2. POLITICAL AIMS & POLICY METHODS

Gustav Lindstrom, Eric Luiijf

Section 2: Principal Findings

- There is growing convergence across national security strategies (NSS) with respect to identified threats and challenges (e.g., proliferation of weapons of mass destruction, terrorism, state failure, etc.).
- Most NSS include non-traditional threats, including a cyber security dimension. The cyber dimension is frequently recognised as cross-cutting a variety of critical infrastructure sectors and other sectors important to society (e.g., energy security).
- There are suggestions that political will (and understanding) is still limited when it comes to tackling cyber security risk factors.
- National cyber security strategies (NCSS) are used to provide guidance to policy-makers and other stakeholders regarding cyber security policy priorities and potential resource allocations. They can also form an important part of a nation's declaratory policy.
- Among the principal categories subject to cyber threats as identified in existing NCSS are critical infrastructures, economic prosperity, national security, and societal well-being.
- An examination of 19 NCSS suggests there are diverging understandings of cyberspace. Some equate it closely to the internet while others embrace a broader definition.
- Less than half of the NCSS examined define terms like 'cyber security'.

2.1. INTRODUCTION

Concepts of national and international security have changed considerably since the end of the Cold War. In particular, there has been a noticeable shift from the concept of combating specific threats to reducing and mitigating risk factors to society as a whole. As noted by NATO in its 1991 Strategic Concept:

> 'The primary role of Alliance military forces, to guarantee the security and territorial integrity of member states, remains unchanged. But this role must take account of the new strategic environment, in which a single massive and global threat has given way to diverse and multi-directional risks.'[159]

Starting in the mid-1990s, the notion of 'Comprehensive Security' (originally put forward by the OSCE[160] in 1990) became more prominent. This concept facilitated a broader and deeper interpretation of security needs and requirements, and helped inform the idea of 'enhanced' or 'expanded security' that identified security policy dimensions in other domains such as food, health and the environment.[161] The recognition that security was fundamentally more than the territorial integrity of the state led to an even more radical shift. The Human Security concept (developed mostly under the aegis of the UN)[162] directly questioned the 'state-centric' approach to security, and put the needs of the individual first. The rise of Human Security as a concept had a direct influence on the more 'state-centric' approaches of Comprehensive or Expanded Security as well.[163] On the one hand it helped launch the notion of 'individual' or 'societal' needs, and how national security could be re-conceptualised as being primarily orientated to help meet the satisfaction of these needs through variously defined 'services'. On the other hand, it was increasingly recognised that threats and risks to these societal needs were not easily categorised as being primarily an 'internal' or 'external' security issue.

The need to create a more unified approach to meet a variety of security challenges, coupled with the need to do so with limited resources, was a principal driver for the introduction of national security strategies in the late 1990s and the early 2000s.

2.1.1. Aims of National Security Strategies

The formulation of national security strategies (NSS) is a relatively recent phenomenon. Presently, a majority of countries possessing a national security strategy can trace their initial security strategy to the late 1990s or early 2000s. In the United States, one of the earliest developers of a NSS, initial concepts and

---

159 NATO, *The Alliance's New Strategic Concept* (London: NATO, 1991).

160 OSCE, *The OSCE Concept of Comprehensive and Co-operative Security. An Overview of Major Milestones (SEC/CPC/OS/167/09)* (Vienna: OSCE, 2009).

161 For a discussion on the development of various security concepts in Europe and the Mediterranean Area, as well as the role of NATO, see: Hans G. Brauch et al., *Security and Environment in the Mediterranean: Conceptualising Security and Environmental Conflicts*(Berlin et al.: Springer Verlag, 2003).

162 UNDP, Human Development Report 1994. New Dimensions of Human Security, (Oxford and New York: Oxford University Press, 1994), http://hdr.undp.org/en/reports/global/hdr1994.

163 For a discussion on the development of expanded security and Comprehensive Security concepts during the early 1990s, see Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (Cambridge: Cambridge University Press, 2009). 136-37.

policy statements were already formulated in the late 1940s.[164] A facilitating factor was the signing of the 1947 National Security Act which, among others, set up the National Security Council. In 1986, through the Goldwater-Nichols Department of Defense Reorganization Act, the US made the formulation of a NSS a requirement.

Outside of the United States, the introduction of NSS has been a fairly recent development. Establishing a NSS has substantial appeal because it encourages policy-makers to identify strategic objectives ('ends'), to pinpoint the resources available to reach those objectives ('means'), and to provide a guide on how such resources are to be applied to reach stated objectives ('ways'). Ideally, a NSS contains strategic objectives that are consistent with national values and interests. As an overarching strategic document, a NSS often includes political, internal security, foreign policy, defence structures and economic dimensions.

A well-formulated NSS should do at least three things. Firstly, it should enable government departments and ministries to translate a government's national security vision into coherent and implementable policies. It should also facilitate the production of 'sub-strategies' across different domain areas that are consistent with the overarching NSS (e.g., a strategy for combating terrorism). Since most NSS highlight resources needed to achieve national security objectives, they should likewise provide guidance on R&D in new security capabilities, future procurements, investments, and budget decisions. Ultimately, a NSS is the 'peak' national security document for a government, sited at the apex of a whole set of different policy documents that – ultimately – should refer back and get their guidance from the NSS.[165]

Secondly, a NSS should clarify how the state might act in international affairs – enabling a more proactive rather than reactive foreign policy. To illustrate, a NSS could be helpful in determining what elements of national power (e.g., diplomatic, information, military, economic) are most likely to be employed to reach specific international objectives. Besides informing international policy making, a NSS should serve to communicate strategic thinking to other states and the international community at large.

---

164 See, for instance, US National Security Council, *NSC 68: United States Objectives and Programs for National Security* (Washington, DC: FAS, 1950). This document was declassified in 1975. As a *de facto* NSS, NSC 68 shaped US foreign policy substantially during the Cold War era.

165 Although the hierarchies can be relatively difficult to establish, one example of such a document progression would be from the UK: The UK Cabinet Office, *The National Security Strategy of the United Kingdom. Security in an interdependent world.* informed the UK Cabinet Office, *Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space.*, which, in turn, provided the frame for the UK Home Office, *Cyber Crime Strategy* (Norwich: The Stationery Office, 2010).

Thirdly, a NSS should not exist in a strategic vacuum. On the contrary, it should be linked to existing national and international strategies to the extent that it is feasible to encourage a harmonised set of policies that are shared with likeminded partners. The linking of a NSS with other strategies may also be helpful to promote coordination, cooperation and collaboration. At the international level, it may also serve to facilitate a Whole of System approach (examined in greater detail in Section 3).

A NSS usually contains both explicit and implicit elements. Most current documents tend to be fairly explicit with respect to perceived threats and challenges, even if the understanding of the term 'national security' may differ from country to country or evolve over time. While strategies typically outline threats and challenges, they may be less forthcoming on which threats are of greatest concern. Likewise, strategies are usually less explicit when it comes to how the government may address identified threats and challenges, including resources that may be necessary or questions about which departments should take the lead in response.[166] This is not altogether surprising since a NSS usually serves to provide strategic guidance to government ministries and agencies. Ambiguity concerning policy responses may also be useful to discourage potential adversaries from engaging in certain behaviours or actions.

2.1.2. Trends in National Security Strategy Formulation

An examination of current national security strategies suggests four trends. First, there seems to be a growing convergence among policy-makers with respect to the key threats and challenges facing states. As shown in Table 4, examples of oft-cited threats and challenges include the proliferation of weapons of mass destruction, terrorism, state failure, and organised crime, besides, of course, cyber security threats.

There may be several explanations for this trend. For example, convergence with respect to threats and challenges across countries' NSS may arise when policy-makers are formulating a NSS to analyse existing strategies and use elements of those strategies as a basis for their own strategic reflection. Another factor may be the global impact of events such as terrorist attacks (the 9/11 attacks in New York and Washington D.C., the Madrid train bombings in March 2004, and the London transport attacks in July 2007, etc.) that have led policy-makers to converge on a shared set of security threats and challenges.

---

166 Catherine Dale, National Security Strategy: Legislative Mandates, Execution to Date, and Considerations for Congress, (Washington, DC: Congressional Research Service, 2008), http://fpc.state.gov/documents/organization/106170.pdf.

Table 4: Comparison of Threats and Vulnerabilities: Select NATO Member States Security Strategies/White Books

Country	Document type	Year	Examples of Threats / Vulnerabilities
France	White Book	2008	'Weapons of Mass Destruction' (WMD); terrorism; ballistic missile proliferation; cyber attacks; espionage; criminal networks; health risks; citizens abroad in vulnerable areas
Germany	White Book	2006	International terrorism; proliferation and military build-up; regional conflicts; illegal arms trade; fragile statehood; transportation routes; energy security; uncontrolled migration; epidemics and pandemics
Hungary	Security Strategy	2012	Terrorism; proliferation of WMD; unstable regions/failed states; illegal migration; economic instability; challenges to information society; global natural, man-made and medical sources of danger; regional challenges; internal challenges
Netherland	Security Strategy	2007	Breaches of international peace and security; 'chemical, biological, radiological, and nuclear' (CBRN); terrorism; international organised crime; social vulnerability; digital lack of security; economic lack of security; climate change and natural disasters; infectious diseases and animal diseases
Poland	Security Strategy	2007	Organised international terrorism; organised international crime; energy security; illegal migration; weakened transatlantic links; frozen and regional conflicts; weak levels of integration of economic life and financial markets; environmental threats; internal challenges (e.g., population changes, infrastructure, energy storage)
Spain	Security Strategy	2011	Armed conflicts; terrorism; organised crime; financial and economic insecurity; energy vulnerability; proliferation of weapons of mass destruction; cyber threats; uncontrolled migratory flows; emergencies and disasters; critical infrastructures; supplies and services
United Kingdom	Security Strategy	2010	International terrorism; hostile attacks upon UK cyberspace; major accident or natural hazards; an attack on the UK or its overseas territories; risk of major instability; organised crime; severe disruption to satellite communications; disruption to oil or gas supplies; short to medium term disruption to international supplies of essential resources
United States	Security Strategy	2010	WMD; space and cyberspace vulnerabilities; energy dependence; climate change; pandemic disease; failing states; global criminal networks

A related development explicit in some NSS (e.g., the United States and the United Kingdom) is the recognition that a diverse set of threats and challenges requires an integrated all-hazards risk management approach.[167] Taking a broader perspective, policy-makers and analysts embracing this concept are more inclined to examine national vulnerabilities, gauge the possible consequences of a threat, and seek innovative ways to protect society as a whole. Reinforcing the trend towards risk management is the realisation that national means are not unlimited, requiring a more careful analysis of where and how finite means should be employed.

The shift to a national risk management paradigm is visible in those NSS that highlight the need to enhance national resilience or underscore the importance of incorporating an 'all-hazards' approach. While the overarching goal of achieving comprehensive security remains (and some might argue is promoted), this development acknowledges that achieving a 100% protection level is neither feasible not realistic. Thus the need to identify new defensive and mitigating measures to provide security.

A second trend, related to the first point, is that national security strategies are identifying 'new' threats and challenges. As noted earlier, a broader understanding of the term 'security' is likely contributing to this trend.[168] Table 4 provides some illustrations such as climate change, energy supply, health risk, and cyber security. The inclusion of these challenges is often accompanied by the recognition of their complexity and far-reaching implications. The case of climate change, for instance, is considered a long-term challenge whose impact may not be felt for several decades. However, addressing it requires action today, preferably in a collective manner at the international level. Complicating these efforts is the perception that the effects of climate change may be more severe on some parts of the world than in others, leading to more disparate cooperation. With respect to cyber security, it is frequently included in new NSS as a 'new' threat. Its inclusion or perceived importance, however, does not necessarily translate to increased awareness at the senior policy level of the scope of the challenge. While there is no authoritative international survey of government decision-makers and senior policy-makers with respect to their perception of the cyber security challenge, there are suggestions that political will is still limited when it comes to tackling cyber security risk factors. For example, while policy-makers agree that international cooperation is necessary

---

167 According to the Department of Homeland Security Risk Lexicon, defined as the 'incorporation and coordination of strategy, capability, and governance to enable risk-informed decision making (see US Department of Homeland Security, DHS Risk Lexicon, (Washington, DC: Risk Steering Committee, 2008), http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf. 19.).

168 A school of academic thought (the Copenhagen School) has forwarded the concept of 'securitisation' to reflect the tendency of a broader understanding of the concept of security. For more, see Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security. A New Framework For Analysis* (London: Lynne Rienner Publishers, Inc., 1998).

to mitigate cyber challenges, a 2010 survey of policy-makers, specialists, business executives, community leaders and journalists carried out by the EastWest Institute indicates that little is being done: 'Track 1 diplomacy on worldwide cybersecurity cooperation is not working well on the tactical level and practically non-existent on the strategic level.'[169] Underscoring the importance of political will, 36% of those surveyed saw political/policy as the key ingredient to address principal cyber challenges, followed by 27% identifying technical solutions, 16% listing business and legal measures (for each), with the remaining 5% singling out legal means.[170]

It is important to note that decision-makers' and policy-makers' perceptions can change quickly. This was most visible in the aftermath of the distributed denial of service (DDoS) attacks on Estonia in April/May 2007, after which cyber security issues increasingly entered the political agenda. The release of national cyber security strategies (many of which came out in 2009-2011) also point in the direction of a greater acknowledgement of the relevance of cyber security. A 2012 report by McAfee and the Brussels based Security & Defence Agenda[171] that surveyed policy-makers in several countries found that 45% of respondents believe cyber security is as important as border security.[172]

A third trend with respect to the formulation of a NSS is a greater awareness of the link between internal and external security. In the aftermath of 9/11 and coupled with the identification of new threats such as pandemics, it became increasingly evident that internal and external security should be considered more in tandem, especially as risk factors and challenges from the outside do not necessarily stop at external borders. The reverse may be true as well. For example, a set of cartoons in a local newspaper in Denmark led, over time, to major internal security events in several other nations external to Denmark. It included, for instance, arson attacks on a Danish embassy and people rioting in other nations.

A stronger, more dynamic link between internal and external security in existing NSS has wide-ranging implications for policy-makers. Among others, it highlights the need for greater cooperation across government departments, especially those that deal with internal security (interior and justice) and those that handle external security (foreign affairs and defence). It also requires policy-makers to

---

169 EastWest Institute, International Pathways to Cybersecurity. Report of Consultation, (Brussels: EastWest Institute, 2010), http://www.ewi.info/system/files/CyberSummaryReport.pdf. 1.

170 Ibid., 3.

171 Brigid Grauman, Cyber-security: The vexed question of global rules. An independent report on cyber-preparedness around the world, (Brussels: Geert Cami, 2012), http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf.

172 Specifically, the survey included in-depth interviews with 80 policy-makers, cyber security experts in government, business and academia in 27 countries. Also surveyed were 250 'world leaders' in 35 countries. For more information, see ibid.

think carefully about how resources might be allocated to satisfy internal and external security objectives. For some, a stronger connection between internal and external security may translate into a more active foreign policy ('best defence is a good offence'). Others may perceive the need to strengthen internal security and resilience to better withstand external security challenges. For all these reasons, the establishment of a NSS is increasingly becoming an interagency project that can provide a holistic vision for national security.

A fourth point is that, while most NSS traditionally include a security, political and economic dimension, present-day NSS go a step further by clearly recognising the need to combine traditional security policies, development cooperation policies, and economic tools at large to promote security and development. The combination of civilian and military assets is also encompassed in new concepts such as civil-military coordination (CMCO) and the 'Comprehensive Approach'.[173]

This trend underscores the dynamic and changing nature of NSS. It also points to a greater recognition that a combination of different tools is required to address 21st century threats and challenges. To a certain degree, this development is not surprising given the inclusion of both traditional and non-traditional security threats in NSS. Over time, capturing the complexity of the international security landscape is likely to strengthen the role of having a NSS as a strategic platform to derive follow on strategies and policies.

2.1.3. Integrating Cyber Security in National Security Strategies

As noted in Section 1, several NSS include a cyber security dimension. The references made to the cyber domain can take several forms. A majority of the NSS identify cyber threats as a new security challenge that policy-makers should be aware of. Many also highlight that the cyber domain can impact other sectors or domains, e.g., energy, health and environment. As a cross-sector issue, it is important to discern both the enabling characteristics of cyber across different domains as well as potential risk factors.

Some strategies go a step further by identifying a particular cyber security dimension that is of concern. An example that is visible in some strategies is the need to protect 'critical infrastructures' (CI) – i.e., those utilities and services that are necessary to maintain societal needs, such as electric power, communications, but also banking. Countries such as France and the UK integrate a cyber dimension

[173] Some analysts also like to include concepts such as 'Civil-Military Cooperation' (CIMIC) which focuses on how deployed military elements best interact with civilian counterparts to achieve desired effects.

more extensively into their overall security planning, for example by providing details on major cyber attacks and their application for espionage (France)[174] as well as the benefits cyberspace offers to industry, government and the general population (UK).[175] The UK NSS also notes that cyber attacks are considered among the four high priority risk factors over the next five years. In the case of the Spanish NSS, an entire section is dedicated to cyber threats which also describe specific lines of action that can be considered in response to a cyber threat.[176]

As noted earlier, in the aftermath of the distributed denial of service attack on Estonia in April 2007, the cyber dimension took on a more prominent role. The media coverage of specific supposed state-sponsored malicious software (such as Stuxnet, Duqu and Flame) and cyber espionage attacks on various nations and international organisations is likely to further attune countries to the importance of cyber security, especially with respect to critical information infrastructure protection (CIIP).[177] Looking ahead, the cyber security dimension will increasingly be covered in stand-alone NCS strategies.

The overall trend can be summarised as follows: most recent NSS documents acknowledge the need to address cyber security, and give this issue the highest priority compared with other risks. Sometimes, as in the United States NSS of 2010, they will deal with cyber security both as its own discrete element, but also as a horizontal issue that crosses a number of other NSS goals.[178] In nearly all cases there will be subsequent and subordinate documents that deal specifically with the threat to national cyber security and, subordinate to that, specific documents addressing specific cyber threats, such as within a military or law enforcement environment.

---

174 French Secretariat-General for National Defence and Security, *Information systems defence and security. France's strategy.*

175 UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.*

176 Spanish Government, *Spanish Security Strategy. Everyone's responsibility* (Madrid Spanish Government, 2011). 60-4.

177 Sometimes abbreviated as CI(I)P. Some countries use CIIP as a clear sub-category to overall CIP; while other countries equate CIIP to NCS.

178 Within the US NSS 2010, one specific goal is mentioned: 'Secure Cyberspace'. However, 'cyber' is mentioned at least as often among other NSS goals as within the specific 'Secure Cyberspace' goal (see White House, *National Security Strategy*.).

2.2. THE NATIONAL CYBER SECURITY DIMENSION

2.2.1. Themes in National Cyber Security Strategies

To date, over 20 states have released a national cyber security strategy (NCSS) or national information security strategy, many of them unveiling one in 2011.[179] With respect to NATO members, nearly half have produced a NCSS that details national visions, guiding principles, perceptions of the threat, and strategic objectives.[180]

Table 5: Examples of National Cyber Security Strategies

Nation	Issued	Lead Agency	English version	Other languages
Australia	Nov 2009	Attorney-General	Cyber Security Strategy[181]	-
Canada	Oct 2009	Public Safety Canada	Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada[182]	French
Czech Republic	Jul 2011	Ministry of Interior	Cyber Security Strategy of the Czech Republic for the Period 2011-2015[183]	Czech
Estonia	Sep 2008	Ministry of Defence	Cyber Security Strategy[184]	Estonian
France	Feb 2011	General Secretariat for Defence and National Security	Information systems defence and security. France's Strategy[185]	French

179 Among these are Australia, Canada, the Czech Republic, Estonia, France, Germany, India, Japan, Lithuania, Luxembourg, the Netherlands, New Zealand, Romania, Slovakia, South Africa, South Korea, Spain, Switzerland, Uganda, the United Kingdom and the United States. Countries in the process of finalising their NCSS include Austria, Finland and Turkey.

180 For an overview of these see Eric Luiijf, Kim Besseling, and Patrick De Graaf, 'Nineteen National Cyber Security Strategies,' *International Journal of Critical Infrastructures* (forthcoming).

181 Australian Attorney-General's Department, *Cyber Security Strategy.*

182 Canadian Department for Public Safety, *Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada.*

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

184 Estonian Ministry of Defence, *Cyber Security Strategy* (Tallinn: Estonian Ministry of Defence, 2008).

185 French Secretariat-General for National Defence and Security, *Information systems defence and security. France's strategy.*

Nation	Issued	Lead Agency	English version	Other languages
Germany	Feb 2011	Federal Ministry of the Interior	Cyber Security Strategy for Germany[186]	German
India	Apr 2011	Ministry of Communications and Information Technology	Discussion Draft on National Cyber Security Policy[187]	-
Japan	May 2010	Information Security Policy Council	Information Security Strategy for Protecting the Nation[188]	Japanese
Lithuania	Jun 2011	Government of the Republic of Lithuania	Programme for the Development of Electronic Information Society (Cyber-Security) for 2011-2019[189]	Lithuanian
Luxembourg	Nov 2011	Government of the Grand Duchy of Luxembourg	Not available online	French[190]
Netherlands	Feb 2011	Ministry of Security and Justice	The National Cyber Security Strategy (NCSS). Strength through Cooperation[191]	Dutch
New Zealand	Jun 2011	Ministry of Economic Development	New Zealand's Cyber Security Strategy[192]	-
Romania	May 2011	Ministry of Communications and Information Society	Not available online	Romanian[193]

186 German Federal Ministry of the Interior, *Cyber Security Strategy for Germany.*

187 Indian Ministry of Communications and Information Technology, *Discussion Draft on National Cyber Security Policy (New Delhi: Government of India, 2011).*

188 Japanese Information Security Policy Council, *Information Security Strategy for Protecting the Nation (Tokyo: National Information Security Center, 2010).*

189 Lithuanian Government, Re*solution NO 796 on the Approval of the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019* (Vilnius: Information Technology and Communications Department, 2011).

190 Luxembourg Government, *Stratégie nationale en matière de cyber sécurité (*Luxembourg: Government of the Grand Duchy of Luxembourg, 2011).

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

192 New Zealand Ministry of Economic Development, *New Zealand's Cyber Security Strategy* (Wellington: New Zealand Ministry of Economic Development, 2011).

193 Ministry of Communications and Information Society, *Strategia de securitate cibernetica a României* (Bucharest: Ministry of Communications and Information Society, 2011).

Nation	Issued	Lead Agency	English version	Other languages
Slovakia	2008	Ministry of Finance	Slovak National Strategy for Information Security[194]	Slovakian
South Africa	Feb 2010 approved Mar 2012	Department of State Security	Notice of Intention to Make South African National Cybersecurity Policy[195]	-
South Korea	Aug 2011	Korea Communications Commission	-	Korean[196]
Spain	May 2011	Spanish Government	Part of Spanish Security Strategy: Everyone's responsibility[197]	Spanish
Switzerland	Jun 2012	Federal Department of Defence, Civil Protection and Sport	National Strategy for Protection of Switzerland against Cyber Risks[198]	German;[199] French
Uganda	Nov 2011	Ministry of Information and Communication Technology	National Information Security Strategy[200]	-
United Kingdom	Nov 2011	Cabinet Office	The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world[201]	-
United States	Feb 2003	White House	The National Strategy to Secure Cyberspace[202] (also CNCI, HSPD-7, 60 day Review)	-

194 Referenced by: http://www.webcastlive.es/4enise/archivos/T14/T14_Daniel_Olejar_CominiusUniversity.pdf.

195 South Africa Department of Communications, *Notice of Intention to Make South African National Cybersecurity Policy (Draft approved 11 March 2012)* (Pretoria: South Africa Government, 2010).

196 Not available online.

197 Spanish Government, *Spanish Security Strategy. Everyone's responsibility.*

198 Publication expected second half of 2012.

199 Swiss Federal Department of Defence, Civil Protection, and Sports, *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken* (Bern: Swiss Confederation, 2012).

200 Uganda Ministry of Information and Communications Technology, N*ational Information Security Strategy (NISS Final Draft)* (Kampala: Uganda Ministry of Information and Communications Technology, 2011).

201 UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.*

202 White House, *The National Strategy to Secure Cyberspace.*

The analysis of 19 NCSS by Luiijf et al. shows that several key themes and visions are highlighted across those strategies. Among the most recurrent are:

- Maintaining a secure, resilient, and trusted electronic operating environment,
- Promoting economic and social prosperity/promoting trust and enable business and economic growth,
- Overcoming the risk of information and communications technologies, and
- Strengthening the resilience of infrastructures.

The visions are translated into strategic objectives which are broken down further into a wide variety of priorities. With respect to the vision of maintaining a secure cyberspace, some countries express the need to raise awareness of the cyber risk, secure government systems, adopt an appropriate regulatory framework, modernise the legal framework, tackle cyber crime, or reinforce critical infrastructures. These and related objectives are also thought to contribute to economic prosperity by promoting trust and resilience.

There are differences in how states translate their visions into strategic objectives. A principal explanatory factor behind this may be countries' diverging understanding of cyberspace. Some countries take a broad view of cyberspace that includes infrastructures (such as control systems in critical infrastructures) and others take a much narrower view of cyberspace, equating it more closely to the internet. To illustrate, the United States is at one end of the spectrum with a broad definition of cyberspace, even implicitly acknowledging the importance of social networks.[203] In the Dutch NCSS, cyberspace is likewise defined broadly, including chip cards and in-car systems.[204] On the other side of the spectrum, countries like Australia, Canada, Germany, New Zealand and Spain place an emphasis on the internet and internet connected information technologies (additional details are provided in Section 2.3.1).

Beyond diverging perceptions of key concepts such as cyberspace, existing NCSS tend to have varying views on cyber threats. Among the principal cyber threat categories identified in existing NCSS are threats to:

- Critical infrastructures,
- Economic prosperity,
- National security,

---

[203] See Section 1.

[204] Luiijf, Besseling, and Graaf, 'Nineteen National Cyber Security Strategies.'

- Societal well-being,
- Public confidence in information and communication technologies,
- Economic prosperity, and
- Globalisation.

While some of these categories are acknowledged in all or most NCSS (e.g., cyber threats to critical infrastructures) some categories – such as threats to globalisation or societal well-being – are described explicitly or implicitly in few strategies.[205]

Existing NCSS also identify the sources of cyber threats. Among the principal dimensions identified are cyber threats via large-scale attacks, terrorists, foreign nations, espionage, organised crime, or political activism against ICT-based services. Some threat categories – such as cyber threats from organised crime – are highlighted in most NCSS. Other dimensions, such as threats from activists or extremists, figure in a couple of NCSS. The four categories referenced most frequently across the examined NCSS were organised crime, cyber threats from foreign nations (cyber war), cyber threats associated with terrorists, and espionage.[206]

Overall, roughly half of the NCSS examined demonstrate a direct link with the states' NSS. Most often, this takes the form of a reference to the NSS' identification of cyber as a potential security challenge or an acknowledgement of security objectives outlined in the NSS. It is, however, more difficult to gauge the different NCSS' relationship with other strategies and policies of importance. It is expected that such linkages become more reinforced over time. Factors that might expedite such a process range from refining the definitions of key concepts used in NCSS to strengthening the potential for public-private cooperation in the cyber domain.

An issue for future consideration is how existing NCSS can cope with rapidly changing threat dynamics. In other words, with no formal review mechanism in place, many NCSS may become irrelevant or unable to provide guidance when facing a new type of cyber challenge. Only a few countries have released more than one NCSS.[207] For example in the United States, several NCSS-type documents have been released.[208] In light of this limitation, it is interesting to note that some

---

205 Ibid.

206 Ibid.

207 Japan, for instance, has released a second version of a NCSS, but it mainly represents a refinement of the initial strategy. The UK revised its 2009 NCSS after a political signature change.

208 For a complete overview, see Rita Tehan, Cybersecurity: Authoritative Reports and Resources, (Washington, DC: Congressional Research Service, 2012), http://www.fas.org/sgp/crs/misc/R42507.pdf.

countries such as Germany and Japan indicate in their NCSS that there is a risk of a mismatch between technology development and security policy.[209]

2.2.2. Aims and Addressees

Consistent with other sub-strategies developed in support of a NSS, a NCSS aims to provide guidance to policy-makers regarding cyber policy priorities and potential resource allocations. However, these NCSS can also have other roles as well: they can play an active role in shaping the international image of a nation, and indicate where it thinks future collaboration would be possible. Within this context, a NCSS is a vital document for international partners to discern what the actual administrative responsibilities and whom the likely interlocutors are. A NCSS – or, indeed, a subordinate document focusing on the international cyber issues[210] – is a prerequisite to be actively able to engage with a nation's friends and allies on the issue.

In addition, a NCSS can form an important part of a nation's declaratory policy – indicating to potential adversaries where red lines may be drawn before retaliation can be expected, and what capabilities exist, or are being developed, to execute this type of policy. For instance, the United States has repeatedly warned that it would consider a serious cyber attack an 'act of war'.[211] The Russian Information Security Doctrine of 2000 makes it clear that 'an information attack' is not confined to cyber attack, but indeed can mean any kind of severe criticism of the Russian government.[212]

There are also less obvious components of a NCSS that are often intended purely for specialist observers. While these often depend on interpretation, they can be among the most significant. For example, one recent NCSS implied that a particular state had achieved a breakthrough in signal intelligence decryption technology, which facilitated real time cyber attribution. Although this statement is open to interpretation, if accurate, it would have significant implications for the entire nature of inter-state cyber conflict. In a related vein, many NCSS and associated documents are used to specify declaratory policy on cyber retaliation.[213]

---

209 Ibid.

210 One such example is: White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World.*

211 Most recently in the US DoD Cyber Strategy, commented on in the Wall Street Journal (see Siobhan Gorman and Julian E. Barnes, 'Cyber Combat: Act of War,' *The Wall Street Journal*, 30 May 2011.).

212 See, for instance, Alexander Klimburg, 'Mobilising Cyber Power,' *Survival* 53, no. 1 (2011): 41-60.

213 For some further notes on this, see Jason Healey, 'Bringing a Gun to a Knife Fight: US Declaratory Policy and Striking Back in Cyber Conflict,' *Atlantic Council Issue Brief*, September 2011.

With respect to cyber threats, vulnerabilities and measures, existing NCSS target a number of stakeholders. Principal among them, in terms of explicit mention in different NCSS, are government/national security officials, critical infrastructure operators, and citizens. Given the important link between the public and private sectors *vis-à-vis* cyber security, other stakeholders addressed in NCSS tend to be large organisations and small- and medium-sized enterprises. Both are mentioned explicitly in the NCSS by 11 out of the 19 nations examined by Luiijf et al.[214] A final stakeholder category, the Internet Service Providers, is acknowledged in one third of existing NCSS, perhaps somewhat surprising given their potential role in addressing cyber threats and vulnerabilities.

2.3. IMPLEMENTING CYBER SECURITY STRATEGIES

2.3.1. The Use of Terms

One of the findings by Luiijf et al.,[215] in studying 19 NCSS is that less than half of the nations explicitly define terms such as 'cyber security' in their NCSS. Some of the other nations explain cyber security in a descriptive text. One third of the nations, however, discuss cyber security without defining the term at all. The European Network and Information Security Agency (ENISA) observed the same lack of definitions, and presents recommendations to remediate that in the Member States of the European Union.[216]

Early in 2011, the Russian-US bilateral working group of the East West Institute (EWI) and Moscow University drafted an international cyber terminology framework. They defined cyber security as 'a property of cyberspace that is an ability to resist intentional and unintentional threats and respond and recover'.[217] The term 'cyber crime' is defined by only three of 19 NCSS studied by Luiijf et al., neither does the Convention on Cybercrime, ratified by many nations, define it.[218] It would appear that only Romania defines all cyber-related terms in its NCSS.

---

214 Luiijf, Besseling and Graaf, 'Nineteen National Cyber Security Strategies.'

215 Ibid.

216 ENISA, National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace, (Heraklion: ENISA, 2012), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport. 12-3.

217 EastWest Institute and Moscow State University, Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations, (Brussels and Moscow: EastWest Institute and Moscow State University, 2011). 31.

218 Council of Europe, *Convention on Cybercrime (ETS No. 185).*

In general, a national strategy may have different objectives: (1) to align the Whole of Government, (2) to coherently focus and coordinate public and private planning, and to convey the envisioned roles, responsibilities and relationships between all stakeholders, and (3) to convey one's national intent to other nations and stakeholders.[219] Examples of (3) are power projection and posing the national strategy as intent to become the lead nation or global player in the specific domain, or in global cyber security in the case of a NCSS.

The lack of properly defined cyber-related terms can lead to a significant level of confusion within one's own country. Moreover, as the cyber threat is global, proper definitions assist in understanding the cyber security approach of other nations, alliances, and international organisations and vice versa. For that reason, a NCSS without a properly defined, and, if possible, internationally harmonised cyber terminology framework, fails to meet any of the three objectives. The best approach is, therefore, to align one's national definition to the harmonised understanding of other nations.

2.3.2. The Role of Transparency

Depending on the political objective behind the NCSS, the NCSS may be largely strategic, or may include a list of operational and even tactical objectives to be accomplished.[220] To date, many of the strategies that have included a specific task listing have assigned a classified status to most of the document – this, for instance, was originally the case in the UK and the US examples. As far as relatively detailed NCSS are concerned, only the Netherlands' NCSS provides a fairly detailed, unredacted view of the activities proposed. Sometimes specifics are released after a short period of time: the US Comprehensive National Cybersecurity Initiative (CNCI) featured a list of 18 initiatives initially and only 12 of those have been made public.[221]

Transparency within cyber security, however, means more than listing the goals of the strategy. In an optimal case it would disclose the process behind a strategy, allowing outside observers to take stock of the individual steps involved, and potentially remove any doubt about the specifically stated aims within the strategy.

Another form of transparency is to make the NCSS online and available to one's own population and globally by providing an English-language version. As Table 5

---

219 Luiijf, Besseling, and Graaf, 'Nineteen National Cyber Security Strategies,' 2.

220 Ibid., 15.

221 See White House, *The Comprehensive National Cybersecurity Initiative (as codified in NSPD-54/HSPD-23).*

shows, most nations except Slovakia and South Korea provide an online version of their NCSS. Luxembourg and Romania do not provide an English translation.

2.3.3. Addressing Stakeholders

Nations use different structuring, types of wording, and layouts in their NCSS depending on the intended audience. Accessibility, therefore, ranges from large blocks of text for the purpose of aligning the Whole of Government, to a layout with photos and explanatory call out boxes to make the NCSS accessible for the general public, SMEs (Small and Medium Size Enterprises) and other businesses. Also, the historical, cultural, legal, organisational and political structure of a nation can lend to significant differences in working with stakeholders, ranging from a cooperative approach, public-private partnership, to mandatory legislation and regulation. Therefore, it is not just a simple copy and paste of policies, organisational structures, procedures and processes. A transposition to one's own national frameworks is required.[222]

Internal stakeholders such as critical infrastructure operators are often addressed through specific (traditional stovepiped) legislation and regulation mechanisms of bodies like the European Union, and specific regulators/regulatory commissions in various countries. Most liberal-democratic nations depend upon varying degrees of a stick-and-carrot approach where, through public-private partnerships, the private sector is allowed to regulate its own security posture as long as the public sector perceives there to be a good overall cyber governance structure. If the private sector fails to accomplish this on its own, the government steps in and tightens its cyber security legislative and regulatory frameworks.

An important factor in encouraging the private sector is the overall level of cyber security literacy and awareness. The importance of this issue is explicitly recognised by most NCSS. However, NCSS often have difficulty addressing the amorphous groups concerned and mostly simply state that organisations and individual citizens are responsible for a proper level of cyber security without going into detail. More significantly, there is often no particular government stovepipe that is responsible for following-up with detailed sub-strategy on this issue. Either the issue is treated only within CIP programmes and therefore not communicated to the public at large, or it is done on a mass scale, usually missing the more specialised audience in the critical infrastructure entirely. Therefore, the coherent spreading of cyber security awareness – probably one of the most significant factors influencing a

---

222 Marieke Klaver, Eric Luiijf, and Albert Nieuwenhuijs, The RECIPE Project: Good Practices Manual for CIP Policies. For Policy Makers in Europe, (Brussels: European Commission, 2011), http://www.tno.nl/recipereport. 10-1.

nation's overall level of cyber security – is often a lost agenda, abandoned between governmental stovepipes.

Companies involved in aspects particularly related to national cyber security – in particular ICT hardware and software companies – usually play particularly close attention to NCSS, sometimes also seeking to be involved in the drafting process itself. This can be helpful in appraising policy-makers of the actual technological state as seen from an industry perspective, and also serves the purposes of adjusting possible budgetary guidelines for major future projects. When the NCSS is directly connected to the national CIP programme this can indeed be vital step of the process. However, it is notable that very few governments make cyber software and hardware manufacturers, as well as ICT service providers, responsible for cyber security deficiencies in their products and services. Simultaneously, in more advanced nations, the cyber threat emanating from suspect hardware and software products (usually referred to as the need for 'ensuring security to the ICT supply chain') is increasingly becoming the focus of government action. What is often missing is a considered understanding of how the global internet hardware and software infrastructure, as well as the underlying operating principles such as packet routing, directly influences a nation's NCSS. As the vital components (both hardware and software) are often not only outside of the particular country's jurisdiction but (e.g., in the case of software protocols) outside *any* jurisdiction, most NCSS have few perspectives on how to engage on this issue.[223]

When it comes to communicating a 'national intent' to other countries, governments are on more familiar ground. Besides the exact language used in a NCSS, as well as the individual classification or release requirements that effectively 'set the scene', governments will of course initiate individual international actions or initiatives that underline some of messages communicated in the strategy. Within diplomatic fora, the possibilities for multi-tracked diplomacy[224] are considerable, and indeed the need to engage widely may present a challenge to traditionally-conceived foreign ministries or similar. Track 2 and Track 1.5[225] discussions are increasingly critical in building transparency between nations and increasing mutual understanding. They fulfil a real operational function – bringing senior government officials in touch not only with other government officials, but with the non-state actors that actually build and run most of what is considered cyberspace. Communicating with

---

223 For a more detailed discussion of this issue, see Section 3.

224 There are numerous definitions associated with the term 'multi-tracked diplomacy'. However, the most common and basic differentiations are between 'formal' diplomacy by diplomats (Track 1), 'informal' diplomacy by academics, experts and others (Track 2), and 'quasi-formal' diplomacy by a combination of the two actors (Track 1.5).

225 One particular Track 1.5 series of talks between China and the United States has been ongoing since 2006.

these international (or transnational) non-state actors is an activity that virtually no NCSS has yet managed to accomplish effectively.

2.4. POLITICAL PITFALLS, FRICTIONS AND LESSONS IDENTIFIED

There are a number of political pitfalls and frictions that policy-makers should be aware of when formulating a NSS or NCSS. In no particular order, these are:

Adopt a 'one size fits all' strategy: when formulating a NSS or NCSS, policy-makers may be tempted to consult other countries' existing strategies. While this may be helpful to gauge possible strategy formats and identify national interests, policy-makers should be cautious not to leverage content that is inconsistent with national requirements. To illustrate, transplanting security threats that appear in other strategies but are not germane to the country formulating the strategy may do more harm than good by diverting national resources. If there is a desire to have consistency with the strategies of neighbours and/or allies, policy-makers can mitigate the 'one size fits all' risk by prioritising perceived threats or identified policy responses. The UK, for example, prioritises its perceived security threats, identifying international terrorism, cyber attacks, international military crises, and major accidents or natural hazards as 'the four highest priority risks' over the next five years.[226]

Neglect links with other national / international strategies: to strengthen the relevance of a NSS (or NCSS), it should be consistent with existing and forthcoming stand-alone sub-strategies, especially those that provide greater detail on how a certain threat or challenge will be managed (e.g., a counter-terrorism strategy). Such consistency also makes it easier to identify which resources may be necessary to achieve the strategic objectives listed in a NSS. As shown in this section, establishing links across a NSS and a stand-alone sub-strategy is not always straightforward; about half the NCSS examined did not have a direct link with their states' NSS.

Lack of an update/review mechanism: some countries, such as the United States, have laws or other mechanisms in place to review or update existing NSS and other documents of a strategic nature. For countries that do not have such mechanisms, the formulation of a NSS or NCSS may become a one-time exercise, dependent on political will to be updated and remain valid. Thus, such strategies run a substantial risk of becoming irrelevant with the passage of time. This may be of particular concern to strategies where technological developments can quickly outdate

[226] UK Cabinet Office, *The National Security Strategy: A Strong Britain in an Age of Uncertainty*: 11.

portions of the strategy. To illustrate, the implications of recent developments such as cloud computing and 3D (three dimensional) printing may not be fully captured in NCSS released around 2008.

Lack of a mid-level interagency coordination group: the formulation of a NSS or NCSS requires input from a variety of government departments and agencies. This input can be solicited in a variety of ways, ranging from written statements to formal meetings of relevant stakeholders. In support of this process, the establishment of a mid-level, inter-agency coordination group may be useful to harmonise varying requirements across government departments. In the case of formulating a NCSS, it may also be helpful to translate technical requirements stemming from experts/users at the working level into policy-relevant language for decision-makers.

Failing to identify critical services (NCSS): the protection of critical infrastructures is a common requirement identified in a NCSS. As such, policy-makers have come together to identify what constitutes a critical infrastructure and which deserve special attention. In this vein, it may also be useful to go a step further and pre-identify which services are most critical for the well-being of society. Prioritising amongst these – either in a NSS or stand-alone strategy – may be beneficial in formulating a rapid response in the event of an emergency. To illustrate, the Estonian government has pre-identified 42 critical services, ranging for maintaining the electricity supply to ensuring an ice-free port of Tallinn during the winter months to facilitate the transport of goods and people.

Lack of awareness – especially among policy-makers: the formulation of a strategy is a means to an end. A well-developed strategy should provide policy-makers with guidance of concerning key goals, required resources, and how these could be employed most effectively. In the case of a stand-alone strategy covering a specific area, raising awareness levels among decision- and policy-makers may be particularly important to facilitate implementation. For example, concerning NCSS, strategies may suffer from weak follow-through if senior policy-makers have limited awareness of cyber issues and their implications, especially if there is a perception that the private sector should play the principal role in ensuring cyber security.

The German National Cyber Security Council

In the German Cyber Security Strategy (2011), it was announced that a National Cyber Security Council (NCSC) would be established to help monitor the implementation of the Strategy and be able to react to new developments and threats as they occurred. The NCSC was clearly intended to be a 'political supervision' body that would not replace two other strategic and operational level government coordination bodies that were responsible for facilitating the regular day-to-day activities. Instead, this body is directly advised by the 'National Cyber Response Centre', a cyber intelligence fusion centre and cyber crisis management body, and makes decisions on addressing 'structural weakness' in Germany's national cyber security. Voting members of the NCSC include representatives of the Federal Chancellery; a State Secretary from the Federal Foreign Office; the Federal Ministries of the Interior, Defence, Economics and Technology, Justice, Finance, Education and Research; and representatives of the federal *Länder*. On specific occasions, additional ministries or agencies can be included. Business representatives are invited as associated members. Representatives from academia can be involved as required but, similar to the associate members from the private sector, they do not have any voting status or similar. Between April 2011 and September 2012 the NCSC met three times and published extracts of their deliberations online.