NCSS: A Global Census of National Positions on Conflict, Neutrality and Cooperation

Radu Antonio Serrano Iova[1] and Tomoe Watashiba[2]
[1]Ragnar Nurkse Department, School of Business and Governance, Tallinn University of Technology, Tallinn, Estonia
[2]School of Governance, Law and Society, Tallinn University, Tallinn, Estonia

raduantonio.serranoiova@taltech.ee
tomoetw@tlu.ee

Abstract: The ubiquity of ICT and the increase in cyber threats have pushed countries to view cybersecurity from a national perspective and draft appropriate national strategies on the topic. While containing similar terminology, these strategies are tailored to the national contexts and hence, differ across regions, cultures, and political contexts. Previous research of these documents has been focused on comparative analysis of countries that can either be considered well developed on this topic or for specific subtopics of cybersecurity. However, some of the subtopics have not been addressed, only now having become more prevalent due to current international conflicts and national / regional socio-political scuffles that have spilled into cyberspace. In our paper, we investigate all countries that have published a National Cyber Security Strategy - NCSS - (or any similar document under a different nomenclature, e.g., policy, decree, etc.), specifically in reference to their position on war, neutrality, and international cooperation. Countries maintaining an NCSS will first be identified using international databases, upon which further study of the aforementioned topics in the NCSSs will occur. We hypothesize, that while international cooperation will be present in most, if not all NCSSs, armed conflicts and neutrality will not be addressed at all nor in depth, in those that contain any reference to them. The resulting paper will present a near-global case study of these topics, which can then signify potential areas of improvement, capacity building, and strengthening of democratic coalitions, globally.

Keywords: National Cyber Security Strategy, International Cooperation, Neutrality, Conflicts, Cyberspace

1. Introduction

Russia's latest invasion of Ukraine was not only undertaken through physical means. Since 2014, the latter has been on the receiving end of targeted cyber attacks which only increased during the invasion. Satellite networks, border checkpoints, telecommunication service providers, banks, power stations, governmental services, and even non-governmental, charity, and aid organizations, among others, were attacked in the first two months of the conflict (Przetacznik and Tarpova 2022). Additionally, in 2022 only, Andorra, Australia, Bahrain, China, Costa Rica, Ethiopia, most EU countries (and its own Commission), India, Iran, Jordan, the Marshall Islands, Mexico, Pakistan, the U.K., the U.S.A., Vanuatu, and many other countries, have been targets (and sometimes even perpetrators) of cyber-attacks. Not even international humanitarian organizations, such as the International Committee of the Red Cross, have been exempted from such aggressions (CSIS no date).

These examples and the ubiquity of ICT have resulted in countries publishing their own National Cyber Security Strategies (NCSSs), or similar documents. Although these documents differ in their formatting characteristics, they all present their nation's official position on the issue of cybersecurity. Because of the invasion and the never-ending number of cyber-attacks, we decided to investigate all the countries' references on war, neutrality and international cooperation in these documents. We hypothesize that very few United Nations' (U.N.'s) members have declared their cybersecurity actions during war nor discussed neutrality in any way in their current NCSS. Moreover, we believe that all NCSSs will talk about international cooperation, given the borderless nature of cyberspace, and that countries will reference their allied preferences. This resulting paper will serve as a snapshot of the topics, allowing individual countries to improve themselves and their bi- and multilateral endeavors.

2. Strategy, topics and previous studies

Prior to anything, the concept of a National Cyber Security Strategy (NCSS), or similar document, should be defined. Traditionally, "[a] *strategy of a business forms a comprehensive master approach that states how the business will achieve its mission and objectives"* (Wheelen et al. 2017, p.50). Transposed to the public sector and scaled up to a larger context, a national strategy is *"the identification of national interests and ambitions and the use of various resources (national and other) to preserve or pursue those interests and ambitions"* (Cornish, Lindey-French and Yorke 2011). Framed more specifically toward the notion of the security of a country, it becomes then a national security strategy. These documents are usually addressed to "*adversaries or potential*

enemies" (Drew and Snow 1988, p.48). However, by being public, in addition to serving as possible intimidation to an enemy, they might serve political purposes such as influencing public opinion, swaying specific constituencies (Caudle 2009), and even communicating with existing and potential allies, or non-aligned stakeholders. The cyberspace has become part of national security, as evidenced by multiple writings (e.g. Reveron 2012; Yannakogeorgos and Lowther 2016; Libicki 2018) throughout the years. Therefore, an NCSS is a document that identifies interests and ambitions related to national cybersecurity and communicates the use of resources to reach those goals.

Like national security strategy, an NCSS can "*vary widely in length, format and complexity*" (DuMont 2019), from country to country. Given that language, year of publication, and national contexts differ across the world's NCSSs, this variety can easily affect the title and contents of the document. However, as the logical offshoot of the former, some of an NCSS' characteristics are handed down. Some of these, compiled by DuMont (2019) include: having an endorsement by the governmental leader, reflecting national values, articulating national interests, declaring a strategic vision, identifying and assessing future challenges, and containing risk assessments, resources overviews, timeframes effectiveness measurements and implementation guidance. Therefore, a high-level document that presents most, if not all, of these elements would be considered as an NCSS and studied as one of its peers. Some outlier variations have been named 'national policy' or 'national doctrine'

Another variable that might have also affected the selection process is the 'cyber security' term. Sidestepping the linguistical connotations of having it in a single word, or not, some documents are titled using the terms information security, digital security, and Information and Communications Technology (ICT) security. While these were sporadic cases, and some even due to their translation into English or original date of publication, we have taken them all as synonyms. Von Solms and Van Niekerk's (2013) position on two of those terms (even though they acknowledge that cyber security and information security are often used interchangeably) could shed additional light for those inquiring about the similarities and differences in terminology. Nevertheless, it is within this variety of terminology and contexts that we felt that a global study was necessary to discover and present the countries' positions on the topic of warfare, neutrality, and cooperation.

2.1 Warfare / War/ Conflict

According to Merriam-Webster's dictionary, 'warfare' is defined as "*military operations between enemies (hostilities, war),*" also meaning "*an activity undertaken by a political unit (such as a nation) to weaken or destroy another.*" (Merriam-Webster no date) Oppenheim's International Law similarly defines war as "*a contention between two or more states, through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases*" (Lauterpach 1952, p.220). In understanding the use of 'warfare' or 'war' in our analysis, we have followed these general definitions, essentially understanding war or warfare as a hostile operation between two or more parties, usually involving extensive employment of forces aimed at countering the other(s). Conflict is a state where friction exists between parties, diplomatically, economically, politically, militarily and/or otherwise; yet to treat some conflicts as 'war' for states has significant legal implications and consequences, such as the application of the law of war and the law of neutrality, suspension of non-hostile relations (e.g. trade, diplomatic, treaty relations) between the belligerents, as well as the prohibition of the Use of Force under Article 2(4) of the U.N. Charter (Greenwood 1987). Therefore, in a factual sense, States avoid using 'state of war,' yet often, in the colloquial use of the terms, 'war', 'warfare' or 'conflict' are used more or less interchangeably. In this analysis, we, therefore, have followed the interchangeable usage of these three words.

2.2 Neutrality

In this analysis, the word 'neutrality' has been identified from two different angles, one from the law of neutrality as defined in the International Humanitarian Law (IHL) and the other from the internet/technological neutrality. The law of neutrality, when applied in cyberspace, entails duties such as abstention/non-participation, better expressed as "…*abstain*[ing] *from committing any acts of kinetic or cyber hostility against belligerents and providing them with military assistance, such as the provision of cyber weaponry or the recruitment of a cyber "corps of combatants"…"* or prevention, meaning *"…neither allow nor tolerate certain types of malicious activities on its territory and infrastructure*…" as well as the maintenance of impartiality, "…*apply[ing] every restricting measure and prohibition in the context of its neutral duties and rights in a non-discriminatory manner toward all belligerents.*" (Cordey and Kohler 2021, p.1). There are other elements, including the respect for a neutral state's territorial integrity and the ban of cyber operations against/from/through neutral nations,

particularly for a belligerent country, with both neutral and belligerent states to be taken into account. The law of neutrality's applicability is confined to international armed conflicts (IAC) as defined in IHL and state actors.

Internet / technological neutrality is another aspect of neutrality that is relevant to this analysis, and it is generally understood to mean that Internet Service Providers (ISPs) ensure 'neutrality' in the flow of the internet traffic, treating equally, the contents that pass through their cables, cellular towers, satellites and other core infrastructures (Wu 2003), and "[w]*hen providing internet access services, providers of those services should treat all traffic equally, without discrimination, restriction or interference, independently of its sender or receiver, content, application or service, or terminal equipment*" (European Union 2015, Preamble (8)).

2.3 International Cooperation

In this analysis, we have approached the term 'international cooperation' from the perspectives of both development assistance with a closer connotation to capacity-building and part of confidence-building measures where information and intelligence sharing may be conducted between/among countries. The capacity-building, in general term, is defined by the U.N. as "*the process of developing and strengthening the skills, instincts, abilities, processes and resources that organizations and communities need to survive, adapt, and thrive in a fast-changing world*" (U.N. no date) and in a more specific case of 'cyber capacity-building,' we have followed the meaning of assistance or cooperation to "*strengthen a country's legal, technical, and policy capability, and protect against malicious cyber activity*" (Naylor, Painter and Hakmeh 2022). Confidence-Building Measures (CBMs) are considered to be "*a verified instrument of international politics, which aims to prevent the outbreak of war or an (international) armed conflict by miscalculation or misperception of the risk, and the consequent inappropriate escalation of a crisis situation*" and they "*achieve this by establishing practical measures and processes for (preventive) crisis management between States.*" (Ziolkowski 2013, p.5). In the cyberspace context, CBMs could include sharing, providing, and exchanging information about cyber threats and vulnerabilities as well as best practices, facilitating communications through voluntary mechanisms such as the meeting of experts, provision of contact data, sharing of information through workshops, etc., at international and regional levels.

2.4 Past studies

Previous studies regarding NCSSs have compared EU and NATO cybersecurity strategies to national cyber security strategies (Štitilis, Pakutinskas and Malinauskaitė2017), attempted to discover governance trends (Shackelford and Kastelic 2014) and even present correlations between NCSS development to that of a digital economy (Teoh and Mahmood 2017). Other studies, for example, have focused on a comparative contents analysis of NCSSs of selected countries, often considered to be more 'advanced' or 'elaborate,' to identify differences and similarities, and to draw conclusions on recommended approaches and contents to be potentially considered by policymakers (OECD 2012; Luiijf, Besseling and Graaf 2013; Newmeyer 2015; Sabillon, Cavaller and Cano 2016; Shafqat and Masood 2016). In a similar vein, an attempt to utilize the quantitative analytical tool (e.g., Latent Dirichlet Allocation) for more comprehensive and automated analysis and understanding of texts has also been conducted (Kolini and Janczewski 2017), as well as more in-depth country-specific investigations (for example, see Daricili and Özdal 2018; Hurel 2020; Beecroft 2021).

3. Methodology

The methodology used for this article involved the systematic collection and synthesis of existing information, i.e. literature review. A literature review is a great way to summarize findings to uncover areas where research (Snyder 2019) or improvements are needed. As described by Snyder (2019), the aim of a systematic review allows for the identification of all evidence that fits a criterion to answer a particular question or hypothesis.
Out of the 193 member states of the United Nations, this study was conducted on the states that had publicly available National Cyber Security Strategies or similarly high-level national documents on the topic, in December 2022 and early January 2023. Identification of these states was conducted mainly through the eGA's National Cyber Security Index (available at https://ncsi.ega.ee/) and UNIDIR's Cyber Policy Portal (available at: https://cyberpolicyportal.org/). The former is *"… a global live index, which measures the preparedness of countries to prevent cyber threats and manage cyber incidents …"* and *"… also a database with publicly available evidence materials and a tool for national cyber security capacity building."* (eGA no date) The latter is *"an interactive map of the global cyber policy landscape. It provides profiles of the cyber policies of all 193 UN Member States…"* and *"… seeks to support informed participation by relevant stakeholders in all policy processes*

and promote trust, transparency, and cooperation in cyberspace." (UNIDIR no date) The benefit of these tools is that they provide direct links to official third-party websites that might contain the NCSS or similar document. The NCSS, of every country that had one, was checked to verify that it was an official document (i.e., published by official sources, the government of that country) and that it was the current version. For this latter characteristic, even if a NCSS had an expiry date, it would still be considered the current one if it was still publicly present in a governmental website and if no other NCSS had been published. For example, there was a nation that had a previous version of their NCSS in English, but the current one was only found in their official language. In this case, the one in the official language was the current official document.

After all corresponding NCSSs were identified, they were individually searched on the three proposed topics: warfare, neutrality and international cooperation. The keywords used were 'war', 'warfare', 'conflict', for the first topic, 'neutrality', 'neutral', for the second one, and 'cooperation', 'collaboration' in the international context, for the third one, with the corresponding terms in other languages. Their presence was noted, grouped, and analyzed further, as presented in the next section. For a more compact presentation of the results, the countries presented in the subsequent section have been noted using the ISO 3166-1 alpha-3 country codes, in the alphabetical order of their full names. The ISO 3166 standard can be found at: https://www.iso.org/iso-3166-country-codes.html

4. Results

In the end, 113 (out of the 194) U.N. member states had publicly accessible current NCSS, or a similar high-level document. Most NCSSs were presented in their national languages, but they also had a version in English, which allowed for an easier execution the topic search. After English, the NCSSs were found to be drafted in Spanish, French, Russian, Portuguese, Arabic and Romanian, with the remaining ones each in a different language (see

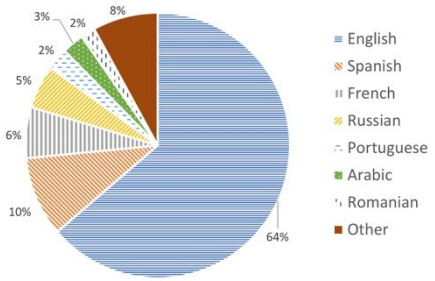

Figure 1 Language availability of the NCSSs

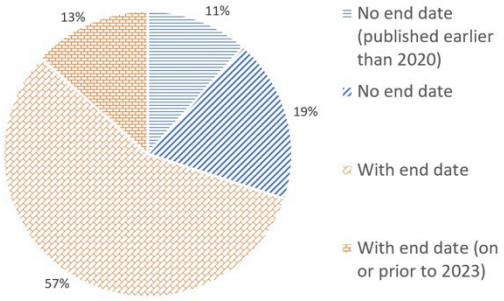

Figure 2 NCSSs with and without end dates). While there is no obligation to publish an NCSS in English or any alternate language, the majority of the countries have done so, with some even specifying that the translation is a courtesy and should any discrepancies arise, the NCSS in their national language shall prevail.

The large majority of the NCSSs have been established for a definite period of time, i.e., 79 of them contain an end date. However, 15 of them have an end date of 2023 or prior, meaning that they are close to or already expired. The remaining 34 NCSSs do not have an end date, out of which 13 have been published prior to 2020, with the oldest entry dating back to 2003, followed by 2011.

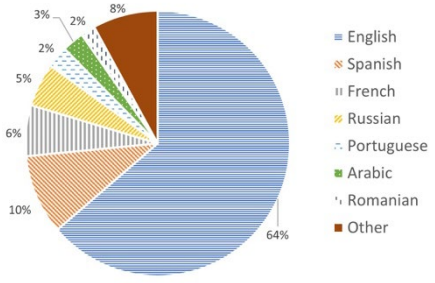

Figure 1 Language availability of the NCSSs

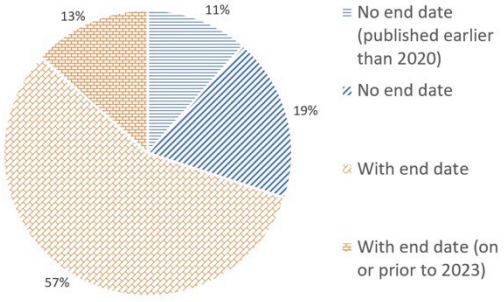

Figure 2 NCSSs with and without end dates

On the topic of warfare, 66 of the NCSS mention the terms 'war', 'warfare', 'conflict' and their types, in multiple lines of context, sometimes more than once in a single document (Figure 3). More than half of them allude to war / conflict, or a specific type thereof, as a threat to the nation, and in most cases in the sections describing the current situation of the country or the reasons behind the creation of the NCSS. As presented in Figure 3, in this context, we have the highest variety of descriptors referencing different types of warfare or conflict. The

second most common context was regarding the prevention of war or conflicts. Similarly, there was not much specificity, with the common trend being the need to prevent such armed or cyber actions. Next, we have thirteen nations that talk about their preparations for or existing preparedness in case cyber, hybrid, armed or cyberspace warfare. These will be discussed in more detail in upcoming paragraphs describing Figure 4. In the less mentioned contexts, six countries clearly state the entity / organization responsible for cyber warfare, while four of them outright express that it is an area of improvement for their state, and three others declare that the cyberspace is a domain of warfare. Finally, in the miscellaneous context we have both Japan and Malta, since the former alludes to the necessity of international collaboration, while the latter that it would work to establish its own national position.

Type of War / Warfare / Conflict	Context	Countries
Cyber, Hybrid, Military, Information, Cyberspace, International, Armed, Asymmetric, Electronic, Psychological, Imagological, Command-control	As a threat	AUS - AUT - BEL - BGR - BFA - CYP - EGY - EST - ETH - GEO - GRC - HUN - IRQ - JPN - KEN - LTU - LUX - MLT - MCO - MNE - MOZ - NLD - NGA - PNG - PHL - PRT - KOR - MDA - RWA - SRB - SVN - CHE - TJK - TKM - GBR
Cyber	As a domain of Warfare	ALB - LTU - UKR
Information, Cyber, Electronic	As area of Improvement	GMB - LBN - ZAF - TJK
Cyber	Organizational Responsibilities	BRA - BGR - SWZ - SEN - ZMB - VNM
Armed, Cyber, Cyberspace	Prevention of	ARG - AUT - CHL - CHN - HRV - CZE - FRA - DEU - MCO- NZL - ROU - ESP - UGA - USA
Cyber, Hybrid, Cyberspace, Armed	Preparedness	DEU - LVA - MUS - NLD - MKD - NOR - POL - KOR - RUS - ZAF - SWE - CHE - THA
Cyberspace, International	Miscellaneous	JPN - MLT

Figure 3 Mentions of war / warfare / conflict in 66 NCSSs

Figure 4 presents the 13 countries that reference their preparations and preparedness for or during times of war. Most of them allude to existing capabilities, albeit in extremely short descriptions, while a few of them state that they will or must prepare such capabilities. There is no other presential common trend apart from the fact that a majority of these NCSS are currently outside their ending date.

Country	Title of the Document	Preparedness
DEU	Cyber Security Strategy for Germany 2021	In case of conflict, contact persons will be available, and already established, reliable channels of communication can be used. (p. 114)
LVA	Informatīvais ziņojums "Latvijas kiberdrošības stratēģija 2019.–2022. gadam" (Informative report "Latvia's Cyber Security Strategy for 2019-2022")	Similarly, in times of crisis and war, the government must ensure the protection of information and cyberspace using active and passive defence measures to prevent external influence on the population and paralyzing government action (Task 2.2). (p. 17)
MUS	Republic of Mauritius National Cyber Security Strategy 2014 - 2019	National cyber resilience will be tailored to ensure the preparedness and predictive capabilities required by the goals and to facilitate its operating capability during cyber conflicts and post-conflict recovery. (p. 8)
NLD	Nederlandse Cybersecuritystrategie 2022-2028 (Dutch Cyber Security Strategy 2022-2028)	The government has offensive and defensive cyber capabilities that are effective in times of peace and war. (p. 38)
MKD	Republic of Macedonia National Cyber Security Strategy 2018 - 2022	5. Development of national procedures in time of peace, crisis, a state of emergency and state of war, in order to manage incidents which will enable efficient intra-institutional cooperation, where every institution have a pre-defined role, will employ appropriate protocols and procedures, as well as information exchange, communication and coordination channels. (p. 18)
NOR	National Cyber Security Strategy for Norway	Civilian support of the Norwegian Armed Forces in the event of cyber security challenges in times of crisis and armed conflict is provided within the framework of the total defence concept. (p. 10)
POL	Cybersecurity Strategy of the Republic of Poland for 2019 - 2024	The Armed Forces of the Republic of Poland, as the fundamental element of the state defence system, should be involved in activities in cyberspace at the same level as in the air, on the ground and at sea, in peacetime, during war and in crisis situations alike. (p. 24)
KOR	National Cybersecurity Strategy	Promote cooperation in sectors such as national defence, intelligence, and law enforcement, as well as exchange with the private sector to respond to cybersecurity threats, including acts of war, terrorism, and crime. (p. 23)
RUS	Указ Президента Российской Федерации от 05.12.2016 г. № 646 Об утверждении Доктрины информационной безопасности Российской Федерации (Decree of the President of the Russian Federation of December 5, 2016 No. 646 On approval of the Information Security Doctrine of the Russian Federation)	8. National interests in the information sphere are: ... ...b) ensuring the stable and uninterrupted functioning of the information infrastructure, primarily the critical information infrastructure of the Russian Federation (hereinafter referred to as the critical information infrastructure) and the unified telecommunication network of the Russian Federation, in peacetime, during the immediate threat of aggression and in wartime;
ZAF	National Cybersecurity Policy Framework for South Africa	In order to protect its interests in the event of a cyber-war, a cyber defence capacity has to be built. (p. 24)
SWE	A national cyber security strategy Skr. 2016/17:213	An effective national cyber defence is developed and strengthened in peacetime and as part of total defence planning and must be capable of functioning in peace, crisis and war. (p. 18)
CHE	National strategy for the protection of Switzerland against cyber risks (NCS) 2018-2022	In order to prevent such activities, Switzerland must therefore include cyber defence and cyber diplomacy in its preparations for potential conflict. (p. 4 - 5)
THA	National Cybersecurity Strategy 2017-2021	3. Have a plan to face cyber threats when there is a national cyber crisis or cyber war. (p. 39)

Figure 4 Preparedness in case of war / warfare / conflict

Out of the 133 NCSS, only five countries reference the concept of neutrality in their documents. Two of them refer to Internet neutrality, two others to technical/technological neutrality, and the last one to Information neutrality (Figure 5). No other NCSS explores the any neutrality concepts, associated or not, with cybersecurity.

Country	Title of the Document	Mention of Neutrality
BLR	Концепция информационной безопасности Республики Беларусь (Concept of Information Security of the Republic of Belarus)	CHAPTER 8 **INFORMATION NEUTRALITY** 31. In international relations, the information sovereignty of the Republic of Belarus is ensured, among other things, on the basis of the principle of **information neutrality**, which provides for a peaceful foreign information policy, respect for the generally recognized and generally accepted rights of any state in this area, and the exclusion of the initiative to interfere in the information sphere of other countries aimed at discrediting or challenging their political, economic, social and spiritual standards and priorities, as well as damaging the information infrastructure of any states and participating in their information confrontation...
CHL	National Cybersecurity Policy	Therefore, the policy includes and promotes the following: ... - ...the principle of respecting **Internet neutrality** is also included, so that Internet service providers may not discriminate or arbitrarily restrict the access to any content whatsoever, unless there is a legal justification to do that. (p. 20)
SWZ	Eswatini National Cybersecurity Strategy 2020 - 2025	It is important that the established cybersecurity legal and regulatory framework for Eswatini is suitably applicable and **technology neutral**. (p. 21)
KGZ	Стратегия кибербезопасности Кыргызской Республики на 2019-2023 годы (Cybersecurity Strategy of the Kyrgyz Republic for 2019-2023)	At the same time, it is necessary to take into account international experience, best practices and recommendations, but at the same time proceed from the specific conditions of the Kyrgyz Republic, which include the following: ... - an extremely small volume of the domestic market of tools and solutions for the information technology and communications industry, including the cybersecurity sector of the Kyrgyz Republic, and almost complete dependence on foreign suppliers of software and hardware products. This circumstance increases the importance of the task of developing a national certification system for imported products in the field of information technology, as well as testing it for vulnerability and undeclared capabilities in order to maintain **technical neutrality** and sovereignty.
ESP	National Cybersecurity Strategy 2019	To do this, it [Spain] will defend an interoperative, **neutral**, open and diverse **internet**, a reflection of international cultural and linguistic plurality, based on a system of democratic, representative and inclusive governance resulting from agreement and consensus. (p. 39)

Figure 5 Mentions of neutrality in only 5 NCSSs

International cooperation was discussed in all the NCSS, apart from two countries. Forty-nine countries only mentioned international cooperation as general as possible, with the rest being a bit more specific and presenting a mixture of mentions ranging from 'regional', 'bilateral' and 'multilateral' to specific countries, country blocs and/or organisations. Additionally, fifteen nations used non-binding terminology such as 'strategic (foreign) partners', 'like-minded countries', 'friendly countries', 'strategic allied countries', 'ally/allies', 'similar thinking countries', 'partners abroad', 'international partners' (Figure 6). Two outlier cases used a different approach for noncommittal terms for international cooperation; the Russian Federation, which mentioned 'interested parties' and Brazil, declaring 'the largest possible number of countries'. The most mentioned country bloc was the EU, with appearances in twenty-six individual NCSS, and the most mentioned organizations were the NATO, the UN and the OSCE, with eighteen, sixteen and thirteen mentions respectively.

International Cooperation and terms mentioned	Countries
"International" only	ARG - AUS - BGD - BLZ - BRA - CPV - CAN - CHL - CHN - COL - CRI - DOM - ECU - SLV - ETH - GTM - IND - IRL - ISR - JOR - KEN - KIR - LBN - MYS - MRT - MUS - MEX - MAR - MOZ - NZL - NIC - MKD - NOR - PAN - PRY - PHL - QAT - MDA - RUS - RWA - SAU - SEN - CHE - TJK - TUN - TKM - UKR - GBR - USA
"Regional"	AFG - BEN - CZE - SWZ - GMB - IRQ - JAM - KAZ - KWT - KGZ - MWI - NGA - ROU - ZAF - ZMB - UGA
"Bilateral" or "Multilateral"	BLR - BFA - HRV - MCO - MLT - TUR
Specific Countries (or Country blocs)	AUT - CYP - FIN - FRA - GEO - DEU - GRC - ITA - SGP - ZAF - THA
Specific Organizations	BEN - EGY - MCO - MNE - PAK - PER - SRB - LKA - UGA - VNM
Both specific Organizations and Countries (or Country blocs)	ALB - BLR - BEL - BGR - BFA - HRV - CZE - DNK - EST - HUN - ISL - JPN - KAZ - LVA - LTU - LUX - MLT - NLD - NGA - PRT - WSM - SVK - SVN - ESP - SWE - ZMB - TTO - VUT
"Strategic Partners", "Like-minded countries", "Friendly countries"	ALB - DNK - EGY - EST - GEO - JPN - LVA - PNG - POL - PRT - KOR - ROU - SWE - THA - VNM
No mention of cooperation at all	BHR - ARE

Figure 6 International Cooperation expressed in NCSSs

5. Discussion

Overall, we found that the fact that 113 (out of the 194) member states have publicly accessible NCSS shows higher interest and need for this or similar types of policy documents for member states. Given the evolving nature of technology and its effect on the government and citizens, having an effective cyber security strategy for the operation and protection of national assets, including its infrastructure and people, has become one of the key national strategic issues to address at all levels of society. As NCSSs serve to define a vision for national cyber security and, sometimes, the implementation policies and plans for all stakeholders concerned, with significant implications for coordination of both technical and personnel resources within a given timeframe, it is commendable that the majorities of member states have fresh NCSSs with a definite period of time. With most of the dates being very recent, we can say that the formulation of NCSS is a recent, up-to-date phenomenon.

Also, with a sheer number of publicly available NCSSs and oftentimes with their translations in major languages, we see that one of their purposes is of an international nature, that is, to communicate how states perceive and act in terms of cyber affairs, particularly to other states – 'like-minded' or not. Therefore, in addition to domestic coordination and resource mobilization purposes, the critical aspect of NCSSs and their publication is sharing of the nations' positions and views about cyberspace governance with foreign policy implications, and our analysis of the three key aspects ('war', 'warfare', 'conflict'/ 'neutrality', 'neutral'/ 'cooperation', 'collaboration' in the international context) has given valuable comparative insight as to states' positions and views about these aspects.

In terms of 'war', 'warfare', and 'conflict', it is recognizable from the analysis that we could almost say that it is a common understanding among most states that the threat in cyberspace from foreign states or non-state actors is potentially at the scale and scope of 'war', 'warfare' or 'conflict'. And from this rather collective use of 'war', 'warfare', and 'conflict' in the analysis, we understood that the inference might be made in terms of why the overwhelming number of NCSSs includes the term 'international cooperation' in varieties of contexts. One way of averting such a threat of 'war', 'warfare', and 'conflict' is through, for example, helping to eliminate 'safe heavens,' in the interconnected and transborder nature of cyberspace – filling the gap where potential loopholes exist for malicious exploitation of cyber vulnerabilities in other states by extending capacity-building assistance – and by establishing CBMs for more enhanced and organized information sharing. Thus, we understood that states see the merit of international cooperation as the mitigation of potential risks for their peace and security, both domestically and internationally, and have placed the importance, which is reflected in the number of NCSSs addressing international cooperation. Nevertheless, both hypotheses are validated given that only 13 countries have expressed their cybersecurity-related actions in case of war and most NCSSs discuss international cooperation.

In terms of the large appearance of the EU as a block and NATO as an organization for international cooperation, it is undiscernible from our analysis whether, for example, the need for these collective efforts to counter a threat of 'war', 'warfare', and 'conflict' in cyberspace is the result of more intensively felt or shared threat in the EU block or among NATO member states with a suggestion of a commonly perceived 'enemy', or whether, simply, it is because more collaborative frameworks exist in the EU or NATO context. Given that it is rather conclusive that states seek international cooperation as countermeasures to the threat of 'war', 'warfare', and 'conflict' in cyberspace, further study could be conducted, in more region or country-specific context, to excavate who is collaborating or seeking to collaborate in which context, which may assist states in refining their cybersecurity strategies.

Lastly, with a minimal number of references to neutrality, more or less confined to internet or technical/technological neutrality, and no mention of law of neutrality in the meaning of IHL in cyberspace, we can validate our first hypothesis and can only conclude that it is an area where decisive positions or views in terms of strategies are not yet prevalent among states, or states are still unwilling to express their positions to the outside world, maintaining a "*persistent policy of silence and ambiguity*" (Efrony and Shany 2018, p.588) that is rather frequent in issues pertaining to the identification of state practice or views in cyberspace. Given the complexity and uncertainty of the concept of neutrality itself in cyberspace, we understand that the overview of the fact of its absence is telling us of the difficulties ahead in terms of strategizing neutrality in cyberspace context both domestically and internationally.

6. Conclusion

This paper presented a global snapshot of the national positions on conflict, neutrality, and cooperation with regards to cybersecurity, of all countries (113) that have publicly released an NCSS. As hypothesized, very few countries (13) reference their cybersecurity-related preparations and preparedness for or during times of war (even though more than half discuss warfare in other general topics), and even less (5) delve into the topic of neutrality. With 111 nations discussing international cooperation, the other side of the hypothesis is similarly proven.

Future research might delve into individual national case studies, or more in-depth bi-/multi-lateral comparative studies of these topics within the cybersecurity context. While outside the scope of this study, during its course, we also discovered the existence of International Cybersecurity Strategies in some countries. It would be worthwhile to study those and compare them to their national counterparts, or between different countries. We also realize that the topic of war would be presented in more detail in (National) Defence Cyber Security Strategies; however great care must be undertaken to separate the national and institutional documents for such future studies.

By the time of this paper is published, some of the more 'outdated' NCSS might have been updated with newer versions. For them, and all new versions that will appear in the coming years, we wish to articulate the need to present a national position on war / conflict and neutrality, given the recent flare-ups between countries, as possible deterrence, CBMs, and communication instruments. This would also mean that it would be also necessary to make NCSSs publicly available. A few countries were not included in this study due to their NCSS not being publicly accessible nor available.

Acknowledgement

This article has been partially supported by the Doctoral School in Economics and Innovation, ASTRA "TTÜ arenguprogramm aastateks 2016-2022", Project code: 2014-2020.4.01.16-0032.

References

Beecroft Nick. (2021) *The UK's Cyber Strategy Is No Longer Just About Security* [Online]. Carnegie Endowment for International Peace, https://carnegieendowment.org/2021/12/17/uk-s-cyber-strategy-is-no-longer-just-about-security-pub-86037.

Caudle Sharon L. (2009) "National Security Strategies: Security from What, for Whom, and by What Means." *Journal of Homeland Security and Emergency Management* 6(1): Article 22.

Cordey Sean and Kohler Kevin. (2021) *The Law of Neutrality in Cyberspace*. ETH Zurich.

Cornish Paul, Lindey-French Julian and Yorke Claire. (2011) *Strategic Communications and National Strategy*. The Royal Institute of International Affairs: Chatham House.

CSIS - Center for Strategic and International Studies. (No date) *Significant Cyber Incidents* [Online]. CSIS, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Daricili Ali B. and Özdal Barış. (2018) "Analysis of the Cyber Security Strategies of People's Republic of China." *The Journal of Security Strategies,* 14(28): 1–35.

Drew Dennis M. and Snow Donald M. (1988) *Making Strategy: An Introduction to National Security Processes and Problems*. Maxwell Air Force Base: Air University

DuMont Malia. (2019) *Elements of national security strategy* [Online]. Atlantic Council, https://www.atlanticcouncil.org/content-series/strategy-consortium/elements-of-national-security-strategy/.

Efrony Dan and Shany Yuval. (2018) "A Rule Book On The Shelf? Tallinn Manual 2.0 On Cyberoperations and subsequent state practice." *The American Journal of International Law* 112(4): 583–657

eGA. (No date) *NCSI – Methodology* [Online]. eGA, https://ncsi.ega.ee/methodology/.

European Union. (2015) *REGULATION (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union*.

Greenwood Christopher. 1987. "The Concept of War in Modern International Law." *International and Comparative Law Quarterly* 36(2): 283–306.

Hurel Louise M. (2020) *Brazil's First National Cybersecurity Strategy: An Analysis of its Past, Present and Future* [Online]. Internet Governance Project, https://www.internetgovernance.org/2020/04/05/brazils-first-national-cybersecurity-strategy-an-analysis-of-its-past-present-and-future/.

Kolini Farzan and Janczewski Lech. (2017) "Clustering and Topic Modelling: A New Approach for Analysis of National Cyber security Strategies." *PACIS 2017 Proceedings* 126.

Lauterpach Hersch. (1952) *Oppenheim's International Law Volume 2, Disputes, War and Neutrality*. 7th edition. Longmans

Libicki Martin C. (2018) *Conquest in Cyberspace: National Security and Information Warfare, Conquest in Cyberspace: National Security and Information Warfare*. Cambridge: Cambridge University Press.

Luiijf Eric, Besseling Kim, and Graaf Patrick de. (2013) "Nineteen national cyber security strategies." *International Journal of Critical Infrastructures* 9(1-2): 3–31.

Merriam-Webster. (No date) *Warfare Definition & Meaning* [Online]. Merriam-Webster, https://www.merriam-webster.com/dictionary/warfare.

Naylor Esther, Painter Christopher and Hakmeh Joyce. (2022) *How does capacity-building make cyberspace better?* [Online]. Chatham House, https://www.chathamhouse.org/2022/02/how-does-capacity-building-make-cyberspace-better.

Newmeyer Kevin P. (2015) "Elements of National Cybersecurity Strategy for Developing Nations." *National Cybersecurity Institute Journal* 1(3): 9–19.

OECD. (2012) *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*. Paris: OECD

Przetacznik Jakub and Tarpova Simona. (2022) *Russia's war on Ukraine: Timeline of cyber-attacks* [Online]. EP, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

Reveron Derek S. (2012) *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington D.C.: Georgetown University Press

Sabillon Regner, Cavaller Victor and Cano Jeimy. (2016) "National Cyber Security Strategies: Global Trends in Cyberspace." *International Journal of Computer Science and Software Engineering* 5(5): 67–81.

Shackelford Scott and Kastelic Andraz. (2014) "Toward a State-Centric Cyber Peace? Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity." *New York University Journal of Legislation and Public Policy*, 2016, Kelley School of Business Research Paper No. 15-4.

Shafqat Narmeen and Masood Ashraf. (2016) "Comparative Analysis of Various National Cyber Security Strategies." *International Journal of Computer Science and Information Security* 14(1): 129–136.

Snyder Hannah. (2019) “Literature review as a research methodology: An overview and guidelines.” *Journal of Business Research* 104: 333–339.

Štitilis Darius, Pakutinskas Paulius and Malinauskaitė Inga. (2017) “EU and NATO cybersecurity strategies and national cyber security strategies: A comparative analysis.” *Security Journal* 30, 1151–1168.

Teoh Chooi S. and Mahmood Ahmad K. (2017) “National cyber security strategies for digital economy.” *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*.

U.N. (No date) *Capacity-Building* [Online]. U.N., https://www.un.org/en/academic-impact/capacity-building.

UNIDIR. No date. *About* [Online]. UNIDIR, https://cyberpolicyportal.org/about.

Von Solms Rossouw and Van Niekerk Johan. (2013) “From information security to cyber security.” *Computers and Security* 38: 97–102.

Yannakogeorgos Panayotis A. and Lowther Adam B. (2016) *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Florida: CRC Press

Wheelen Thomas, Hunger J David, Hoffman Alan N., Bamford Charles. (2017) *Strategic Management and Business Policy: Globalization, Innovation and Sustainability*. Harlow: Pearson Education.

Wu Tim. (2003) “Network Neutrality, Broadband Discrimination.” *Journal on Telecommunication & Hightech Law* 2: 141–175.

Ziolkowski Katharina. (2013) *Confidence Building Measures for Cyberspace – Legal Implications*. Tallinn: NATO CCDCOE.