the Convention and it established the supranational European Court of Human Rights. The International Humanitarian Law (IHL) is applied during armed conflict. Its purpose is to limit the hardship and suffering of the civilian population by providing a minimum standard of protection. The protection is based on Geneva Conventions and its Additional Protocols, as well as the Hague Conventions. Significant portions of these treaties are also recognised as customary law. IHL contains rules for warfare such as the principles on proportionality, necessity, distinction and non-discrimination.

Table 2. **International cooperation in international law and norms creation**

	International cooperation[31]	International legal framework[32]	Harmonisation[33]	Fundamental rights, human rights
Canada	X	X (military aspects)		
Croatia	X	X	X	X
Czech Republic	X	X		X
Denmark	X			
Estonia	X	X		X
France	X	X		X
Germany	X	X		
Greece				
Hungary	X	X		X
Iceland	X	X	X	
Italy	X	X	X	X
Latvia	X	X	X	X
Lithuania	X			
Luxemburg	X		X	
Montenegro				
The Netherlands	X	X	X	X
Norway				
Poland	X		X	X
Portugal				
Romania				
Slovakia	X	X	X	X
Slovenia				
Spain	X	X	X	
Turkey	X		X	X
UK	X	X		X
USA	X	X		X

[31] This category in the table is meant to give examples of how NCCS relates to international collaboration or work that is conducted through international organisations.

[32] This category in the chart is meant to give examples in the NCSS attitude towards international law and other involvement with legislation.

[33] This category represents whether the strategy has addressed the need to harmonise domestic law with international obligations.

4. Combating cyber crime

Various incidents related to crime within the cyber domain have occurred over recent years,[34] and they have attracted public attention to crime affiliated with information and communication technology (ICT). States deal very differently with the topic of cyber crime and have, of course, certain measures to counter this type of crime. One aspect is domestic collaboration which spans from classic police and law enforcement institutions (e.g. customs and border guard authorities) to intelligence services. But the cyber aspect of crime is also a cross border and cross sector phenomenon with various implications. And, to this extend, the international collaboration is very important, because cyber crime incidents are almost borderless. The different strategies States have issued have also different approaches, however, the respective civilisations are all equally affected by cyber crime.

4.1 Cyber crime

Related to this, one has to bear in mind that there is no commonly accepted definition of cyber crime. States have their own view and domestic definition of this topic, but one common aspect is that the act itself involves a computer (in a way that it has some artificial calculating ability) and is connected to a network. The computer may have been used in the commission of a crime, or it may be the target. This definition represents a holistic approach and also encompasses devices connected to the internet as part of the so-called internet of things.[35] The term cyber crime covers a wide range of criminal activity and a wider range of skillsets of the perpetrators. So, in other words, cyber crime is a sophisticated attack against computer hardware and software. This can be distinguished from cyber-enabled crime, where many 'traditional' crimes have taken a new turn with the advent of the Internet, such as crimes against children, financial crimes and even terrorism. It is also worth mentioning that cyber crime is not only conducted by top level hackers or genius criminals. More often, the necessary skill set to commit cyber crime is available to anyone who is able to access the Internet. Hacking, in the meaning of illegal access, is much less complex than it was a few years ago, as the respective knowledge is widely available through all facets of the Internet and even an average user can use this knowledge. Another aspect is the business model of 'crime as a service' as well as target tailored software.

States recognise cyber-criminal threats as among the most challenging and emerging issues on their agendas. It is currently estimated that the annual cost of cyber crime in the world today is approximately $6 trillion.[36] Cyber crime is frequently both international in nature and technically and legally complex making it challenging for states to effectively deal with it. As a matter of international law enforcement, it is often difficult to effectively cooperate and collaborate with other states in terms of time, resources and interests. Additionally, there is not only a need for a growing number of specialists to investigate and trace cyber criminals using the ever improving means and methods of the digital age and cyberspace, but also there is an urgent requirement to revise and supplement existing international and domestic legal regimes because existing laws are often not tailored to deal

[34] Notable recent example include attacks conducted by applying 'Wannacry', 'Locky' and 'NotPetya' ransomware. For further reading see e.g.: Iain Thomson, "Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide", The Register, June 28, 2017, https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/; "Wannacry: Everything you still need to know because there were so many unanswered Qs", May 20, 2017, https://www.theregister.co.uk/2017/05/20/wannacry_windows_xp/ ; Unbreakable Locky ransomware is on the march again, https://www.theregister.co.uk/2017/01/20/locky_ransomware_horrorshow_returns/

[35] See https://ec.europa.eu/home-affairs/what-we-do/policies/organised-crime-and-human-trafficking/cyber crime_en .

[36] Cyber Security Ventures, Annual Report 2016, October 16, 2017, https://cybersecurityventures.com/hackerpocalypse-cyber crime-report-2016/ .

with the complexities of today’s cyber crime. However, complexity in style and forms of cyber crime increases the difficulty of fighting back. In this sense, fighting cyber crime calls for international cooperation and agreements.

To clarify, it helps to consider computer crime provisions, which exist on three different levels: international, regional and domestic regulations, all of them in a multilateral and bilateral approach. Various organisations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and an international scale. One of those international organisations is the Council of Europe, which established an internationally recognised binding norm framework: the Convention on Cyber Crime of the Council of Europe, which is as commonly known as the Budapest Convention. Initially established in 2001 in Budapest, the Convention came into force in 2004. There are currently 56 ratifications by states around the world. The Convention is a framework treaty and guideline for nations on this special field of crime which, of course, needs to be implemented through domestic legislation. The Convention is the first international treaty on crimes committed via the Internet and other computer networks. It addresses such areas as the infringement of copyright, computer-related fraud, child pornography and violations of network and information security. It also contains a series of powers and procedures such as the searching of computer networks and interception. The Convention has also an additional protocol dealing with racist and xenophobic related offences committed through computer systems.

The Convention’s main objective, according to the preamble, is to pursue a common international criminal policy aimed at the protection of society against cyber crime, especially by adopting appropriate legislation and fostering cross-border co-operation. To foster the multinational cooperation, it is mandatory for signing states to establish a 24/7 hotline and appointed points of contact. The Convention also requires that the procedural domestic laws of the signatory states concerning proof of evidence, saving of data and chain of custody must be harmonised.

There is also a great taxonomy of cyber crime related actions which do not compellingly do fulfil the criteria of crime such as target fingerprinting,[37] modification of data, intrusion attempt and spam. But there are actions which are recognised as crimes such as unauthorised access to transmissions, denial of service, malicious code and account compromise[38].

Within the Convention[39] there are clearly formulated offences against confidentiality, integrity and the availability of computer systems which attempts to achieve and uphold the classic aims of information security. Also, the access, interception and interference, both with data and systems without permission is assessed as an offence under the Convention. The misuse of devices and the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed […] primarily for the purpose of committing of the abovementioned crimes is also a criminal offence.

Also, computer-related forgery, fraud, child pornography and copyright infringement are regulated. With these regulations most of the today’s known acts of cyber crime can be prosecuted by law enforcement authorities.

[37] Actions performed in order to gather information about a target by directly communicating with the target. Instructive: https://www.cybersecurity-review.com/websites-can-now-track-you-online-across-multiple-web-browsers/

[38] Council of Europe Convention on Cyber Crime, ETS No.185, Articles 1-6.

[39] Council of Europe Convention on Cyber Crime, ETS No.185, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, last accessed May 14, 2018.

Another aspect of cyber crime is cyber terrorism. This is generally understood to be intimidation or coercion of a government or an organisation or even an individual to advance their political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them. Cyber terrorism, in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources.[40] As such, a simple propaganda piece on the Internet that there will be bomb attacks during the holidays can be considered cyber terrorism. There are also hacking activities directed and orchestrated towards individuals and organisations conducted by groups within networks, intended to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

In the European Union (EU), on a regional level, the main regulation is the Botnet Directive.[41] It was implemented EU-wide in September 2015. The aim of this directive is to criminalise cyber attacks against information systems. In addition to the content of the Budapest Convention, the Botnet Directive names certain penalties of up to 2 years in prison for committing certain offences. Due to the legal character of the EU directive, it was easier to have a common understanding on penalties and of course for procurement reasons EU member states are not bound to adopt this directive in a particular manner, but can choose how to adopt it. Another aim was to improve cooperation between states' competent authorities within the European Union. The directive also recognises the protection of critical infrastructure and specifies certain penalties, by contrast with the Budapest Convention.

States do not always address the topic 'cyber crime' *expressis verbis* within their respective cyber strategies. All of the respective states cope with those challenges arising from the issue.

As shown below, all NATO member states have a cyber strategy and all of them are signatories to the Budapest Convention. However, almost all of the 29 member states address cyber crime in their strategies. The above mentioned states that address cyber crime focus on the Budapest Convention, information sharing and exchange and on capacity building:

Table 3. **Budapest convention aspects in NCSS-s**

NATO Country	Signatory and ratification to Budapest Convention	Combatting cybercrime aspects within strategy
Albania	X	Not in English
Belgium	X	Not in English
Bulgaria	X	Not in English
Canada	X	X
Croatia	X	X
Czech Republic	X	X
Denmark	X	X
Estonia	X	X
France	X	X
Germany	X	X
Greece	X	X
Hungary	X	X

[40] Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA).

[41] EU Directive 2013/40/EU on attacks against information systems.

Iceland	X	X
Italy	X	X
Latvia	X	X
Lithuania	X	
Luxembourg	X	X
Montenegro	X	X
The Netherlands	X	X
Norway	X	X
Poland	X	X
Portugal	X	X
Romania	X	Not in English
Slovakia	X	
Slovenia	X	X
Spain	X	X
Turkey	X	X
UK	X	X
USA	X	X

4.2 Budapest Convention aspects

The nation states cover aspects of countering cyber crime in different ways. One approach is referring to the Budapest Convention. The topics related to the Convention that have received the widest coverage by states are enhancing the capacity of law enforcement and providing assistance to partners in fighting serious cyber crime.[42] Especially by increasing the assistance to partners, the pressure on criminal networking organisations is enhanced because from the perspective of the criminals the 'safe haven' is missing. Strengthening international legal frameworks, with emphasis on promoting and improving the implementation of the Budapest Convention and accompanying protocols is another important aspect due to the fact that harmonised legal frameworks leads in the end to filled legal gaps.[43] By reinforcing the operational mechanisms for legal mutual aid the fight against cyber crime is also more efficient and effective because time sensitive issues, evidence handling and extradition are handled in a faster manner.[44] This aspect is also mentioned in connection with fostering close cooperation between law enforcement authorities worldwide and achieving global harmony in criminal law based upon the Budapest Convention.[45] Lastly, encouraging other nations to accede to the Council of Europe Convention on Cybercrime, or to ensure that their laws and procedures are at least as comprehensive, is also mentioned.[46]

[42] Canada.

[43] Croatia.

[44] France.

[45] Germany.

[46] USA.

As seen, all of these principles have a strong international element, and even strategies that are otherwise inward-looking acknowledge the importance of international cooperation when it comes to combating cyber offenses. It is worth mentioning that the Budapest Convention is only one part of the overall norm and legislation creation approach nations undertake (see chapter 2 for a more detailed discussion on how international law and cyber norms).

4.3 Information sharing and exchange

From a more practical point of view, no legal instrument targeting international cyber crime could be enforced to its full potential unless information on criminal incidents and operations, suspects, malicious traffic, malware and crime statistics can be efficiently exchanged between cross-border actors. That is why some states recognise within their strategy that supporting international cooperation in terms of information sharing in the field of cyber crime within the EU, NATO member states and third countries is an important aspect.[47] The improvement of information exchange between states to achieve more effective and timely prosecution of cyber crime with an international dimension is also one goal of the Budapest Convention, but beside this, improvements and active participation in various initiatives and projects to exchange best practises are also part of the international fight against cyber crime.[48]

Another approach beside this is to use the available possibilities of the existing cooperation models through contact points and the possibilities of swift information sharing through the channels of Europol, Eurojust, Interpol and other international organisations in this sector.[49]

4.4 Capacity Building

States can only effectively address the threat cyber crime poses to their societies and economies if they have the capacity to cope with this issue. One aspect is, as mentioned above, to eliminate ‘safe harbours’ and to raise the costs and risks as well as reduce the rewards for cyber criminals by focusing on pursuing the criminals who persist in attacking citizens and businesses. Due to the international nature of cyber crime, working together with domestic and international partners to target criminals wherever they are located and to dismantle their infrastructure and facilitation networks is key to success. Law enforcement is tasked to raise awareness and standards for cyber security in collaboration with domestic cyber security agencies. To this end, it is important to address the perceived impunity and build international partnerships and enhance collaborations with industry. Also, it is vital to develop and establish a 24/7 reporting and triage capability in so-called Action Fraud.[50]

4.5 Recommendations

Although from the perspective of fighting cyber crime international collaboration is relatively well-covered, there are ways in which states could after the basics have been laid down, go deeper and more specific.

[47] Croatia.

[48] Estonia, Spain.

[49] Croatia.

[50] UK.

4.6 Harmonisation

The first big step was undertaken by implementing the Budapest Convention. This document is a very comprehensive tool to fill out all legal gaps around the world. If more and more states adopt and implement this convention, this will be a crucial step forward in the fight against cyber crime.

4.6.1 Internationalise, internationalise, internationalise

International cooperation in regard of cyber crime is not mentioned within each and every reviewed strategy. In some cases, this can lead to the impression that a state does not foresee international cooperation against cyber crime at all. This cooperation can also be fostered if, as some strategies mention, existing law enforcement networks are used and exploited. In particular, international information exchange and sharing of evidence between respective agencies should be harmonised and institutionalised. The use of synergy effects of international cooperation in fighting cyber crime can be in a way, that certain standards of incident handling (e.g. standard operating procedure) are shaped and outlined. Also, the creation of a common knowledge database is established.

4.6.2 Raise the cost, increase the pressure

By fostering the implementation of the Budapest Convention to a wider audience among nation states, safe harbours and bases for criminals are closed down. Criminals face a greater chance of being brought to justice and take the risk of prosecution into consideration if legal regulations are harmonised (see above) and the guideline-providing Budapest Convention is in place. The cooperation between law enforcement authorities is also enhanced by using the principles of the Budapest Convention.

5. Harmonised standards for information security

5.1 Harmonised standards for information security

To one degree or another, states address information security within their cyber security strategies. Most advanced modern-day societies rely upon information technology, especially with respect to critical (information) infrastructure.[51] Accordingly, there is an urgent need to have such systems protected and operational under all circumstances. Beyond critical infrastructure, there are other computer systems (such as private individual computers and general business systems) which need protection as well. Cyber-related economic disruption may have a negative effect on the overall economy of a state and cause cross-border and cross-sector implications. A comprehensive risk assessment will necessarily lead to better preparation with respect to which assets and parts of network need to be protected from cyber attacks. There are different approaches to risk assessment such as multi-national, national and sectorial. One has to bear in mind that information itself (e.g. Big Data) is one of the most valuable assets and commodities in an advanced society. Therefore, it is important to know what exactly is meant by *information security*, particularly with respect to cyber strategies. One internationally used definition of information security is: '[t]he protection against the threat of theft, deletion or alteration of stored or transmitted data within a cyber system'.[52]

A good information security environment minimises risks and, of course, leads to overall protection and prevention of dangers to critical infrastructure and related information. Some important assessment, analysing and auditing instruments and methods are internationally recognised.

The International Organisation for Standardisation (ISO) and the International Electro-technical Commission (IEC) form the specialised system for worldwide standardisation in various fields.[53] All in all, 119 full members from all around the world take part through their respective national bodies in the development of international standards through technical committees established by the respective organisations to deal with particular fields of technical activity. There are also correspondent members, which observe the development of ISO standards and strategies by attending ISO technical and policy meetings as observers. Correspondent members are free to adopt ISO International Standards nationally, but cannot take part in decision making processes. International Organisation for Standardisation and IEC technical committees collaborate in fields of mutual interest. International Standards for management systems provide a model to follow in setting up and operating management systems. This model incorporates the features on which experts in the field have reached a consensus as being the international state-of-the-art. There is also an expert committee dedicated to the development of international management systems standards for information security, otherwise known as the Information Security Management System (ISMS) family of standards. Through the use of the ISMS family of standards, organisations can develop and implement a framework for managing the security of their information assets including financial information, intellectual property and employee details, or information entrusted to them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information. The ISMS family of standards is intended to assist organisations of all types and sizes to implement and operate an ISMS, and consists of several standard frameworks covering various fields.

[51] See definition in Chapter 6.

[52] ENISA, "Definition of Cybersecurity V 1.0", December 2015, 11.

[53] Homepage of International Organization for Standardization, last accessed May 14, 2018, https://www.iso.org.

In practise, those standards are recognised in conducting an overall comprehensive assessment and actions to be undertaken to achieve a secure information environment. Beside this, one means of conducting a risk assessment is to clarify what aims are to be achieved. There are three general protection aims that information security tries to achieve: confidentiality, integrity and availability.

- Confidentiality means that stored and saved data and information are only to be read and modified by authorised personnel. This also applies during the transmission process.
- To provide integrity of data and information, they are not meant to be altered unnoticed and every change must be logged.
- To avoid down time, availability of data is essential, and data has to be accessible to the right recipient in a proper time.

Beside this, there are also more protection aims like the authenticity, accountability, anonymity and non-repudiation of information:

- Authenticity describes the verifiability and trustworthiness of certain information.
- Accountability of information is to clearly assign a particular action to a specific communication process.
- In some cases, information and the fact of providing information has to be anonymous.
- With the help of electronic signatures, it is easier to attribute certain actions to particular actors.

For instance, the International standard ISO/IEC 27001 of the ISO 27k family specifies an Information Security Management System (ISMS) as an overarching management framework through which the organisation identifies, analyses and addresses its information risks, as well as its security. The ISMS ensures that the security arrangements, once decided, are up to date with the security threats arising not only from software and hardware issues, but also from all kind of origins.

The standard covers all types of organisations (e.g. commercial enterprises, government agencies and non-profits), all sizes (from micro-businesses to huge multinationals) and all industries or markets (e.g. retail, banking, defence, healthcare, education and government). This is clearly a very wide brief.

ISO/IEC 27001 does not formally mandate specific information security controls since the controls that are required vary markedly across the wide range of organisations adopting the standard. Recognising international standards (see above) within the respective strategies leads to better overall cooperation in terms of national and international cooperation because those standards are used as a common basis. It also produces an environment of compliance and can lead to fewer incidents of, for example, data breaches. The use of standards also helps the respective national authorities to get the whole picture and, in case of an incident, it helps mitigate the cross-border consequences because in the other affected country and involved side of the border, authorities handle the case the same way and use the same taxonomy. Furthermore, standardisation helps achieving the goal of international interoperability of systems (soft and hard).

Table 4. **Internationally harmonised standards in NCSS-s**

NATO Country	ISO treaty party	Standardisation aspects within strategy
Albania	Correspondent member	Not in English
Belgium	X	Not in English
Bulgaria	X	Not in English
Canada	X	X
Croatia	X	X
Czech Republic	X	X
Denmark	X	X
Estonia	X	X
France	X	Nothing on ISO and/or standards
Germany	X	X
Greece	X	Not found yet in English
Hungary	X	X
Iceland	X	X
Italy	X	X
Latvia	X	Nothing on ISO and/or standards
Lithuania	X	X
Luxembourg	X	X
Montenegro	Correspondent member	X
The Netherlands	X	X
Norway	X	X
Poland	X	Not on ISO
Portugal	X	
Romania	X	Not in English
Slovakia	X	X
Slovenia	X	X
Spain	X	X
Turkey	X	X
UK	X	X
USA	X	X

While some states mention ISO standards clearly as a reference, the majority do not. However, this does not mean that they do not recognise any standards on information security, but they may have only a national approach.

5.2 International context of ISO standards

ISO standard 27001 is clearly only recognised within one strategy[54] for direct technical coordination between the national regulatory authority for the area of electronic communications and national and international authorities responsible for the area of information security. It is a common among the strategies, that security and quality are identified to be connected with each other. Therefor the quality of IT and communication products and services necessary for the secure operation of the cyberspace should meet the requirements of international best practices, with special emphasis on compliance with international security certification standards. In determining cyber security requirements for public procurement in information technology and communications, Hungary intends to encourage equipment manufacturers and service providers to submit bids to create the highest possible level of cyber security, with special emphasis on compliance with international certification standards[55]. Establishing security standards and requirements for products and systems implementing security protocols is also mentioned. In this context, there is a furthermore a need for the introduction of processes to certify the compliance to security standards and, where appropriate, implementation of new procedures for the procurement of ICT products formulated on the national territory. These standards and procedures should always guarantee international interoperability.[56] Some strategies clearly state that full compliance with international requirements, security standards and protocols[57] and establishing a compliance management structure to fulfil the compliance with the requirements on information security and to ensure that information resources are managed in accordance with the requirements of international standards and examples of good practice are achievements to reach.[58]

Bearing in mind that cyberspace is an interconnected and open system by nature, another strategy emphasises that the strategic objective is to build an integrated, functional and efficient cyberspace, in accordance with international standards and principles.[59] Of course, what standards and principles are definitely referred to it is left blank, but to simply mention the intention is quite a good step forward. The promotion of benefits and advantages of standards for cyber security throughout the community of states is one objective mentioned.[60] A bit inward looking, but still in connection with international standards based on recognised security standards, is the aspect to have an increased use of international security standards in public administration, which then contributes to more comprehensive and systematic security efforts.[61] Another aspect mentioned is that standards evolve and are changed from time to time. One strategy refers to this and states that one objective is the active participation in the preparation of standards and norms as well as regularly evaluation and assessment of international law, including treaties and trends and standards in the field of cyber security.[62] Beside the abovementioned issues, it is also important to harmonise national law with international standards, therefore one strategy foresees the creation of a domestic legislation conforming to international standards, which also contains cyber security auditing standards.[63]

[54] Croatia.

[55] Hungary.

[56] Iceland.

[57] Italy.

[58] Lithuania.

[59] Montenegro.

[60] USA.

[61] Norway.

[62] Slovakia.

[63] Turkey.

5.3 Recommendations

5.3.1 Common basis

All strategies should cover the aspect of ISO because, as said above, implementing international recognised standards into all of the respective strategies will lead to a common basis and a uniform understanding. A compliance environment and well understood standard procedures can mitigate or even prevent breaches of information security. Also, the intention of nations is shown and documented to act according to a common approach to improve information security. Those best practises which are recognised and laid out within the ISO standards are not meant only for critical infrastructure, but can also have an additional value for every sector and every business. By using those standards, international cooperation is fostered and enhanced because the same taxonomy is used, and identical procedures are applied.

5.3.2 Save money

ISO standards implementation and documentation procedures cost money, but one has to bear in mind that this money will be saved on the other hand by fewer incidents or at least mitigated effects. Additionally, the ISO standard tool box is a well-structured risk mitigation tool and channel for the management aspect of information security, because information security and cyber security are not solely an issue of the ICT specialists, but of the management level of the respective authority or company. Applying those standards can lead to the end functionality and not documentation matters.

6. Critical information infrastructure protection as a cooperative objective

Critical infrastructure consists of assets that are essential for the functioning of the society or economy of a nation. Many such assets are dependent on an ICT system and many ICT systems themselves constitute critical infrastructure. For example, the EU Critical Infrastructure Directive defines critical information infrastructures as ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).[64]All the studied strategies do mention critical information infrastructure[65] protection (CIIP) among the top national cyber security priorities. This is, however, an area where even the most efficient whole of government or whole of nation style approach will not take us far. Stakeholder cooperation and international collaboration play a vital role in critical information infrastructure protection.

Firstly, data communications networks, fixed or mobile telephony and electronic banking are critical services that are to a large extent, if not entirely, outsourced to the private sector, which first and foremost is driven by economic profit. Secondly, due to economic or efficiency considerations the companies responsible for operating the aforementioned services do not limit their infrastructure to the territory of any given nation state; the services depend on a complicated cross-border network of physical infrastructure, software, human resources and services. A previous study carried out by the CCD COE in 2015 revealed that 8 out of 15 studied states explicitly mentioned ICT and communications among the services making up critical infrastructure, and ICT and finance are also the two sectors that the respondent states (Austria, Belgium, Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, the Netherlands, Spain and Turkey) describe as being the most critically influenced by cross-border dependencies.[66]

The aspect is only very sporadically covered in the national cyber security strategies studied in the current research. As a general rule, any effort to enhance, maintain or protect CII entails a strong collaborative element and is best handled by adopting a clear Whole-of-System approach. Sometimes the references to CIIP in strategies are excessively general, whereas often CIIP is viewed as a predominantly PPP issue and the international dimension is less recognised. Similarly, in 2015 Shackelford and Kastelic noted that while more than half of the 20 most technically and economically advanced among the studied nations [67] mentioned the importance of PPP in CIIP, only about one tenth highlighted the need for international partnerships.[68]

NATO Allies seem to value PPPs and cross-border cooperation to an equal degree, with a slight preference given to the former. The following table illustrates how different cooperation/collaboration models are addressed in the strategies of NATO Allies:

[64] Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection.Official Journal L, 345(23), 12.

[65] Critical Information Infrastructures (CII) are IT and ICT systems that operate key functions of the critical infrastructure of a nation.

[66] Kaska, Kadri, and Lorena Trinberg. ‘Regulating Cross-Border Dependencies of Critical Information Infrastructure’. NATO CCD COE, 2015. Sample: Austria, Belgium, Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, the Netherlands, Spain, and Turkey.

[67] Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Republic of Korea, Mexico, Russia, Saudi Arabia, South Africa, Turkey, the United Kingdom, the United States (EU not included in the sample).

[68] Shackelford, Scott J., and Andraz Kastelic. "Toward a State-Centric Cyber Peace: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity." *NYUJ Legis. & Pub. Pol'y* 18 (2015): 914.

Table 5. **Models of cooperation in CIIP**

NATO Country	Public-Private dependencies	Cross-border dependencies (international level)	Regional
Canada	X	X	North-America
Croatia	X		EU
Czech Republic	X	X	EU/Central-Europe
Denmark	X		(x)
Estonia	X		
France	X	X	X
Germany	X	X	EU
Greece	(x)		
Hungary	X		EU, Central/Eastern Europe
Iceland	X		
Italy	X	X	
Latvia	X	X	
Lithuania	X		
Luxembourg			
Montenegro			
The Netherlands	X	X	EU
Norway	X		
Poland	X	X	
Portugal	(x)	X	EU
Slovakia	X	X	
Slovenia	X	X	X
Spain	X	(x)	(x) EU
Turkey			
UK	X	X	X
USA	X	X	

The cross-border dependency of CIIP can be addressed from multiple angles; for instance, the need to specifically regulate the (collaborative) management of CII in special laws or treaties, emphasising the no-harm principle and thereby sending an unequivocal signal that a state is willing to play its part in the interdependent organisation of CIIP. Economical means, subsidies and exemptions can be applied to promote cross-border collaboration among private companies. All of the studied strategies pay great attention to the protection of CII, but most do not explicitly highlight the international collaborative aspect. CIIP is at its very core an international task and therefore cross-border collaboration might be taken for granted and not spelled out in black and white.

However, Canada and Croatia, for instance, stress the importance of international collaboration, Italy notes the connection between compliance with international standards and the UK seems to take a true whole-of-system approach, stating that:

> ‘[t]he transformation brought about by this digitalisation creates new dependencies. Our economy, the administration of government and the provision of essential services now rely on the integrity of cyberspace and on the infrastructure, systems and data which underpin it. A loss of trust in that integrity would jeopardise the benefits of this technological revolution.’[69]

Spain, Estonia and Hungary have addressed cross-border dependencies and foreseen measures in national cyber security legislation.[70] Canada continues draw links to the Action Plan for Critical Infrastructures throughout the strategy and also thoroughly covers the need for cross-sectoral and cross-border cooperation[71] .Croatia, on the other hand, targets the issue of CIIP from a more national (whole-of-nation) point of view, whereas the strategy makes a passing reference to the cross-border dependencies while addressing European critical infrastructures. The Czech Republic emphasises the necessity for stronger private-public cooperation.[72] Similarly, Estonia views CIIP as a PPP issue and hence assumes that the cross-border nature of CIIP can be solved within the private sector.[73] Germany stipulates that:

> ‘[e]nsuring cyber security, enforcing rights and protecting critical information infrastructures require major efforts by the state both at national level and in cooperation with international partners.’[74]

Most NCSSs state clearly that cyber security is vital to their CI, and the EU member states link their ECSS to the European Critical Infrastructure Protection Directive and the NIS Directive. The fact that CIIP is well-covered at the regional EU level again speaks for strengthening the cooperation between NATO and EU, since CIIP is undoubtedly a common interest.

However, the majority of the first-generation strategies are quiet on the specific measures taken to promote cooperation and information sharing. This is most often due to the simple fact that there are no concrete governmental incentives (funding programmes, liability exemptions, tax credits, grants) in place. Therefore, as a

[69] UK

[70] In Spain, CI operators must detect and assess cross-border dependencies in the main security plans they have to develop, while CII administrators are required to identify the relationship between ICT and the essential service provided by the CI operator, which must then also be represented in the operator and facilities security plans. In Estonia, the providers of the vital services are required by law to ensure the continuous operation of the vital service in a manner and by means not dependent on information systems located in foreign countries; vital service providers are obliged to perform risk analysis of continuous operations that also consider IT risks. National level risk analyses mandated by the national cyber crisis coordination body (Estonian Information System Authority) include cross-border dependency aspects. In Hungary, there are obligations specified by legal regulation for the state and local government levels, including restrictions regarding data storage and management on territories outside of the European Union or, in certain cases, outside of Hungary. Kaska, Kadri, and Trinberg, Lorena, 2015, 18.

[71] Canada,10-13.

[72] International Telecommunications Union *et al*, Guide to Developing a National Cyber Security Strategy, 2018 (forthcoming).

[73] Ibid.

[74] Ibid.

first step a strategy should aim to set up such encouraging or compelling incentives. Secondly, it should proceed to emphasise the cross-border aspects and create the foundations for cooperation and coordination, which may include specialised information exchange frameworks among CII operators regardless of their location. However, these two strategic measures would only prove viable once a state has a clear overview of how its CII depends on cross-border actors, and therefore the mapping of such dependencies should be declared a priority. The latter would lead to higher levels of situational awareness and facilitate cross stakeholder cooperation in crisis management.[75]

Perhaps the most notable international CII programmes to date are the relevant European Network and Information Security Agency (ENISA) initiatives. ENISA functions as a facilitator of information exchange between member states and EU institutions and identifies best practices and shortcomings, maps threats and strategies against them. However, while providing valuable research and know-how, ENISA's role in practical CIIP has to date remained moderate. Another question is whether governments are actually best placed to foster international CIIP. [76] To this question each and every government can answer differently and also reflect their perspective in the NCSS. When a government decides to take a secondary role, it should nevertheless aim to create a regulatory environment that bolsters cross-border collaboration of the CII operators.

6.1 Recommendations and best practices

6.1.1 Define

Any claim or objective focusing on international collaboration on critical information infrastructure protection should start with defining the key concepts and identifying stakeholders:

> ''Critical infrastructures' Critical infrastructures are organisations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences' (Germany, p 9).

> 'Critical information infrastructure shall mean an electronic communications network, information system or a group of information systems where an incident that occurs causes or may cause grave damage to national security, national economy or social wellbeing' (Lithuania).

6.1.2 Make a statement

If a cyber security strategy aims to reiterate the importance of cross-border collaboration between all stakeholders, whether public or private, it should be stated clearly and followed up by a short explanation:

> 'Ensuring cyber security, enforcing rights and protecting critical information infrastructures require major efforts by the state both at national level and in cooperation with international partners. Given the shared responsibilities of the state, the industry and the society a cyber security strategy will only be successful if all players act as partners and fulfil their tasks together. The same applies to the international context. Since IT

[75] Ibid.

[76] Cukier, K.N., Mayer-Schönberger, V. and Branscomb, L., "Ensuring (and insuring?) critical information infrastructure protection," Harvard Belfer Center, 2005.

> systems are interconnected in global networks, incidents in other countries' information infrastructures may also indirectly affect Germany.'
>
> 'The disruption of critical infrastructure and cyber systems can have direct impacts on businesses and communities on both sides of the Canada–United States border. Attacks on interconnected cyber networks can have cascading effects across industrial sectors and national borders. For this reason, Canada will be active in international forums dealing with critical infrastructure protection and cyber security'.

6.1.3 Set standards

The strategy should highlight specific legislative and regulatory frameworks (when in existence) that outline minimum cyber security standards and requirements for CI/CII operators, taking into account the economic and social constraints they may be facing (ITU, 4.1.3)[77]. This sends a strong signal that your government is determined to follow principles of due diligence and no harm, and to invest in keeping pace with technological developments.

> 'The strengthening of our capabilities to protect critical infrastructure and strategic assets from cyber attacks, with the aim also to ensure their business continuity and the full compliance with international requirements, security standards and protocols' (Italy).

6.1.4 Elaborate

Few of the studied strategies pointed out particular means for promoting cross border or public-private collaboration. However, some were able to hint at particular problems and also suggest in broad terms how the government plans to address them. This, however, assumes that the national cyber security management structure and organisation is clear enough and there is sufficient accurate data and years of state practice that enable pinpointing particular issues. It is understandable that states prefer not to jump into premature conclusions in first generation strategies:

> 'The Government will also make sure that the right regulatory framework for cyber security is in place and harmonised with regimes in other jurisdictions so that UK companies do not suffer from a fragmented and burdensome approach'.
>
> 'Organise crisis training and (CII, edit.)security breach tests at a national, regional and international level in cooperation with the Cyber Defence Unit of the Armed Forces' (Latvia, p.9)

6.1.5 Regulate, but do not forget to reward

Integrating concrete market levers and incentives is an objective that reaches far beyond the realm of CIIP and touches upon all fields in cyber security that depend on balancing public and market interests, information sharing and building trust. A strategy that is designed to stand for stronger international collaboration should therefore consider the establishment of government incentives (e.g. direct/indirect funding, liability protection, tax credits, grants) to encourage, and in some cases compel, operators of CIs/CIIs and related services to implement minimum cybersecurity standards and requirements.

[77] International Telecommunications Union et al, Guide to Developing a National Cyber Security Strategy, 2018 (forthcoming).

6.1.6 Introduce metrics

Metrics are sometimes perceived as the weak spot of cyber security strategies, and this seems to be particularly true in regard to areas that are difficult to measure quantitatively. However, the indicators of developed international collaboration include bi- or multi-lateral agreements with foreign governments and the private sector, clear and understandable regulation of cross-border dependencies, joint CIIP exercises, availability of up to date information on international cross-dependencies, etc.

> ‘Information relating to dependencies on critical services provided from outside the Republic of Estonia is kept up to date, the extent of their impact on the functioning of services is promptly evaluated and associated risks are systematically reduced.’(Estonia)’Assessment criterion: Number of institutions taking part in the activities of the European Union’s Critical Infrastructure Warning Information Network (CIWIN)’ (Lithuania).

7. Military cooperation and cooperative crisis management

The Warsaw Summit crystallised the belief that NATO's collective defence and cooperative security must be as effective in cyberspace as in the domains of air, land, sea and space.[78] The Warsaw Summit decision to declare cyber an operational domain was foreshadowed by numerous academic and policy papers, and hints to it were found in many NCSS published prior to summer 2016. It has hence been long acknowledged that national military forces must not only defend themselves from cyber incidents, but also consider how to use their cyber capabilities in concert with their allies.

Also, it has been become evident that offensive capabilities will be increasingly important in the future and in some cases offensive know-how serves as a prerequisite for effective defence. Therefore, while at first look it might seem that the defence forces are only a second or third rank players in cyber security strategies, a strategy should nevertheless clearly determine a military's role, however restricted it might be. The said role is likely to expand and, like everything else in cyber security, rely ever-increasingly on cooperation with both national and international partners. NATO allies are in a particularly interesting position, since their strategies should reflect their willingness to contribute to the aim of collective cyber defence. The latter, however, is a concept that is still in formulation.

Ekstedt *et al.* suggest in the *National Cyber Security Framework Manual*, that collective cyber defence might entail but is not limited to:[79]

- Using the military or civilians to help defend critical infrastructures in an affected nation,
- Using military or civilians to help on crisis management tasks, from the easiest (note taking and call management) to professional incident responders to lead incident response,
- Deploying forensic investigators to assist the investigation,
- Deploying teams or other groups to assist with coordination with NATO or other nations or sectors. For example, a representative of the FS-ISAC588 could travel to the country to help information flow on attacks to finance; or a military liaison team could do the same for military coordination,
- Ordering (or convincing) Internet Service Providers (ISPs) to block attack traffic destined for the nation under attack,
- Ordering (or convincing) ISPs to throttle traffic to the nation suspected of being behind the attack until they cooperate in helping to end the attack,
- Active defences to selectively disrupt Command & Control infrastructure behind the attack,
- Building additional local Internet Exchange Points and other local infrastructure to help them weather the attack and increase their defensive options,
- Ordering or otherwise ensuring that manufacturers of networking gear prioritise shipments to the country under attack to help them build additional capability,
- An Alliance Member deploying its own offensive cyber forces to engage in counter-attacks on behalf of the Alliance.

[78] Minárik, Tomáš, "NATO recognises cyberspace as an operational domain," *Incyder*, July 21, 2016, https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html
[79] Klimburg, 2012,183-184.

Only the last item on the list can be perceived as a strictly military responsibility; others are multi-stakeholder endeavours where the military can only be one among many coordinated actors. Therefore, in the reviewed strategies the militaries are often mentioned only passingly and in relation to crisis management. All the NATO allies also recognise the need and obligation to promote military cooperation within the Alliance and recognise cooperative security and the possibility of collective defence on the occurrence of an armed attack, the level of detail and abstraction, however, is again varied to a large degree; some foresee concrete points of actions and some hint at the possibility of inter alia developing offensive cyber capabilities. The most commonly proposed lines of action can be divided into 5 subcategories.

Information exchange signifies creating common network of sharing data on recent threats posed to military networks with cooperation partners. This information sharing network should also involve the partners responsible for CIIP and combating cyber crime. Information sharing in its ideal form should not be merely a system of information provisioning, where one party would be legally obliged to report to another on either *ad hoc* or regular basis. On the contrary; at its core, information sharing constitutes a two-way value-adding exchange of information. Nearly all the strategies emphasise the importance of information sharing, while only a few mention particular frameworks such as NATO's Cyber Information and Incident Coordination System (CIICS).[80]

Training and education is generally among the top priorities of any NCSS, however when it comes to international military collaboration, about half of the strategies mention it explicitly in this context. This, however, does not imply that the topic is undeservedly omitted; rather it assumes that the general need for cross-sectoral and international collaboration between partners entails also covers the military aspects. Strategies that have chosen a more abstract and less nuanced formulation therefore usually do not go on to give special emphasis to collaboration in military cyber education. One area that belongs to the same cluster, but is often mentioned in more particular terms is joint exercises. Joint exercises are essential to the preparation for collective crises management, and if a state has contributed to or participated in a military cyber exercise (e.g. Locked Shields or Cyber Coalition), it is usually mentioned in the strategies.

Some nations mention **development of cyber capabilities** either explicitly or implicitly. This is in line with the plan to integrate cyber effects (including offensive) contributed by nations to NATO operations. Understandably, nations are very guarded in their phrasing when referring to operational capabilities, hints to the intention to be prepared to act collectively in cyber are usually interwoven in declarations such as:

> 'The development of military cyber defence capabilities will result in cyber defence being a part of broad-based collective defence. The latter will be ensured by involving specialists 11 from the Defence Forces and the Estonian Defence League, as well as other public and private sector professionals'.[81]:

Another feature that greatly enhances any collaboration and will facilitate joint military response is the **technical interoperability** and **unified security standards** for military systems. Creating a baseline requirement of security

[80] CIICS was developed by NATO Communications and Information Agency (NCI Agency), NATO's IT and cyber arm, as part of the Multi National Defence Capability Development (MN CD2) project to share intelligence, detect and thwart cyber-threats at a faster pace and across multiple countries, with Finland set to join the coalition: SC Media, "Cooperative development speeds Nato cyber-intelligence-sharing", February 27, 2017, https://www.scmagazineuk.com/cooperative-developmentspeeds-nato-cyber-intelligencesharing/article/640374/ .

[81] Estonia, 10-11.

ensures that the weakest links of the chain are still resilient and resistant, and technical interoperability supports hands-on technical aid in and communications in both preventive responsive stages.

PREVENTIVE/PREPARATORY	CRISIS RESPONSE
Information exchange frameworks	Information exchange in crisis situation Contributing cyber effects to NATO defence operations
Training and education	
Joint exercises	
Developing advanced cyber capabilities	
Technical interoperability	

The strategies recognise the need for military cooperation within a similar framework that NATO allies have agreed on in other domains. Examples of this approach include references to developing capabilities on an equal par with these available during air, land and water operations (e.g. Estonia), highlighting the need for enhanced information sharing networks (especially in crisis) and joint exercises. However, the particular lines of action and objectives often remain obscure, partly because nations are still working towards a model of cooperation that does not oblige them to reveal their own capabilities in excessive detail. The area where military cooperation is most critical is most likely combating information theft from government and defence contractors.[82] In CIIP, the military is most often expected to step in when the situation has escalated to a crisis, and prior to that the main weight lies on the shoulders of the private sector.

Therefore, while the need for close cooperation is generally acknowledged, few countries are clear in describing how the collaborative aims are pursued. With the exception of states that face adopted a military cyber strategy, armed forces gain moderate attention and often cyber security is viewed as a civil responsibility. The role of the armed forces is seen for the most part as consisting of crisis prevention and response and includes measures that help to build capacity and resilience, develop technical skills and practice decision making in crisis situation.

[82] Steve Ranger, 'NATO just added cyber weapons to its armoury', ZDNet, November 9, 2017, https://www.zdnet.com/article/nato-just-added-cyber-weapons-to-its-armoury/

Table 6. **Military cooperation in NCSS-s**

	Reference to NATO CDP and/or WT	Training and education	Joint exercises	Information exchange	Developing military cyber capabilities	Technical interoperability and unified security standards for military systems
Canada	X	X	X	X		
Croatia	X	X	X	X		
Czech Republic	X		X		X	
Denmark						
Estonia	X	X	X	X	X	X
France		X	X			
Germany	X			X	X	X
Greece	(x)					
Hungary	X		X			
Iceland	X			X		
Italy	X	X	X	X	X	X
Latvia	X	X	X	X	(x)	
Lithuania	(x)	X	X		(x)	
Luxembourg		X	X	X		
Montenegro		X	X	X		X
The Netherlands[83]	X	X	X	X	X	
Norway				X		
Poland	X	X	X	X	X	X
Portugal	X		X			
Slovakia	X	X	X			
Slovenia	X	X	X		X	
Spain		X		X	X	
Turkey				X		
UK	X	X	X	X	X	
USA	X	X	X	X	X	X

[83] References taken from NL Defence Cyber Strategy.

7.1 Recommendations

1. Define the role of the armed forces in cyber security

Understandably, cyber can be easily be viewed as primarily a civilian issue, and it has been sometimes argued that this is in fact the most optimal approach.[84] However, usually the military plays a role, the extent of which may vary from country to country, but in the very least it should entail the protection of military networks and acting in accordance to the international obligations binding the state, which in case of a NATO ally includes collective defence and crisis response.

2. Declare clearly the willingness to operate in cyber as efficiently as in other domains

The majority of pre-Warsaw strategies already include some notices of how the NCSS relates to international commitments before NATO and the allies. Any post-Warsaw strategy should be explicit about how a state interprets these commitments and preferably manifest the state's approaches to collective cyber defence and developing cyber capabilities.

> 'The development of military cyber defence capabilities will result in cyber defence being a part of broad-based collective defence. The latter will be ensured by involving specialists 11 from the Defence Forces and the Estonian Defence League, as well as other public and private sector professionals' (Estonia).
>
> 'The UK will 'develop the ability of [its] Armed Forces to deploy offensive cyber capabilities as an integrated part of operations' (UK).

3. Express commitment to the protection of military networks

Even if a strategy generally envisions the role of the defence forces as minimal, the very least it should contain is a clear adherence to the protection military networks. This is also an aspect of utmost importance from the perspective of international collaboration, since it signals technical expertise, due care and ability to function as a reliable partner.

> 'Protecting the military command and control networks and ensuring their full operational capability and their resilience has always been a top priority for any state' (Italy).

3. Focus on cooperative training and education (including joint exercises)

A strategy that aims to oter military cooperation should include participation in joint xercises among its core objectives.

> *Also in the future, Slovenia will regularly participate in international exercises on cyber security. Besides that, it will also carry out exercises at the national level. The content of each exercise will possibly be consistent with the risk assessment of a specific treat, however, based on the most realistic scenario possible. At least occasionally, exercises will be carried out with the participation of all stakeholder engaged in cyber security assurance. Thus, all the mechanisms, the preparedness and the interaction of participants will be checked.*

[84] Dunn-Cavelty, Myriam, "The militarisation of cyberspace: Why less may be better" Proceedings of the 4th International Conference on Cyber Conflict (CYCON 2012), NATO CCD COE, 2012.

> *Each exercise will be followed by a detailed analysis of the results and drafting proposals for any improvements and, if necessary, upgrading or updating the security incidents response plan.*

4. Go as specific as you can, but not more

All the lines of action are general enough to allow for a wide range of different interpretations. However, some aspects should be clarified. For example, the commitment to promote information sharing might be in vain when not accompanied a structure that establishes which authority takes the role of the intermediary and oversees the flows of information.

Similarly, if the state finds it critical that the military networks of the allies are interoperable, it should be pointed out so that military collaboration would acquire a concrete technical dimension. On the other hand, a strategy should follow the principle of technology neutrality. This would ensure the sustainability of the strategy in the light of rapid technological developments and also maintain that the stakeholders are free to choose the most appropriate and suitable technology to their needs and requirements for development, as long as it meets the set standards of security and interoperability.

8. Crisis management and CERT cooperation

A national (governmental) computer emergency response team is a group of experts tasked with providing rapid response to cyber incidents to maintain the security and integrity of systems.[85] How a CERT is managed and which governmental agency is responsible for the supervision of the CERT is again up to a given state to decide, and therefore the landscape of how CERTs are run and managed is again varied. The structural differences and a high portion of ambiguity in the management structures remain the most prevalent shortcomings of NCSSs, and not only in relation to CERT cooperation. For example, in some countries CERTs function under the mandate of the Ministry of Defence, while in others, a CERT is seen as a maintenance unit for CII and is subordinated to the Ministry of the Economy; others on the other hand manage their CERTs as law enforcement units that run under the supervision of the Ministry of Interior. Therefore, while reviewing the strategies of the NATO allies from the viewpoint of CERT cooperation, it should be kept in mind that there are overlaps with other areas like law enforcement, CIIP and military collaboration. While a strategy is not a regulatory instrument that lays down in detail how a CERT should be managed, it can provide guidance on what to keep in mind while developing the more elaborate regulatory instruments.

Fostering international CERT cooperation

National-level CERTs should be tasked with building relationships and agreements with one another in order for each to receive timely information on potential threats and vulnerabilities and be able to respond effectively to incidents as a result. CERT cooperation should include determining clear points of contact and agreed-upon methods and channels for information exchange. CERT agreements can also allow technical expertise to be exchanged between countries, helping build the ability of CERTs to respond to emerging malware trends and threats.

SOURCE: Microsoft, Developing a National Strategy for Cybersecurity[86]

[85] Hathaway, M. ed., 2014. Best Practices in Computer Network Defense: Incident Detection and Response (Vol. 35). IOS Press, 81.

[86] Goodwin, Cristin Flynn, and J. Paul Nicholas, “Developing a National Strategy for Cybersecurity”, Microsoft, 2013.

Table 7. **Role of CERTs as addressed in NCSS-s**

	Addressing CERT within strategy	CERTs role defined and outlined within the national strategies
Canada	X	
Croatia	X	
Czech Republic	X	
Denmark	X	
Estonia	X	
France	X	
Germany	X	
Greece	X	
Hungary	X	
Iceland	X	
Italy	X	
Latvia	X	
Lithuania	(x)	
Luxembourg	X	
Montenegro	X	
The Netherlands[87]	X	
Norway	X	
Poland	X	
Portugal	X	
Slovakia	X	
Slovenia	X	
Spain	X	
Turkey	X	
UK	X	
USA	X	

A good start is when the strategy recognises that there are not only cyber threats arising from the interconnected system, but also addresses which national institution is responsible for taking care of them and handling cyber incidents. Some strategies directly and frankly address this very obvious topic and make clear what the task and objective are.[88] In this context, a proactive posture of CERT actions as an expert authority and its mandate are

[87] References taken from NL Defence Cyber Strategy.

[88] Denmark.

often mentioned. It is also a common approach to have just one single responsible authority acting as a CERT as a nexus for all actions and information handling.[89]

In case of an incident, it is crucial to provide all information available to the respective CERT. Therefore information sharing among the providers of electronic financial services, regulatory and supervisory bodies, bodies competent for computer security incidents in the area of public electronic communications and criminal prosecution authorities are mentioned within certain strategies[90] to bolster the position of the respective CERT by means of a stronger structure for confidential information sharing and analysis.[91]

The view on the role of a CERT is that it should establish and form a community which acts as a platform of excellence for sharing best practice and information on cyber incidents, and for operational response services to incidents.[92] A unique and very interesting approach is that the established CERT authority will not only manage national cyber incidents, provide an authoritative voice, act as a centre of expertise on cyber security, and deliver tailored support and advice to departments, but also that it will be part of the Intelligence Service Organisation.[93] That can, of course, have advantages and disadvantages. On the one hand it can draw on the world-class expertise and sensitive capabilities of that intelligence organisation, improving support to the economy and society more widely, but on the other hand it can lead to mistrust among the potential customers and partners because they are dealing from their point of view with an ‘intelligence agency’.

Another way to address cyber threats and incidents is to have a holistic all-hazards risk management approach, which means monitoring and providing mitigation advice, as well as coordination of national responses to any cyber security incident. By using this approach, the roles and mandates for the CERT have to be sharpened and widened in terms of its mandate to be the focal point for monitoring and providing advice on mitigating cyber threats and directing the national response to any cyber security incident.[94]

In this context, some strategies foresee that the legal basis for information exchange and sharing, in terms of special legislation for successful risk management to mitigate the consequences of security incidents must be altered or even brand new laws enacted.[95] A national CERT can also be involved in a coordinated manner through cooperation between the public, private and third sectors, taking into account the interconnectedness and interdependence of existing infrastructure and services in cyberspace and internationally.[96] Sometimes, the strategic view of the foundation strategy paper is left behind and typical operational aspect are blended in when a CERT is tasked to develop a national incident handling procedure that will set a cooperation format, contain a communication matrix and a procedure protocol and define each actor’s role to increase national capacities for active cyber defence and cyber attack counter-measures.[97]

[89] UK.

[90] Croatia.

[91] Netherlands.

[92] Portugal.

[93] UK.

[94] Canada.

[95] Croatia.

[96] Estonia.

[97] Czech Republic.

Within the fast-evolving field of ICT, it is crucial to remain up to date. This aspect is covered under the topic 'training and exercises', both in a national and multinational context, for the respective CERT.[98] By mentioning it within the strategy, this tactical aspect becomes a strategic objective and gains the respective and necessary attention and value.

Fields of improvement are also addressed within the reviewed strategies, such as the absence of a legal basis to allow an efficient response to incidents in public electronic communications networks, because the providers of electronic communications and Internet access services are not required to report incidents to the CERT. Consequently, the instructions of the national CERT for service providers regarding the elimination of incidents are not mandatory.[99] Another example is that the cooperation of stakeholders in cyber security assurance is not formally regulated; however, response centres cooperate informally unless there is a legal basis for it. It is also recognised that there is a lack of personnel, material and technical resources and organisation. This includes providing information about incidents and help in their resolution, the exchange of experience or the use of existing capacities.[100]

8.1 CERT international cooperation

To achieve the overall objective of providing security and responding to incidents, certain strategies also address the international cooperation of their governmental CERTs. It is important that the CERTs are promoted to a single authority and platform to act as the national point of contact for other entities.[101] It is also recognised that good cooperation leads to overall success in preventing, handling and mitigating incident consequences.[102] Cooperation can be carried out in more bilateral or regional way through a coordinated, cross-border approach based on the respective nations' strategies and plans,[103] or it can be in a clear international way to involve of national CERTs in an international network. This engagement can be based either on a voluntary[104] contribution or even outlined in a more definite manner[105] to foster cooperation in cybernetic crisis management at the European level; for instance to cooperate with ENISA or at the Nordic regional level within norCERT.[106] An even wider approach of cooperation is described as taking part with an active role in the European, Atlantic and global organisations and Sectoral Incident Handling Centres and in the Board of European Electronic Communications Authorities, FIRST, Trusted Introducer and ITU-IMPACT.[107]

The development of an information and communication platform to facilitate functional and technical levels of communication among the CERTs and to ensure timely and effective interaction between all stakeholders to

[98] Luxembourg.

[99] Lithuania.

[100] Slovenia.

[101] Italy.

[102] Netherlands.

[103] Canada.

[104] France.

[105] Germany, Slovenia, Spain.

[106] Norway.

[107] Hungary, Montenegro.

counter malicious cyber activity are quite good examples of fostering international engagement.[108] However, one has to bear in mind that international cooperation has some limitations when it comes to information sharing, because there are caveats on what, when and with whom nations will share and disseminate information.[109] In addition, it is a good step if the openness is communicated within a strategy paper to benefit from the experiences of other countries.[110]

A more practical point providing the base for cooperation and to improve the cooperation between CERTs is to have the same handling routines[111] and to prepare a set of standard cyber crisis response procedures for incidents and to establish them through cooperation agreements, both valid and applicable at a regional and global level.[112] In this context, the coordinated international response to incidents[113] is also an important point to be fostered, because responses have a greater impact if they are orchestrated and well prepared.

8.2 Recommendations

8.2.1 Share information about your assets

Each strategy should not only mention that there is a national CERT established, but should also make reference to legal regulations in regard of the mandate and scope of the CERT or give at least a hint what role the CERT has. To give information about the clear objectives, capabilities and strategic limits of a CERT leads to a better understanding and assessment for coordinating responses.

8.2.2 Do not remain silent – share your experience

Information sharing among CERTs or other similar institutions (e.g. FIRST), is crucial and should be foreseen and taken into consideration when thinking about the scope and mandate of a governmental CERT. Information sharing and exchange is not only limited between governmental CERTs, and collaboration with the private sector is also very important and has to be observed, not only for issuing early warnings among the community, but also to establish a network of trust. Beside that, the extensive use of information sharing platforms and tools like MISP (Malware Information Sharing Platform)[114], TAXII (Trusted Automated Exchange of Indicator Information)[115] or STIX (Structured Threat Information Expression)[116] is also recommended and should be fostered among the relevant actors within the community.

[108] Italy.

[109] Luxembourg.

[110] Turkey.

[111] Luxembourg.

[112] Slovenia.

[113] USA.

[114] Homepage of MISP threatsharing platform, http://www.misp-project.org/, last accessed 14 May 2018.

[115] Koen Van Impe, „How STIX, TAXII and CybOX Can Help With Standardizing Threat Information," Security Intelligence, March 26, 2015 https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information/ , last accessed May 14, 2017.

[116]Structured Threat Information eXpression (STIX™) 1.x Archive Website, https://stixproject.github.io/, last accessed May 14, 2018.

8.2.3 Say no to Babylon

The consistent use of recognised international standard procedures and terms in regard of cyber incidents should also be considered and actively formulated within a cyber security strategy. Familiarising the CERTs with each other and having a cohesive effect, training, exercises and exchanging personnel for a limited time can be useful. Establishing channels of communication is also useful for technical coordination in the treatment of computer security incidents, as it is undertaken through the quick and fast cooperation of the respective CERTs bodies. The existence of permanent 'single points of contact' would contribute to direct and effective communication and thus also to the prevention and more efficient treatment of incidents.

9. Conclusions

The study aimed to compare how the NCSS-s of NATO Allies address international collaboration in the fields of: law and norm creation, combating cyber crime, technical standards, critical information infrastructure protection, military cooperation, crisis management and CERT cooperation. As a general tendency international collaboration gained the deserved focus when it came to legislative issues, technical standards and fight against cyber crime. At the same time CIIP, military cooperation and CERT cooperation were sometimes looked at from a more internal angle or in case of CERTs, the main hindrance turned out be the absence of concrete management and information sharing structures.

International collaboration is essential for managing trans-border cyber threats. There is no uniform way to deal with legislative matters in NCCS as international law also has various aspects dealing with cyber security matters depending, for example, on the nature of the threat and its origin. A national cyber security strategy gives guidance for future developments in legislation, policies and other recommendations. Participation in international cooperation can lead to new commitments for states. NCSSs have to reflect a nation's contemporary position on international law discussions, while being flexible enough to evolve as understanding continues to grow. An NCSS also has an informative purpose; it informs different stakeholders within the nation and also other nations of current and evolving development of nation's attitude towards legislative matters. There are different maturity stages among countries regarding the digitalisation level of their society and cyber security. While it can be argued that the less developed countries have very little to give to international collaboration and norm development, there is also alternative approach; collaboration with less developed countries can safeguard the common security of all nations when there are no 'weak links' in the global chain.

Like international, national legislation also tends to approach cyber security issues in a fragmented way. All nations have sovereignty over cyber infrastructure and activities located in their territory. International law and the commitments that the state has made confine cross-border activities. On the other hand, the state has to ensure that its territory is not used in a way that affects the rights of and produces serious adverse consequences for other states. International law and the commitments that derive from it (conventions, treaties etc.) may create the need to harmonise national legislation to be compatible with these commitments. While states as a principle enjoy the right to exercise territorial and extraterritorial jurisdiction over cyber activities, a need for possibly completely new domestic legislation can benefit from the best practice of other nations and international collaboration.

Perhaps the one field where strategies almost unequivocally put an emphasis on international collaboration is combating cyber crime. States recognise cyber crime as one of the most challenging and emerging issues on their agendas, and work extensively at the national and multinational levels to cope with this issue. The most relevant tool for an international approach is the Convention on Cybercrime, which helps to facilitate the fight against cyber crime. Information sharing and exchange of relevant data is crucial for success. Similarly, standardisation is often viewed as not only a route towards greater security but also towards harmonisation on the international level. The application of relevant standards is essential for achieving the goals of information security because standardisation itself fosters the overall approach. Beside this, standardisation brings every stakeholder to the same page, but one has to be aware that standardisation just for the sake of standardisation is counterproductive and hampers the overall approach. When it comes to CIIP, CERT and military cooperation the extent to which international cooperation is granted the attention it deserves varies remarkably. In regard of CERTs, international cooperation is the most valuable and underestimated issue. In times of the interconnected and trans-border networks and devices, as well as threats towards those assets, limitation to your own ground and a narrow view is wrong. That is why, from the perspective of a CERT, international cooperation and exchange of information is mission essential to fulfil the task and achieve the respective goals.

Critical information infrastructure protection is among the top three priorities reiterated in every reviewed strategy, but usually the cross-border element receives less attention than it deserves. This might be due to the complexity of the international interdependent network of CII operators. The majority of nations do not mention comprehensive mapping of cross-border CII dependencies as key objectives in their strategies, but this would be the logical first step towards efficient collaboration in CIIP. Also, when it comes to international military collaboration, the need for close cooperation is generally acknowledged, but few countries elaborate on how the collaborative aims are to be pursued. The role of the armed forces gains moderate attention and often cyber security is viewed as a civil responsibility. The role of the armed forces is seen for the most part as consisting of crisis prevention and response and includes measures that help to build capacity and resilience, develop technical skills and practice decision making in a crisis situation. In the light of Warsaw Summit, a strategy should contain a summary of the state's vision on what constitutes cooperative security and collective defence in the cyber domain. A strategy should also send a clear signal of a state's willingness to meet its international commitments and define the military's role, however limited that might be.

Therefore, although strategies that did not aim to build any bridges between like-minded nations were scarce, some areas like CIIP and CERT cooperation (Chapters 5 and 7 respectively) would definitely benefit from more precise formulations and goals. Tables found in the end of each chapter present a visual comparative overview of how NCSSs envision international collaboration and pinpoint areas where it is prioritised and where it should gather a stronger focus.

10. Sources

10.1 Journal articles, books, research papers

1. Cukier, K.N., Mayer-Schönberger, V. and Branscomb, L., "Ensuring (and insuring?) critical information infrastructure protection," Harvard Belfer Center publication, 2005. 2. Dunn-Cavelty, Cavelty, Myriam Dunn. "The militarisation of cyberspace: Why less may be better," in 2012 4th International Conference on Cyber Conflict (CYCON 2012), NATO CCD COE, 2012.
2. Goodwin, Cristin Flynn, and J. Paul Nicholas, "Developing a National Strategy for Cybersecurity", Microsoft, 2013.
3. Kaska, Kadri, and Lorena Trinberg. "Regulating Cross-Border Dependencies of Critical Information Infrastructure," NATO CCD COE, 2015.
4. Hathaway, M. ed., *Best Practices in Computer Network Defense: Incident Detection and Response* (Vol. 35). IOS Press, 2014.
5. Klimburg, Alexander (ed). 'National cyber security framework manual,' NATO CCD COE, 2012.
6. Luiijf, Eric, Kim Besseling, and Patrick De Graaf. "Nineteen national cyber security strategies." International Journal of Critical Infrastructures 6 9, no. 1-2 (2013): 3-31
7. Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press, 2017.
8. Shackelford, Scott J., and Andraz Kastelic. "Toward a State-Centric Cyber Peace: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity." *NYUJ Legis. & Pub. Pol'y* 18 (2015): 895.

10.2 Newspaper articles and web materials

1. Koen Van Impe, „How STIX, TAXII and CybOX Can Help With Standardizing Threat Information," Security Intelligence, March 26, 2015 https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information/.
2. ZDNet, 'NATO just added cyber weapons to its armoury', 9 November 2017.

10.3 Reports, databases and papers by international organisations

1. ENISA, National Cyber Security Strategies Map, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map
2. International Telecommunications Union *et al*, Guide to Developing a National Cyber Security Strategy, 2018 (forthcoming)
3. NATO CCD COE, National Cyber Security Documents Database, https://ccdcoe.org/cyber-security-strategy-documents.html.

4. Organisation for Economic Co-operation and Development (OECD), Cybersecurity, Policy-making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy, 2012 http://oe.cd/cybersecuritystrategies.

5. UN General Assembly. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." *A/68/98* 24, 2013.

10.4 International and national law

European Union

1. Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection.Official Journal L, 345(23), 12.

2. Directive 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, OJ L 194

Council of Europe

1. Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

2. Council of Europe, Convention on Cybercrime, 23 November 2001, ETS No.185.

NATO

1. North Atlantic Treaty, 34 UNTS 243; 43 AJILs 159.

UN

1. United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XV