Nineteen National Cyber Security Strategies

ARTICLE *in* INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION · JANUARY 2013

Impact Factor: 1 · DOI: 10.1504/IJCIS.2013.051608

3 AUTHORS:

Eric Luiijf
TNO
89 PUBLICATIONS **204** CITATIONS
SEE PROFILE

Kim Besseling
TNO
6 PUBLICATIONS **5** CITATIONS
SEE PROFILE

Patrick de Graaf
TNO
3 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Nineteen national cyber security strategies

Eric Luiijf* and Kim Besseling

TNO,
P.O. Box 96864, 2509 JG The Hague, The Netherlands
E-mail: eric.luiijf@tno.nl
E-mail: kim.vanbuul@tno.nl
* Corresponding author

Patrick de Graaf

Capgemini Netherlands BV,
P.O. Box 2575, 3500 GN Utrecht, The Netherlands
E-mail: patrick.de.graaf@capgemini.com

Abstract: A set of nations have published their national cyber security strategy (NCSS). Despite the fact that each of these NCSS intends to address the same set of cyber security threats, large differences exist between the national focal points and approaches. This paper analyses and compares 19 NCSS [Australia, Canada, Czech Republic, Estonia, France, Germany, India, Japan, Lithuania, Luxembourg, Romania, The Netherlands, New Zealand, South Africa, Spain, Uganda, the UK (2009 and 2011), and the USA]. The analysis and comparisons in this paper highlight common approaches as well as weaknesses. The conclusions and recommendations could assist nations in their development of a NCSS and include a proposed structure for a NCSS and hints for its content.

Keywords: cyber security; national strategy; critical infrastructure; national security; policy; cyber crime.

Reference to this paper should be made as follows: Luiijf, E., Besseling, K. and de Graaf, P. (2013) 'Nineteen national cyber security strategies', *Int. J. Critical Infrastructures*, Vol. 9, Nos. 1/2, pp.3–31.

Biographical notes: Eric Luiijf obtained his Masters degree in Mathematics at the Technical University Delft in 1975. After his duties as officer in the Royal Netherlands Navy, he joined the Netherlands Organisation for Applied Scientific Research TNO. He is currently employed by TNO as Principal Consultant Critical (Information) Infrastructure Protection and by the Netherlands Centre for Protection of National Infrastructure as expert Smart Grid and Process Control System Security.

Kim Besseling graduated in the field of Social and Organisational Psychology and obtained her Master degree in Philosophy at Leiden University in 2008. She started her work career as researcher for TNO. Her main focus has been on cooperation in complex endeavours and information management in different application areas (e.g., security and defence). As a consultant, she is currently shifting her attention to social security.

Patrick de Graaf is a Principal Consultant Cyber Security, focused on strategy, organisation and the human factor at Capgemini Consulting. After obtaining his Masters degree in Dutch Law in 1996, he worked five years for the Ministry of Justice and since 2000 for Capgemini.

This paper is a revised and expanded version of a paper entitled 'Ten national cyber security strategies: a comparison' presented at 6th International Conference on Critical Information Infrastructures Security (CRITIS '11), Lucerne, Switzerland, 8–9 September 2011.

1 Introduction

A set of nations have publically developed and published their national cyber security strategy (NCSS) or, alternatively named, a national information security strategy. This paper analyses and compares 19 NCSS of 18 nations: Australia (AUS), Canada (CAN), Czech Republic (CZE), Estonia (EST), France (FRA), Germany (DEU), India (IND), Japan (JPN), Lithuania (LTU), and Luxembourg (LUX). Romania (ROU), The Netherlands (NLD), New Zealand (NZL), South Africa (ZAF), Spain (ESP), Uganda (UGA), the United Kingdom (GBR; 2009 and 2011 versions), and the United States (USA), of which three (CZE, IND, ROU) are draft NCSS.[1] A set of tables is used to present the main comparable and distinguishing elements of the NCSS in a condensed way. As cyber security deals with and addresses the same global set of threats, common focal points and activities could be expected amongst the NCSS, such as international comparable, or even harmonised, definitions and terminology. Due to the global nature of cyberspace, international collaboration could be expected to be one of the highest priorities of each of the NCSS. In this paper, we will review the strategies and discuss whether this is the case or not. In Section 2, we present the definition of a national strategy and provide an outline of what a national strategy should look like. In Section 3, we discuss the diverse national definitions of cyber security. Section 4 contains the general information on the NCSS, their relationships with other strategies, as well as the envisaged threats and recognised threat actors. The NCSS visions, objectives, guiding principles, and the identified stakeholders are discussed in Section 5. Section 6 tables and discusses the key actions which implement and support the individual national vision and objectives. Section 7 describes recent international developments. Section 8 proposes the structure for a NCSS. Section 9 contains the conclusions and recommendations for nations developing a NCSS to address the common and global challenge of cyber security.

2 A national strategy

Wikipedia (2012) defines a strategy as "a plan of action designed to achieve a vision". Other definitions of a strategy include aspects like leadership, a direction or path to achieve the vision, (more nearby) objectives, a desired future, and a set of activities to reach the objectives. From the above, we derived the following definition for a NCSS: "a national plan of action based upon a national vision to achieve a set of objectives that contribute to the security of the cyberspace domain."

In general, a national strategy will have different aims:

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

3 to convey one's national intent to other nations and stakeholders.

Examples of 3 are power projection and posing the strategy as an application to become a lead nation in a specific domain; global cyber security in this case. Stakeholders in the context of a NCSS are the government, government civil agencies, the military, regulatory bodies, critical infrastructure (CI) operators, industry and businesses at large, small and medium enterprises (SME), research and development organisations, universities, individual citizens, and the population at large.

As nations have more national strategies, a NCSS should describe how it relates to other strategies. The NCSS audience ought to understand how the NCSS vision and activities relate to other (higher-order) strategies such as the national security and defense strategy, a national CI protection strategy, a national digital agenda, the national economic development strategy, as well as international strategies such as the Digital Agenda for Europe (EC, 2010).

The NCSS vision, and the direction its strategic objectives points to, shall be as clear as possible to energise all stakeholders to move their joint activities that are postulated by the NCSS in a common direction. Wherever possible, a national strategy has to push back frontiers from the current state.

3 Defining cyber security

A proper NCSS should establish a common ground by defining the key notions and abbreviations. As Table 1 outlines, only eight of the 18 nations define the *cyber security* notion. Two nations descriptively characterise cyber security using a descriptive text. Uganda and the USA explicitly define information security. Six of the 18 nations (CZE, ESP, EST, JPN, LTU, and LUX) discuss cyber security at a strategic level without defining the notion at all. Moreover, the understanding of cyber security differs greatly among the ten nations that have defined or described the concept. Some nations define cyber security in a bottom-up approach as information security properties to be safeguarded and guaranteed. Other nations use a holistic top-down approach and look for the protection against threats from cyberspace.

The lack of a common, harmonised cyber-related definitions across nations may be a cause of confusion between nations when discussing international approaches to the global cyberspace threats. Early 2011, the Russian-US bilateral working group of the EastWest Institute (EWI) and Moscow University drafted an international cyber terminology framework. They defined cyber security as "a property of cyber space that is an ability to resist intentional and unintentional threats and respond and recover" [Rauscher and Yashenko, (2011), p.31]. Despite on-going academic discussions about most of the cyber domain terminology definitions, the cyber security definition by Rauscher and Yashenko may replace many of the national definitions and understandings of cyber security shown in Table 1. Canada's view on cyber security, however, does not match the definition by Rauscher and Yashenko as Canada only addresses deliberate malicious cyber attacks. Two other nations extend the view of (Rauscher and Yashenko, 2011). The UK includes the physical and electromagnetic disruption threats to cyberspace in its definition (CO, 2009, 2011). Germany includes a risk acceptance notion in its definition (BMI, 2010a, 2010b). Similarly to the notion of cyber security, 15 of the 18

nations discuss *cyber crime* without defining it first. Romania is the only nation which defines all cyber-related notions in its NCSS (MSCI, 2011).

Table 1 National understanding of 'cyber security' (when defined or described)

	Definition?	*Cyber Security*
AUS	definition	Are measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.
CAN	descriptive	Is an appropriate level of response and/or mitigation to cyber attacks – the intentional or unauthorised access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information.
DEU	definition	Is the desired objective of the IT security situation, in which the risk of (global) cyberspace has been reduced to an acceptable minimum. Note: German, civil, and military cyber security are defined in similar wordings.
FRA	definition	Is an information system allowing to resist likely events resulting from cyber space which may compromise the availability, the integrity or confidentiality of data stored, processed or transmitted and of the related services that information and communication (ICT) systems offer.
GBR	descriptive	Embraces both the protection of national interests in cyber space and also the pursuit of wider national security policy through exploitation of the many opportunities that cyber space offers [CO, (2009), p.9].
IND	definition	Is the activity of protecting information and information systems (networks, computers, databases, data centres and applications) with appropriate procedural and technological security measures.
NLD	definition	Is to be free from danger or damage due to the disruption or destruction of ICT, or due to the abuse of ICT.
NZL	definition	Is the practice of making the networks that constitute cyber space as secure as possible against intrusions, maintaining confidentiality, availability, and integrity of information, detecting intrusions and incidents that occur, and responding and recovering from them.
ROU	definition	Is normality resulting from applying a set proactive and reactive measures that ensure confidentiality, integrity, availability, authenticity and non-repudiation of electronic information, and the public and private resources and services in cyberspace.
UGA	implicit	References to 'information security': the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction.
ZAF	definition	Is the collection of tools, policies, security concepts, safeguards, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, and organisation and user assets.

4 The 19 NCSS – general information

Table 2 contains some base information on the (draft) NCSS such as the publication date, publication language(s), reference(s), and the scope. The latter include the relationship

with other national and international strategies, the envisioned envisaged threats and recognised threat actors.

With exception of Luxembourg and Romania, all of the non-native English speaking nations mentioned in Table 2 have published an English version of their NCCS on the Internet. Sixteen of the 18 nations published their first NCSS; Japan and the UK have published a second edition of their NCSS. Due to changes in the UK politics, the (CO, 2011) version is different from the (CO, 2009) version in a number of aspects. For that reason, we decided to highlight the differences. The USA cyberspace security strategy (TWH, 2003) was published in a time when the notion 'cyber security' was not as prominently used as it is today. The Obama Administration undertook a cyberspace policy review which resulted in a set of new national cyber security activities (TWH, 2010). The latter document is, however, not a NCSS but states a set of issues to be addressed by an updated NCSS and near- and mid-term action plans (pp.37–38).

4.1 NCSS views on cyberspace

Most NCSS adopt a holistic view on cyberspace. However, the German NCSS explicitly states that it considers only information and communication technology (ICT) connected to internet. The Australian, Canadian, Spanish and New Zealand's NCSS wordings suggest the same narrow view on what comprises cyberspace. The Dutch NCSS explicitly states that it addresses the full range of ICT which, apart from internet-connected ICT, comprises for instance chip cards, in-car systems, and information transfer media. The Czech Republic, Estonia, France, and South Africa concur with the latter view. The other NCSS are less outspoken about this topic but do not explicitly narrow their focus to 'internet only'.

4.2 Relationship with other national strategies

Eight of the 19 NCSS explicitly relate to their nations' national security strategies (Table 2). The Spanish NCSS actually is part of the Spanish national security strategy. A number of nations developed their NCSS as result of an earlier national threat and risk assessment and in some cases the NCSS even comprises a national threat and risk assessment. Interestingly, Uganda uses a strengths, weaknesses, opportunities and threats (SWOT) analysis at the national level to derive its strategic and related activity plan. The Netherlands uses an external cyclic process: one of their NCSS actions is to deliver an annual national cyber threat and risk assessment for inclusion in the national risk assessment register (NRB). In turn, the NRB capability assessment process may trigger the need for an update of the Dutch NCSS.

Most NCSS explicitly state the cyber security threat to their CI. However, the relationship of the NCSS with the national CI protection (CIP) strategy is less explicitly discussed. This may result in conflicting national requirements for their critical (information) infrastructure [C(I)I] operators. It is even more remarkable that nine out of ten EU Member States do not link their NCSS with the European Critical Infrastructure Protection Directive (EC, 2008). Estonia constitutes the exception.

Table 2 National cyber security strategies

	AUS	*CAN*	*CZE*	*DEU*	*ESP*	*EST*
Native language version	(AG, 2009)	(PSC, 2010a)	(MoI, 2011a)	(BMI, 2011a)	(GdE, 2011a)	(KSK, 2008a)
Other language(s)	n/a	French: (PSC, 2010b)	English: (MoI, 2011b)	English: (BMI, 2011b)	English: (GdE, 2011b)	English: (KSK, 2008b)
Issued	11.2009	10.2010	07.2011	02.2011	05.2011	09.2008
First NCSS version?	Yes	Yes	Draft; (1)	Yes	Yes; (2)	Yes
Size (pages)	38	14	10	10	6 of 86 (2)	36
All types of ICT?	Only internet connected systems	Only internet connected systems	Yes	Only internet connected systems	Networked systems only	Yes
Relates to:						
• National security strategy	■	■	■	■	■	□
• Critical infrastructure protection strategy		■		■		■ (3)
• National digital agenda	■					■
• EU digital agenda (EC, 2010)	n/a	n/a	no	■	no	no (4)
• National defence strategy				□		■
Addresses cyber threats to:						
• Critical infrastructure	■	■	■	■	■	■
• Defence abilities	■	■				
• Economic prosperity	■	■	■	■	■	■
• Globalization				■		
• National security	■	■	■	□	■	□
• Public confidence in ICT					□	
• Social life of citizens	■	■	□			■
Addresses cyber threats from:						
• Activism/extremists					□	
• Criminals/organised crime	■	■	■	■	■	■
• Espionage	■	■		■	■	
• Foreign nations/cyber war		■	■	■	■	■
• Terrorists	■	■	■	■	■	■
• Large-scale attacks		□		■	□	
• Mismatch of technology development and security				■		

Notes: ■ = explicitly described, □ = implicitly referenced

(1) The Czech NCSS has been issued as a draft document awaiting discussion, first in the Czech National Security Council, next by the Government of the Czech Republic.
(2) Included in the Spanish national security strategy.
(3) The Estonian NCSS contains the CII strategy and references to the defined CI (sub)sectors.
(4) The EU digital agenda was published after the publication of the Estonian NCSS.
(5) See SGDN (2008).
(6) See HMG (2009, 2010).
(7) The NCSS is five pages long. The Annex with inter alia the assessment and compliance metrics 2011, 2015 and 2019 is 11 pages.
(8) Reference EC (2009).
(9) The national cyber defence plan is planned to be ready in 2015; see LRV (2011b, Annex p.7).
(10) The NCSS draft was accepted in 2012; see DSS (2012).

Table 2 National cyber security strategies (continued)

	FRA	*GBR*	*IND*	*JPN*	*LTU*	*LUX*
Native language version	(SGDN, 2011a)	(CO, 2011)	(DIT, 2011)	Japanese	(LRV, 2011a)	(GGDL, 2011)
Other language(s)	English: (SGDN, 2011b)	n/a	n/a	English: (ISPC, 2009)	English: (LRV, 2011b)	No
Issued	02.2011	11.2011	04.2011	02.2009	06.2011	11.2011
First NCSS version?	Yes	No: (CO, 2009)	Draft	No: (ISPC, 2006)	Yes	Yes
Size (pages)	22	44	20	20	5+11 (7)	11
All types of ICT?	Yes	Implicitly	Implicitly	Implicitly	Implicitly	Implicitly
Relates to:						
• National security strategy	■	■ (6)				
• Critical infrastructure protection strategy	□	□	□		■ (8)	□
• National digital agenda			■	■	■	
• EU digital agenda	no	no	n/a	n/a	no	no
• National defence strategy	■ (5)	□			□ (9)	
Addresses cyber threats to:						
• Critical infrastructure	■	■	■	□	■	■
• Defence abilities	□					
• Economic prosperity	□	■	■	■	□	■
• Globalization			□	■		
• National security	■	■		■	□	
• Public confidence in ICT		■			■	□
• Social life of citizens		■		■		
Addresses cyber threats from:						
• Activism/extremists		■				
• Criminals/organised crime	■	■	■	□	■	■
• Espionage	■	■		□		
• Foreign nations/cyber war	■	■	■	■		
• Terrorists	■	■				
• Large-scale attacks		■	□	■	■	
• Mismatch of technology development and security				■		

Notes: ■ = explicitly described, □ = implicitly referenced

(1) The Czech NCSS has been issued as a draft document awaiting discussion, first in the Czech National Security Council, next by the Government of the Czech Republic.
(2) Included in the Spanish national security strategy.
(3) The Estonian NCSS contains the CII strategy and references to the defined CI (sub)sectors.
(4) The EU digital agenda was published after the publication of the Estonian NCSS.
(5) See SGDN (2008).
(6) See HMG (2009, 2010).
(7) The NCSS is five pages long. The Annex with inter alia the assessment and compliance metrics 2011, 2015 and 2019 is 11 pages.
(8) Reference EC (2009).
(9) The national cyber defence plan is planned to be ready in 2015; see LRV (2011b, Annex p.7).
(10) The NCSS draft was accepted in 2012; see DSS (2012).

Table 2 National cyber security strategies (continued)

	NLD	*NZL*	*ROU*	*UGA*	*USA*	*ZAF*
Native language version	(MinV&J, 2011a)	(MoED, 2011)	(MSCI, 2011)	(MoICT, 2011)	(TWH, 2003)	(DSS, 2010)
Other language(s)	English: (MinV&J, 2011b)	n/a	no	n/a	n/a	n/a
Issued	02.2011	06.2011	05.2011	11.2011	02.2003	02.2010 (10)
First NCSS version?	Yes	Yes	Draft	Yes	Yes	Yes
Size (pages)	9	52	10	54	25	15
All types of ICT?	yes	Networked systems only	Implicitly	Implicitly	Implicitly	Yes
Relates to:						
• National security strategy	□				■	
• Critical infrastructure protection strategy	□				□	
• National digital agenda	■			□		
• EU digital agenda	■	n/a	No	n/a	n/a	n/a
• National defence strategy	□					
Addresses cyber threats to:						
• Critical infrastructure	■	■	■	■	□	■
• Defence abilities	□		■			
• Economic prosperity	■	■	□	■	■	■
• Globalization						
• National security	□	■	■		■	□
• Public confidence in ICT	■	□		■	■	■
• Social life of citizens	■					
Addresses cyber threats from:						
• Activism/extremists	■	■	■			
• Criminals/organised crime	■	■	■	■	□	■
• Espionage	■	■	■		■	
• Foreign nations/cyber war	■		■	■	■	
• Terrorists	■	■	■	■	■	
• Large-scale attacks				□	□	
• Mismatch of technology development and security						

Notes: ■ = explicitly described, □ = implicitly referenced

(1) The Czech NCSS has been issued as a draft document awaiting discussion, first in the Czech National Security Council, next by the Government of the Czech Republic.
(2) Included in the Spanish national security strategy.
(3) The Estonian NCSS contains the CII strategy and references to the defined CI (sub)sectors.
(4) The EU digital agenda was published after the publication of the Estonian NCSS.
(5) See SGDN (2008).
(6) See HMG (2009, 2010).
(7) The NCSS is five pages long. The Annex with inter alia the assessment and compliance metrics 2011, 2015 and 2019 is 11 pages.
(8) Reference EC (2009).
(9) The national cyber defence plan is planned to be ready in 2015; see LRV (2011b, Annex p.7).
(10) The NCSS draft was accepted in 2012; see DSS (2012).

Most of the 19 NCSS address the economical prosperity aspects of the cyberspace realm. Cyber security is considered to be a minimal requirement to enhance the prosperity of the population and to foster economic welfare. For instance, the EU digital agenda for Europe (EC, 2010) should be a driver in this respect for its 27 member states, however only the German and Dutch NCSS refer to this Agenda.

The NCSS of most of the 18 nations show that national governments struggle and debate which governmental department or agency is the lead agency when a major cyber attack or ICT-based disruption affects the nation. As part of their national defence strategy, some nations develop military cyber operations/ cyber defence capabilities. The 2009 UK's NCSS [CO, (2009), pp.14, 26] is more explicit on its military and intelligence capability building in the cyberspace domain than its later 2011 edition (CO, 2011). The French NCSS points to its national security and defence strategy which states the need for (military) cyber defence and deterrence [SGDN, (2011a, 2011b), p.3]. The German [BMI, (2011), p.4] and Dutch [MinV&J, (2011b), p.8] NCSS point to their military cyber operations developments.

4.3 Threat subjects and malicious threat actor objectives

All nations address in their NCSS the cyber threats to their C(I)I. Sixteen nations address this in an explicit manner. Fourteen nations consider the cyber threats as part of their national security of which nine nations mention this explicitly. Only Australia and Canada explicitly state the cyber security risk in relation to their national defence abilities. France implicitly addresses the cyber threat to defence by referring to its White Paper on Defence and National Security (SGDN, 2008).

Germany, India and Japan point in their NCSS at the threat of stagnation of globalisation when the cyber security risk is insufficiently addressed. Related to this threat is the threat of disruption of the societal and social ICT-life of citizens. Six nations explicitly address this threat. The threat of loss of public confidence in the use of ICT is explicitly recognised by six of the 18 nations; the UK recognises this since the 2011 edition of its NCSS. Eight nations completely omit this type of threat in their NCSS despite their outspoken intent to quickly expand their ICT-based society.

All nations except Japan and the USA explicitly pinpoint individuals, criminals, and organised crime as malicious threat actors. Cyber espionage (e-spionage) is explicitly mentioned by ten nations. Thirteen nations identify the threat of hostile activities by foreign nations (e.g., cyber warfare) in their NCSS. Despite the 2011 set of attacks in cyberspace by groups like Anonymous and LulzSec, only the Netherlands, New Zealand, Romania, and the UK (CO, 2011) explicitly recognise (h)activists and extremists as malicious threat actors.

Thirteen nations fear (potential) cyber attacks by terrorists on their C(I)I, something which has not occurred yet [Luiijf, (2008), pp.164–165]. Moreover, Canada, France, New Zealand, Romania, and the UK address in their NCSS the use of cyberspace by terrorists for propaganda, fund raising, communication and planning. In addition, the UK mentions the use of cyberspace to gather intelligence on terrorists (CO, 2009).

Germany, Japan, Lithuania, and the UK (CO, 2011) explicitly address the threat of large-scale cyber attacks to their C(I)I. This is not surprising in the case of Japan as Japan has experienced several large-scale (and publically known) cyber attacks to its

governmental and business systems in the recent past. The other three nations, however, have not experienced large-scale cyber attacks yet when they published their NCSS.

Both the German and Japanese NCSS refer to the threat of mismatches between functional ICT developments and an appropriate level of cyber security related to those developments. Interestingly, none of the other nations addresses this important global topic of threats due to ICT innovation.

UK's 2009 NCSS includes jamming and signal modification of, for instance, GPS signals, and high-power radio frequency transmission with, for instance, a High Power Microwave, damaging unprotected electronics as cyber security threats to address (CO, (2009), pp.13–14). These may not be digital as a threat, but are definitely harming digital assets. None of the other NCSS refer to these threats despite growing international concerns about criminals applying these technologies. Therefore, it is a surprise that (CO, 2011) does not put these threats and challenges to the fore anymore.

5 Visions, objectives, and principles

5.1 National cyber security visions

Using the definition of a NCSS in Section 2, a NCSS should present a focal point at the horizon, a vision. Table 3 shows that twelve nations explicitly provide such a vision. The other nations have a more implicit description of their strategy's focus. Eight NCSS put a focus on the economic prosperity of the digital society. Eight nations put a focus on the confidence of the citizens and companies of the digital society. Estonia, victim of a serious and prolonged cyber attacked in Spring 2007, promotes the cyber security of other nations (see Table 3). Its vision of "the enhancement of cyber security in other nations" is unique amongst the set of NCSS.

Table 3 The national visions on cyber security

AUS	Explicit	The maintenance of a secure, resilient and trusted electronic operating environment that supports the national security and maximises the benefits of the digital economy.
CAN	Explicit	Our national plan for making cyberspace more secure for all Canadians.
CZE	Explicit	Define interests and intentions of the Czech Republic in the field of cyber security needed to build up a credible information society with solid legal foundations, which is committed to a secure cyber transmission and processing of information in all domains of human activities and makes sure that the information can be used and shared freely and safely.
DEU	Explicit	The Federal Government aims at making a substantial contribution to a secure cyberspace, thus maintaining and promoting economic and social prosperity in Germany.
ESP	Explicit	Ensuring the security of Spain, its citizens and inhabitants in the cyberspace domain.
EST	Implicit	Primarily seeks to reduce the inherent vulnerabilities of cyberspace in the nation as a whole. This will be accomplished through the implementation of national action plans and through active international cooperation, and so will support the enhancement of cyber security in other countries as well.

Note: [1]Lithuania mixed its vision with a set of SMART performance criteria.

Table 3 The national visions on cyber security (continued)

FRA	Implicit	France must retain its areas of sovereignty, concentrated on the capability necessary for the maintenance of the strategic and political autonomy of the nation: {…} and cyber-security are amongst the priorities.
GBR	Explicit	Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society.
IND	Implicit	Providing right kind of focus for secure computing environment and adequate trust and confidence in electronic transactions becomes one of the compelling priorities for the country given the growth of IT sector in India and India's prominent role in the IT global market.
JPN	Implicit	The government is responsible for overcoming risks concerning usage of ICT through reinforcing the protection for the critical infrastructures that support socioeconomic activities and which are closely connected to the nation's day-to-day life and should also take organised and immediate action to ensure national security and effective crisis management.
LTU	Implicit	The development of security of electronic information, ensuring cyber security in order to make Lithuanian residents feel secure in cyberspace.[1]
LUX	Explicit	Strengthen the cyber security and resilience of infrastructures and contribute to ensure the protection of citizens, professionals and society.
NLD	Explicit	Security and confidence in an open and free digital society.
NZL	Implicit	Outline the Government's response to the growing cyber threat and highlights initiatives for individuals, businesses and government to strengthen New Zealand's cyber security position.
ROU	Explicit	To underpin the objectives, principles and directions of cyber security in Romania in a coherent and consistent fashion with respect to knowledge development, prevention, and the countering of cyber risk and cyber threats
UGA	Explicit	The vision is to provide a strategic direction for the national information security in order to promote trust and enable business and economic growth.
USA	Explicit	The purpose of the strategy is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact.
ZAF	Explicit	To establish an environment that will ensure confidence and trust in the secure use of ICT.

Note: [1]Lithuania mixed its vision with a set of SMART performance criteria.

5.2 Strategic objectives

Table 4 outlines the strategic cyber security objectives of 17 nations. Germany, however, presents in (BMI, 2011a, 2011b) a set of strategic priority areas which other NCSS present as action lines. Most NCSS contain between three and four strategic objectives. Nations such as Germany, Romania, Uganda, and South Africa with more than four objectives either seem to mix their strategic objectives with action lines (for example, Luxembourg) or present their key action lines.

Table 4 Strategic objectives of the NCSS

AUS	1	All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online
	2	Australian businesses operate secure and resilient ICT to protect the integrity of their own operations and the identity and privacy of their customers
	3	The Australian government ensures its own operations and the identity and privacy of their customers
CAN	Meeting the cyber security threat by:	
	1	Securing government systems
	2	Partnering to secure vital cyber systems outside the federal government
	3	Helping the Canadians to be secure online
CZE		To maintain a safe, secure, resistant and credible environment that makes use of available opportunities offered by the digital age.
DEU	Strategic security areas rather than strategic objectives are presented:	
	1	Protection of critical infrastructures
	2	Secure IT systems in Germany
	3	Strengthening IT security in the public administration
	4	National cyber response centre
	5	National cyber security council
	6	Effective crime control in cyberspace
	7	Effective coordinated action to ensure cyber security in Europe and worldwide
	8	Use of reliable and trustworthy IT
	9	Personnel development in federal authorities
	10	Tools to respond to cyber attack
ESP	*The Spanish NCSS is integral part of the Spanish national security strategy (EES) with the objective to defend the Spanish vital and strategic interests and values.*	
EST	1	Establish a multilevel system of security measures
	2	Expand national expertise in and awareness of information security
	3	Adopt an appropriate regulatory framework to support secure and extensive use of ICT
	4	Consolidate national position as one of the leading countries in international cooperative efforts to ensure cyber security
FRA	1	To be a world power in cyber defence
	2	To guarantee the French national freedom to decide by protecting national information
	3	To reinforce the cyber security of critical infrastructures
	4	To ensure the safety in the cyberspace
GBR	1	To tackle cyber crime and be one of the most secure places in the world to do business in cyberspace
	2	To be more resilient to cyber attacks and better able to protect our interests in cyberspace
	3	To have helped shape an open, stable and vibrant cyberspace which our public can use safely and that supports open societies

Table 4 Strategic objectives of the NCSS (continued)

IND	1	To further ICT in India as an engine for economic growth and prosperity
	2	To create a security framework for securing of cyber space
JPN	1	Reinforced policy to counter cyber attacks
	2	Policies to adapt to changes in cyber security environment
	3	Active/dynamic cyber security measures (see ISPC, 2009)
LTU	1	Ensure the cyber security of state-owned information resources
	2	Ensure an efficient functioning of critical information infrastructure
	3	Seek to ensure the cyber security of residents of, and persons staying in Lithuania.
LUX	1	Ensure the operational protection of infrastructures and ICT systems
	2	Modernise the legal framework
	3	Develop national and international collaboration
	4	Inform, educate and raise awareness about the cyber security risk
	5	Establish mandatory norms and standards.
NLD	1	To reinforce the security of the digital society, in order to increase confidence in the use of ICT by citizens, business and government in order to stimulate the Dutch economy and to increase prosperity and well-being of its citizens.
	2	Proper legal protection in the digital domain is guaranteed and societal disruption is prevented.
	3	Adequate action will be taken if things were to go wrong.
NZL	1	Raise awareness and online security of individuals and small businesses
	2	Protecting government systems
	3	Build strategic relationships to improve cyber security for critical infrastructure and other businesses.
ROU	1	Adapt the legal framework and institutional dynamics to the threats from cyberspace
	2	Establish and implement minimum security requirements for national cyber infrastructure with relevance for the functioning of critical infrastructure
	3	Ensure the security and resilience of the Romanian cyber infrastructure
	4	Promote and develop national and international cooperation
	5	Increase the security culture through awareness of the population about cyberspace vulnerabilities, risk, threats and the need to protect cyber systems.
UGA	1	Streamline the implementation of information security nationally and internationally
	2	Profile, classify and protect critical information infrastructure from disruption
	3	Establish a framework responsible for the monitoring of the information security
	4	Promote secure e-commerce and e-government services and other national IT projects
	5	Safeguard the privacy rights of individuals through good information security governance
	6	Development of a culture of cyber security awareness at national level and build human resource capacity
	7	Uphold information security risk management and attain a good information security maturity

Table 4 Strategic objectives of the NCSS (continued)

USA	1	Prevent cyber attacks against US critical infrastructure
	2	Reduce national vulnerability to cyber attacks
	3	Minimise damage and recovery time from cyber attacks that do occur
ZAF	1	Establish relevant cyber security structures
	2	Reduce cyber threats and vulnerabilities
	3	Forster public-private cooperation and coordination
	4	Promote and strengthen international cooperation on cyber security
	5	Build capacity and promote culture of cyber security
	6	Promote compliance with appropriate technical and operational cyber security standards

Large differences between the national strategic objectives exist due to different starting points and visions like a safe, secure and resilient ICT environment, economic prosperity, national security, and (military) defence. Australia, Canada, Lithuania and New Zealand structure their objectives along a similar stakeholder-based schema: government, CIs and businesses, and citizens/individuals. Japan explicitly recognises the need for agile adaption to new and upcoming cyber security threats in their set of strategic objectives. Germany touches this topic as well [BMI, (2011a), p.12, (2011b), p.8], but does not state any related activities.

France follows a different approach as it states its ambition to become a world power in cyber security and to maintain information superiority in the national part of cyberspace. France is the only nation to explicitly follow this path, although some other NCSS support some form of power projection. For instance, the UK gathers intelligence on criminals, terrorists, and other adverse actors in cyberspace and exploits such information to disrupt cyber crime and to reduce the motivation and capabilities of adversaries operating in cyberspace [CO, (2009), p.4, 16]. Derrick (2011) published that MI6 hacked al-Qai'da's online magazine *Inspire*. According to this publication, a web article on 'Make a bomb in the Kitchen of your mom' was replaced with recipes for 'The best cupcakes in America'. This is an example of the implementation of this strategy, although [CO, (2011), p.26] covertly refers to cyber exploitation activities which fall under "some of the activity the Government has set in train is necessarily classified" [CO, (2011), p.9].

5.3 Guiding principles and framework conditions

Table 5 shows that ten of the 18 nations relate the content of their NCSS to guiding principles or framework conditions. France, India, Japan, Lithuania, Luxembourg, New Zealand, Uganda and South Africa lack references to any guiding principle in their NCSS. Eight nations refer to the protection of civil liberties and other (inter)national democratic core values. Germany and Romania do not reference these values in their NCSS. Eight nations refer to cooperation and public-private partnerships (PPP) as a cyber security framework condition. The Czech Republic, the USA (and the eight nations lacking guiding principles) do not mention PPP as a cornerstone to their NCSS.

Table 5 Guiding principles of the NCSS (when described)

AUS	1	National leadership.
	2	Shared responsibilities.
	3	Partnerships.
	4	Active international engagement.
	5	Risk management.
	6	Protecting Australian values.
CAN	No explicit guiding principles, but references the NCSS of USA, UK and Australia. "Many of the guiding principles and operational priorities set out in those reports resemble our own" [PSC, (2010a, 2010b), p.8].	
CZE	1	Abide the principles of a democratic society and duly consider legitimate interests of its citizens, business sector and public administrations and agencies in relation to citizens.
	2	Adequate cyber security measures to protect and guarantee national security will respect privacy, fundamental rights and liberties, free access to information, and other democratic principles.
	3	National cyber security measures balance the need to guarantee security with the respect for fundamental rights and liberties.
DEU	All stakeholders have to act as partners and fulfil protection tasks together. Enforcement of international rules of conduct, standards and norms.	
ESP	1	Comprehensive approach.
	2	Coordination.
	3	Efficient use of resources.
	4	Anticipation and prevention.
	5	Resilience.
	6	Responsible interdependence.
	Moreover, the NCSS executive summary points at respect for democratic values, human rights and the rule of law.	
EST	1	Cyber security should be integrated in routine processes of national security planning.
	2	Cyber security through coordinated efforts of all stakeholders, public and private sector and civil society.
	3	Advance effective public-private cooperation to protect the critical information infrastructure.
	4	Every ICT owner is responsible and shall manage identified risk; foster general societal awareness and state of readiness.
	5	Closely cooperate with international organisations and other nations.
	6	Pay attention to protect human rights, personal data and identity.
GBR	1	A risk-based approach.
	2	Working in partnership.
	3	Balancing security with freedom and privacy.

Table 5 Guiding principles of the NCSS (when described) (continued)

NLD	1	Linking and reinforcing existing cyber security initiatives.
	2	Public-private partnership and clear responsibilities, powers and safeguards.
	3	Individual responsibility to secure cyberspace (citizens, businesses, the public administration and its agencies).
	4	Active international collaboration.
	5	Security measures are balanced and proportional with respect to public and national security versus safeguarding of fundamental human rights.
	6	Self-regulation if possible, legislation and regulation when required.
ROU	1	Coordination: joint activities are carried out based on converged cyber security action plans in accordance with the duties and responsibilities of each stakeholder.
	2	Cooperation: all public and private stakeholders collaborate at national and international level to ensure adequate response to cyberspace threats.
	3	Efficiency: optimal management of available resources.
	4	Prioritisation: the national focus is on securing the infrastructure which supports the national critical information infrastructure.
	5	Dissemination: transfer of information, expertise, and good practices to protect the cyber infrastructure.
USA		Privacy and civil liberties need to be protected.

5.4 Stakeholders addressed by the NCSS

Table 6 shows a breakdown of the cyber security stakeholders recognised by the NCSS. It is easy to see that the NCSS bias to government, national security, and CIs. Fourteen of the 18 nations expect their citizens to take an active role in cyber security. Japan, Luxembourg, Spain, and South Africa only mention end-users in relationship to awareness raising.

Both South Africa's and Japan's NCSS focus on their respective government and the CIs. Lithuania and Romania put their focus on the government, CIs, and the population. Remarkably, their NCSS do not address SME, internet service provider (ISP), and large organisations and businesses.

ISP are only explicitly addressed by the NCSS of Australia, Czech Republic, Germany, Estonia, New Zealand, and the UK. Whereas the UK's Cabinet Office did not mention ISP in its 2009 NCSS (CO, 2009), the 2011 edition refers to ISP that have "to help individuals identify whether their computers have been compromised and what they can do to resolve the compromise and protect themselves from future attacks" [CO, (2011), p.31]. Australia's ISP, supported by the Australian government, undertake a set of joint activities to raise the cyber security of their operations and their customers. According to the Australian NCSS [AG, (2010), pp.18–19], these activities include an ISP Code of Practice and the identification of compromised customer systems.

Germany, Estonia, the UK, and the USA explicitly consider the global cyber infrastructures as cyber security stakeholders. In general, these stakeholders (e.g., backbone providers) operate outside the direct influence sphere of nation states.

Table 6 The NCSS directly addresses the following types of stakeholders with respect to threats, vulnerabilities and measures

	Citizens	*SME*	*ISP*	*Large organisations*	*CI operators*	*The state/national security*	*Global infrastructure and issues*
AUS	■	■	■	■	■	■	□
CAN	■	□	□	■	■	■	□
CZE	■	■	■	■	■	■	
DEU	■	■	■	□	■	■	■
ESP	□	□	□	□	■	■	
EST	■	■	■	■	■	■	■
FRA	■	■	□	■	■	■	□
GBR	■	■	■	■	■	■	■
IND	■	■	□	■	■	■	
JPN	□	□		□	■	■	□
LTU	■				■	■	
LUX	□	□	□	□	■	■	
NLD	■	■	□	■	■	■	□
NZL	■	■	■	■	■	■	
ROU	■				■	■	
UGA	■	■		■	□	■	
USA	■	■	□	■	■	■	■
ZAF	□	□		□	■	■	

Notes: □ = when discussed in the NCSS but limited set of related actions/activities

6 Tactical/operational level action plans

6.1 SMARTness

Table 7 outlines the actions and activities mentioned in the NCSS. The table shows that all nations have defined tactical action lines and often a set of detailed operational actions in support of their strategic cyber security objectives. As most NCSS express an urgent need to take action, one would expect a specific, measurable, achievable, realistic and timely (SMART) definition of the actions. Smartness, allows national parliaments to be able to perform their oversight role as well as other herders of cyber security to monitor the progress of the NCSS action lines. It helps to detect insufficient progress which can be addressed in time to make the NCSS a success. Unfortunately, only Japan, Lithuania, and Uganda nations have defined their planned activities to a certain level of SMART-ness:

1 Japan's SMART approach relates to a quality management approach.

2 Lithuania's NCSS has an annex which for each of the planned tasks states the responsible stakeholder(s) and a set of compliance metric indicators. The latter describes the actual 2011 situation, and the projected 2015 midway and 2019 target situations.

3 Uganda defines sub-objectives supporting its NCSS objectives with the related responsible stakeholder, the expected outcome, the timeframe, source of funding, and a budget plan for each year in the period 2011–2014.

The other nations state most of their activities in a non-SMART way.

6.2 Adaptability to future threats

Although Germany and the USA also mention the dynamics of the ICT-threat and the threats related to ICT innovation, Japan is the only nation which regards the agile adaption to emerging cyber security threats as a strategic objective and plans a set of related tactical and operational activities. This shows that Japan approaches the cyber security issues more from a wider, (technological) dynamic, security perspective than other nations. As an example, Japan addresses the security aspects of IP version 6 as well as the cyber security of home appliances, such as solar panels, fridges and washing machines, which actively participate in smart (energy) grids. Apart from Japan, France specifically intends to address the cyber security of cloud computing. Most other nations seem to try to incorporate flexibility and adaptability less explicitly in their NCSS through vaguer description of objectives.

6.3 Planned actions in detail

A wide array of action areas is elaborated on by the 19 NCSS, with often a considerable overlap. All nations except Uganda explicitly address in their NCSS the protection of their own CIs including the government's own ICT. Some nations refer to already existing activities rather than starting new ones. Five nations (Canada, Germany, UK, The Netherlands, and the USA) explicitly refer to their military cyber security capabilities and plans; the French NCSS suggests an equivalent approach. The Dutch NCSS points to cyber operations structures and activities of the Ministry of Defence which are outlined in MinDef (2012). In a similar way, the German NCSS points in BMI (2011a, 2011b) to cyber operations plans of the German Armed Forces (*Bundeswehr*).

All nations but South Africa mention plan to develop a cyber security awareness programme. Apart from community-wide programmes, Germany, the Netherlands, South Africa, the UK, and USA develop cyber education and training programmes for specific groups of civil servants such as defence personnel and law enforcement experts.

Fifteen nations (excluding Spain, Uganda and the UK) strengthen their ICT crisis management and response measures to address major cyber-related disruptions. National and sector-specific exercises are often related to these activities, although Table 7 shows that only ten nations specifically mention national exercises in their NCSS. Six nations (Australia, Canada, Czech Republic, France, Lithuania, and the UK) refer to the development of cyber disturbance detection capabilities at the national level.

Table 7 Key action lines and planned actions

Key actions and action lines	*AUS*	*CAN*	*CZE*	*DEU*	*ESP*	*EST*
Active/dynamic security measures						■
Awareness and training/information security campaign	■	■ (objective 3)	■	Action 2	■	■
Adaptable policy to new ICT risk				□		
Continuity and contingency plans					■	■
Critical infrastructure protection	■	■	■	Action 1	■	■
Cryptographic protection				(Action 8)	■	
Cyber arms control					■	
Defence cyber operations/intervention, training and exercises		■		■	□	□
Develop and share good practices					■	
Economic growth	■	■	■		■	■
Education and training	■	■	■	(Action 9)	■	■
Exercises	■	■		■		■
Explicit holistic view					□	
Exploitation to combat threats						
Improved security of ICT products						
Information sharing/ exchange	■	■	■	Action 4		■
Intelligence gathering on threat actors	■	■			■	
International collaboration	■	■	■	Action 7	■	■
Legislation/legal framework			■		■	■
Mandating security standards			■		□	■
National detection capability	■	■	■			
National response capability/ICT crisis management	■	■	■	Action 4		■
Privacy protection	■	■				□
Promote cyber crime convention		□		Action 6		■
Protection of non-critical infra	■	■	■			
Public-private partnership	■	(Objective 2)	■		■	■
Reducing adversary's motivation and capabilities						
Research and development	■	■	■			■
Resilience against disturbances/threat and vulnerability reduction	■					
Secure protocols and software				Action 2		
Secure sourcing of products				Action 8	■	
Self protection of the government	■	(Objective 1)	■	Action 3	■	□
Strategic cyber security council			ICBCS	Action 5		
Threat and vulnerability analysis	■	■	■	Action 4		
Tracing criminals and prosecution	■	■		Action 6		Policy MoJ
Actions defined SMARTly?	No	No	No	No	No	No

Notes: ■ = specific activities; □ implicitly indicated

Table 7 Key action lines and planned actions (continued)

Key actions and action lines	*FRA*	*GBR*	*IND*	*JPN*	*LTU*	*LUX*
Active/dynamic security measures			■	■ (objective 3)		
Awareness and training/information security campaign	Action 7	■	■	■	■	■
Adaptable policy to new ICT risk				■ (objective 2)		
Continuity and contingency plans		Telecom law	■	■	■	■
Critical infrastructure protection	Action 4 (objective 3)	■	■	Action line 1	■	■
Cryptographic protection	■			■		
Cyber arms control						
Defence cyber operations/intervention, training and exercises	□	■				
Develop and share good practices						□
Economic growth		□ (objective)	■	Action line 4 (objective)	□	■
Education and training	■	■	■			■
Exercises		□	■		■	■
Explicit holistic view				Action line 3		
Exploitation to combat threats		■ (see text)				
Improved security of ICT products						
Information sharing/ exchange		■	■			■
Intelligence gathering on threat actors		■	■			
International collaboration	Action 6	■	■	Action line 5	■	■
Legislation/legal framework		■	■		■	■
Mandating security standards						■
National detection capability	Action 2	□			■	
National response capability/ICT crisis management	Action 2		■	Action line 2	■	■
Privacy protection	□		■	■		
Promote cyber crime convention		■				
Protection of non-critical infra		□	□	□		□
Public-private partnership		■	■	■		■
Reducing adversary's motivation and capabilities		■				
Research and development	Action 3	■	■			■
Resilience against disturbances/threat and vulnerability reduction	Action 4	■	□	Action line 1		■
Secure protocols and software	■		■			
Secure sourcing of products	■	■				
Self protection of the government	■ (objective 2)	■	□	■	■	■
Strategic cyber security council		Only gov.				■
Threat and vulnerability analysis	Action 1	■	■		■	■
Tracing criminals and prosecution	Action 5		■	■	■	
Actions defined SMARTly?	No	Limited	No	Yes	Yes	No

Notes: ■ = specific activities; □ implicitly indicated

Table 7 Key action lines and planned actions (continued)

Key actions and action lines	*NLD*	*NZL*	*ROU*	*UGA*	*USA*	*ZAF*
Active/dynamic security measures					■	
Awareness and training/information security campaign	Ongoing; intensify	■	Objective 5	■	Priority 3	
Adaptable policy to new ICT risk						
Continuity and contingency plans	Telecom law			■	□	
Critical infrastructure protection	Ongoing	■	■	□	Ongoing	■
Cryptographic protection						
Cyber arms control						
Defence cyber operations/intervention, training and exercises	■				■	
Develop and share good practices			■	■		■
Economic growth	□ (objective)			■	□	■
Education and training	Action line 6		■	■	□	□
Exercises	■	■			□	■
Explicit holistic view					Priority 5	□
Exploitation to combat threats						
Improved security of ICT products	■					
Information sharing/ exchange	■		■	■	■	
Intelligence gathering on threat actors	■					
International collaboration	■	□	Objective 4	■	Priority 5	■
Legislation/legal framework	Review		Objective 1	■		□
Mandating security standards			■			□
National detection capability						
National response capability/ICT crisis management	Action line 4	■	■		Priority 1	■
Privacy protection	■					
Promote cyber crime convention	■	Considering			■	
Protection of non-critical infra	□					
Public-private partnership	Action line 1		Objective 3	■		■
Reducing adversary's motivation and capabilities						
Research and development	Action line 6	■	■	■	■	□
Resilience against disturbances/threat and vulnerability reduction	Action line 3	■	Objective 2		Priority 2	
Secure protocols and software					■	■
Secure sourcing of products						
Self protection of the government	■	■	■	■	Priority 4	■
Strategic cyber security council	All actors					
Threat and vulnerability analysis	Action line 2				■	■
Tracing criminals and prosecution	Action line 5		■		■	
Actions defined SMARTly?	Some	No	No	Partly	No	No

Notes: ■ = specific activities; □ implicitly indicated

All nations but New Zealand mention international collaboration as an action line or high priority topic. New Zealand only does mention its current international security partners and partners in combating cyber crime. However, most NCSS fail to explain their envisioned international collaboration activities in detail other than sharing information, for instance via the national computer emergency response teams (CERTs). This despite the fact that the cyber crime does not stop at borders. The majority of the cyber threats therefore requires swift collaborative international action as adversaries and cyber criminals will not wait until multiple national authorities finally agree to act.

With respect to combating international cyber crime, Estonia, Germany, The Netherlands and USA expressed that they intend to promote the cybercrime convention (CoE, 2001) to other nations. Canada intends to ratify the cybercrime convention treaty; the UK did so in May 2011. Moreover, the Czech Republic, Estonia, Luxembourg, and Romania intend to update their legislation and consider to mandate a set of minimum cyber security standards to protect their government systems and critical information and information-based infrastructures.

Four nations (France, Germany, Spain, and the UK) explicitly refer to secure sourcing of cyber security products and to own development of so-called government-off-the-shelf (GOTS) hardware and software to be used as part of the critical and sensitive government infrastructures and sometimes in national CI. The UK implicitly mentions its information assurance agencies. The other 14 nations do not make clear whether GOTS hardware and software is a high priority issue or not. The Dutch NCSS has the intent to put software quality on the international agenda. The idea is to reduce the number of cyber security vulnerabilities by promoting higher software quality and introducing software liability for manufacturers. This idea does not meet with response as none of the other NCSS fosters the same idea. Spain finds itself in an equivalent position where it intents to foster cooperation to develop agreements on cyber arms control [GdE, (2011b), p.62], although this is very much in line with Russia's attempts for a Cyber Treaty (Markoff and Kramer, 2009), and the recent China, Russia, Tajikistan and Uzbekistan 2011 initiative to the General Assembly of the United Nations for an 'International Code of Conduct for Information Security' (UN, 2011).

6.4 NCSS institutionalisation

The Czech Republic, Germany, Japan, Luxembourg, and the Netherlands institutionalised a cyber security board (CSB) or council (CSC) at the strategic level. The Czech Republic established an Interdepartmental Coordination Board for Cyber Security, the ICBCS. Japan established an intra-governmental board as well. The German CSC also is an intra-governmental council, but private stakeholders are allowed to participate as observers. The Dutch CSC has members from public and private organisations as well as from R&D institutions/academic organisations. In a similar manner, South Africa established a National Cyber Security Advisory Council (NCAC).

Germany and the Netherlands refer to new military operational cyber security capabilities; Canada will extend their existing defence capabilities. Some other nations, like the USA do have military objectives but these are stretched out in separate (military) strategic as well as cyber operations doctrine documents.

At the operational level, most nations state in their NCSS that they will strengthen their national CERT if it already exists; other nations plan to establish a national CERT.

Several nations mentions the strengthening of their digital police and digital forensic capabilities.

7 International NCSS developments

At the moment of writing, we understand from public sources that Slovakia and South Korea have non-public NCSS. Various other nations such as Austria, Belgium, Finland, and Turkey are in the process of developing a NCSS. Switzerland issued its NCSS just when the final version of this paper had to be submitted; therefore no analysis has been made of VBS (2012).

In the mean time, the European Network and Information Security Agency (ENISA) has started activities to develop a Good Practice Guide on NCSS which, according to ENISA (2012, p.4) will present good practices and recommendations on how to develop, implement and maintain a NCSS. The (ENISA, 2012) document presents some preliminary findings based upon some of the NCSS discussed in this paper. It also contains a set of recommendations to EU's Member States (p.12). The recommendations lack to address some of the findings in this paper. The need for a harmonised definition of cyber security, as identified by this paper, is considered as a long-term action. ENISA recommends to the Member States to recognise the evolution of cyberspace and the dynamics of cyber security threats by making their NCSS a living document.

In 2011, the USA issued the international strategy for cyberspace which envisions a future cyberspace environment that "rewards innovation and empowers individuals; connects individuals and strengthens communities; builds better governments and expands accountability; safeguards fundamental freedoms and enhances national and international security" [TWH, (2011), p.8]. With this strategy, the USA wants to unify its multi-department engagement with international partners on the full range of cyber issues of the global commons 'cyberspace'. The international strategy refers to a set of US "core commitments: fundamental freedoms, privacy of citizens, and the free flow of information" (p.5). The strategy claims a leading USA role in the future of the global commons 'cyberspace'. Three national policy objectives are discussed: strengthening partnerships, defense (dissuasion and deterrence), and economic and technical development (innovation). The section policy priorities (p.17–24), provides a set of (not SMARTly stated) action lines for departments and agencies.

The international strategy promotes an open and interoperable, secure, and reliable cyberspace that "supports international trade, strengthens international security, and fosters free expression and innovation" (p.8). A set of guidance principles or 'cyberspace norms' are proposed. These include both traditional principles (upholding fundamental freedoms, respect to property, valuing privacy, protection from crime, and the right of self-defence) and emerging cyber principles (global interoperability, network stability, reliable access, multi-stakeholder governance, and cyber security due diligence).

The USA assumes other nations and international stakeholders to align their cyber security strategies to align with this view on the global commons. As discussed in Section 3 above, at least a definition of cyber security is required to align the mutual understanding of international partners. A harmonised definition would even be preferable. The (THW, 2011) strategy, however, lacks definitions of terms like cyber

security and cyberspace. However, when developing a NCSS, TWH (2011) may help to align one's own national strategy with this international vision.

8 Proposed structure for a NCSS

Given the global nature of cyber security, nations can and should learn from each others' NCSS approaches. Each nation may have different cultural, legal, and political backgrounds and the intended audience of a national strategy may be quite diverse as well: for instance government policy makers and agencies, CI operators, the public, and foreign nations. Therefore, it is quite natural that national strategies will differ. However, as NCSS attempt to address a global risk in a connected world, one could expect similar sections and elements in the 19 NCSS. As discussed in the previous sections, each of the NCSS lack certain elements found in the other NCSS.

Moreover, some NCSS mix vision, guidance principles, strategic objectives and the more operational actions. Based upon the analysis of the 19 NCSS, we recommend the following structure of a NCSS:

1 Executive summary.

2 Introduction.

3 Strategic national vision on cyber security.

4 Relationship of the NCSS with other strategies, both national and international, and existing legal frameworks.

5 Guidance principles.

6 Relationship with other strategies, both national and international, and existing legal frameworks.

7 Cyber security objective(s), preferably one to four.

8 Outline of the tactical action lines.

9 Glossary, preferably based on an international harmonised set of definitions.

10 [Optional] Annex. Envisioned operational activities defined in a SMART way.

Depending on the intended audience and national customs, the NCSS sections can be interlarded with incident descriptions, statistics, and supporting quotes by key politicians and captains of industry. This contributes to awareness and underlines the importance and relevance. In case a nation decides to include a threat and risk assessment or a SWOT analysis alike MoICT (2011), it can either be inserted between the introduction and the strategic national vision on cyber security, or as a separate annex. The latter probably is better, as it would reflect the difference between (strategic) analysis and strategy.

9 Conclusions and recommendations

In this paper we have compared and analysed 19 NCSS from 18 nations. Comparing the 19 NCSS, major differences in approaches stemming from the differences in starting

points are found: economics, national security, or military defence. Many of the NCSS are unclear about the relationship of the NCSS with existing national and international policies such as about CIP, the European Digital Agenda, and a national security policy.

Only eight nations have defined the notion cyber security. The other ten nations either use descriptive text in their NCSS or a kind of common public understanding. This may cause misunderstandings nationally and internationally. As nations lack a harmonised cyber terminology, they might be hampered in collaboratively addressing the global threats to cyber space. Moreover, nations have a different understanding of the scope of what cyber security is supposed to cover: internet connected systems only or the whole of ICT. The first approach is considered harmful as nations following the internet security approach unwillingly will neglect the protection of not (yet) internet-connected ICT domains, which by the way may be connected to other public networks. Examples are process control systems in CI and non-CI, and medical systems.

All nations state in their NCSS the international threats and the risk of cyberspace. Nevertheless, the NCSS are relatively weak when describing detailed action plans under the topic 'international collaboration'. International topics such as harmonisation activities across international borders, collaborative acceleration of international response to cyber crime and other disturbances, and the tracing of cyber criminals do not seem to be on the priority lists of the nations. Given the ever growing relevance of ICT for the economy and society as a whole, the threats and the cyber security trouble most nations experience on a daily basis, a more aggressive approach and leadership would be expected, especially from the EU nations. In May 2011, the US issued their international strategy for cyberspace (THW, 2011) and asked other nations to endorse the guiding principles, to harmonise legal approaches,[2] to build and enhance military alliances to 'confront potential threats in cyberspace', and to work on the governance issues. No clear embracing by nations of this proposal has been found, however.

Most NCSS lack a dynamic approach to cyberspace (technological) threats and challenges; only the UK mentioned electromagnetic spectrum threats to cyberspace (CO, 2009). Emerging cyber security threats are only explicitly addressed by Germany and Japan in their NCSS, where the innovation cycle of ICT is high causing a fast appearance of new security risk.

When it comes to tactical and operational plans, only three nations use some of the SMARTness criteria. Interestingly, Uganda uses a system of metrics for the current state, the midway milestone, and the end result. Whether a strategy is a success or not, and whether the action plan is on the right track, cannot be measured when SMART criteria lack. Given the global threat, sense of urgency and the need for swift action, transparency is required for all stakeholders. Therefore, we recommend a SMART definition for all NCSS action lines and planned activities. Nations could implement a dashboard, including metrics related to dependence/relevance and to changing threats.

Most NCSS recognise the need for a society-wide approach: citizens, businesses, the public sector, and the government. However, the set of actions aimed at citizens is most often limited to awareness campaigns and information security education at schools. Only Australia has an outreach programme which supports the citizens with national cyber security tools. ISPs take a major role there, whereas that is hardly the case in other nations. This also shows that most nations underrate the risk of loss of public confidence in ICT which may seriously hamper economic prosperity and e-government plans.

We recommend nations that plan to develop a NCSS to consider the analyses and findings in this paper. Section 8 contains an outline for a NCSS that can be used for structuring a NCSS which addresses all relevant topics.

References

AG (2009) *Cyber Security Strategy*, Office of the Attorney General, Australia, available at http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity#h2strategy (accessed on May 5, 2012).

BMI (2011a) *Cyber Sicherheitsstrategie für Deutschland*, Bundesministerium des Innern, Berlin, Germany, available at http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile (accessed on May 5, 2012).

BMI (2011b) *Cyber Security Strategy for Germany*, Federal Ministry of the Interior (Bundesministerium des Innern), Berlin, Germany, available at http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Sicherheit/css_engl_download.pdf?__blob=publicationFile (accessed on on May 5, 2012).

CO (2009) *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*, Cabinet Office, London, UK, available at http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf (accessed on May 5, 2012).

CO (2011) *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, Cabinet Office, London, UK, available at https://update.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf (accessed on May 5, 2012).

CoE (2001) *Convention on Cybercrime*, Council of Europe, ETS No. 185, available at http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm (accessed on May 5, 2012).

Derrick, L. (2011) Available at http://lafiga.firedoglake.com/2011/06/03/finally-an-intelligent-use-for-cupcakes-hacking-terrorist-sites (accessed on May 5, 2012).

DIT (2011) *Discussion Draft of National Cyber Security Policy Version April 6, 2011*, Department of Information Technology, Ministry of Communications and Information Technology, New Delhi, India, available at http://www.mit.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf (accessed on May 5, 2012).

DSS (2010) *Draft Cyber Security Policy of South Africa*, in Annex to Government Gazette/Staatskoerant, Vol. 536, No. 32963, Department of State Security, Republic of South Africa/Republiek van Suid-Afrika, Pretoria, South Africa, available at http://www.info.gov.za/view/DownloadFileAction?id=118895 (accessed on May 5, 2012).

DSS (2012) *11 March 2012 Statement on the Approval by Cabinet of the Cyber Security Policy Framework for South Africa*, Department of State Security, Pretoria, South Africa, available at http://www.info.gov.za/speech/DynamicAction?pageid=461&sid=25751&tid=59794 (accessed on May 5, 2012).

EC (2008) *Council Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection*, European Commission, Brussels, Belgium, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF (accessed on May 5, 2012).

EC (2009) *Protecting Europe from Large-Scale Attacks and Disruptions: Enhancing Preparedness, Security, and Resilience – COM(2009)149*, European Commission, Brussels, Belgium, available at http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf (accessed on May 5, 2012).

EC (2010) *A Digital Agenda for Europe – COM(2010)245 Final/2*, European Commission, Brussels, Belgium, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R(01):EN:NOT (accessed on May 5, 2012).

ENISA (2012) *National Cyber Security Strategies*, European Network and Information Security Agency, Heraklion, Greece (ENISA), available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport (accessed on June 21, 2012).

GdE (2011a) *Estrategia Española de Seguridad: Una responsabilidad de todos*, Gobierno de España, Madrid, Spain, available at http://www.lamoncloa.gob.es/NR/rdonlyres/D0D9A8EB-17D0-45A5-ADFF-46A8AF4C2931/0/EstrategiaEspanolaDeSeguridad.pdf (accessed on May 5, 2012).

GdE (2011b) *Spanish Security Strategy: Everyone's Responsibility*, Gobierno de España, Madrid, Spain, available at http://www.cidob.org/en/content/download/27940/337722/file/EES_eng.pdf (accessed on May 5, 2012).

GGDL (2011) *Stratégie Nationale en Matiére de cyber Sécurité*, Le Gouvernement du Grand-Duché de Luxembourg, Luxembourg, Luxembourg, available at http://www.gouvernement.lu/salle_presse/actualite/2011/11-novembre/23-biltgen/dossier.pdf (accessed on May 5, 2012).

HMG (2009) *The National Security Strategy Update 2009: Security for the Next Generation*, HM Government, London, UK, available at http://www.official-documents.gov.uk/document/cm75/7590/7590.pdf (accessed on May 5, 2012).

HMG (2010) *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, HM Government, London, UK, available at http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy (accessed on May 5, 2012).

ISPC (2006) *The First National Strategy on Information Security: Towards the Realization of a Trustworthy Society*, Information Security Policy Council, Tokyo, Japan, http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf (accessed on May 5, 2012).

ISPC (2009) *Information Security Strategy for Protecting the Nation*, Information Security Policy Council, Tokyo, Japan, available at http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf (accessed on May 5, 2012).

KSK (2008a) *Küberjulgeoleku Strateegia 2008–2013*, Küberjulgeoleku strateegia komisjon, Kaitseministeerium, Tallinn, Estonia, available at http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013.pdf (accessed on May 5, 2012).

KSK (2008b) *Cyber Security Strategy*, Cyber Security Strategy Committee, Ministry of Defence, Tallinn, Estonia, available at http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf (accessed on May 5, 2012).

LRV (2011a) Electroninės Informac ijos Saugos (Kibernetinio Saugomo) Plėtros 2011–2019 Metais Programa, 2011 m. birželio 29 d. nutarimu Nr. 796, Lietuvos Respublikos Vyriausybės, Vilnius, Lithuania, available at http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_bin?p_id=403385 (accessed on May 5, 2012).

LRV (2011b) Resolution No 796 of 29 June 2011 on the Approval of the Programme for the Development of Electronic Information Society (Cyber-Security) for 2011–2019, Lietuvos Respublikos Vyriausybės (Government of the Republic of Lithuania), Vilnius, Lithuania, Available from: http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf (accessed on May 12, 2012).

Luiijf, H.A.M. (2008) 'Cyberterrorisme', in Muller, E.R., Rosenthal, U. and De Wijk, R., (Eds.): *Terrorisme: Studies Over Terrorisme en Terrorismebestrijding*, Kluwer, Deventer, Netherlands, pp.149–168.

Markoff, J. and Kramer, A.E. (2009) *US and Russia Differ on a Treaty for Cyberspace*, New York Times, June 29, 2009, available at http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all (accessed on May 26, 2012).

MinDef (2012) *Defensie Cyber Strategie*, Ministerie van Defensie, The Hague, The Netherlands, available at http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brochures/2012/06/27/brochure-defensie-cyber-strategie/brochure-defensie-cyber-strategie.pdf (accessed on June 27, 2012).

MinV&J (2011a) *De Nationale Cyber Security Strategie: Slagkracht Door Samenwerking*, Netherlands Ministry of Security and Justice, The Hague, The Netherlands, available at http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/02/22/nationale-cyber-security-strategie-slagkracht-door-samenwerking/de-nationale-cyber-security-strategie-definitief.pdf (accessed on May 5, 2012).

MinV&J (2011b) *The National Cyber Security Strategy (NCSS): Success Through Cooperation*, Netherlands Ministry of Security and Justice, The Hague, Netherlands, available at http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011 (accessed on May 5, 2012).

MoED (2011) *New Zealand's Cyber Security Strategy*, Ministry of Economic Development, New Zealand, available at http://www.med.govt.nz/upload/New%20Zealands%20Cyber%20Security%20Strategy%20June%202011.pdf (accessed on May 5, 2012).

MoI (2011a) *Strategii pro Oblast Kybernetické Bezpečnosti České Republiky na Období 2011–2015)*, Ministry of Interior, Prague, Czech Republic, available at https://moodle.unob.cz/pluginfile.php/15153/mod_resource/content/3/STRATEGIE_Strategie%20pro_oblast_KB%204.pdf (accessed on May 5, 2012).

MoI (2011b) *Cyber Security Strategy of the Czech Republic for the 2011–2015 Period* (*Strategii pro Oblast Kybernetické Bezpečnosti České Republiky na Období 2011-2015*), Ministry of Interior, Prague, Czech Republic, available at http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF (accessed on May 5, 2012).

MoICT (2011) *National Information Security Strategy*, Ministry of Information and Communication Technology, Republic of Uganda, available at http://www.ict.go.ug/index.php?option=com_docman&task=doc_download&gid=49&Itemid=61 (accessed on May 5, 2012).

MSCI (2011) *Strategia de Securitate Cibernetică a României*, 23 May 2011, Bratislava, Romania, available at http://www.mcsi.ro/Transparenta-decizionala/21/Strategie_Cyber_23052011 (accessed on May 5, 2012).

PSC (2010a) *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*, Public Safety Canada/Sécurité publique Canada, Ottawa, Canada, available at http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf (accessed on May 5, 2012).

PSC (2010b) *Stratégie de Cybersécurité du Canada: Renforcer le Canada et Accroître sa Prospérité*, Public Safety Canada/Sécurité publique Canada, Ottawa, Canada, available at http://www.securitepublique.gc.ca/prg/ns/cbr/ccss-scc-fra.aspx (accessed on May 5, 2012).

Rauscher, K.F. and Yashenko, V. (Eds.) (2011) *Critical Technology Foundations*, EastWest Institute, London, available at http://www.ewi.info/system/files/reports/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20%282%29.pdf (accessed on May 5, 2012).

SGDN (2008) *Défense et Sécurité nationale: Le Livre Blanc*, Secrétariat général de la défense et de la sécurité nationale, Paris, France, available at http://www.livreblancdefenseetsecurite.gouv.fr/IMG/pdf/livre_blanc_tome1_partie1.pdf (accessed on May 5, 2012).

SGDN (2011a) *Défense et Sécurité des Systèmes D'information: Stratégie de la France, Paris, France*, Secrétariat général de la défense et de la sécurité nationale, available at http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf (accessed on May 5, 2012).

SGDN (2011b) *Information Systems Defence and Security: France's Strategy*, Secrétariat général de la défense et de la sécurité nationale, Paris, France, available at http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf (accessed on May 5, 2012).

TWH (2003) *The National Strategy to Secure Cyberspace*, The White House, USA, http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (accessed on May 5, 2012).

TWH (2010) *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, The White House, Washington DC, USA, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed on May 5, 2012).

TWH (2011) *International Strategy for Cyberspace*, The White House, Washington DC, USA, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed on May 5, 2012).

UN (2011) International code of conduct for information security, Annex to letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General United Nations, United Nations, New York, USA, available at http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/66/359&Lang=E (accessed on June 2, 2012).

VBS (2012) *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken*, Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport, Switzerland, available at http://www.news.admin.ch/NSBSubscriber/message/attachments/27333.pdf (accessed on June 28, 2012).

Wikipedia (2012) available at http://en.wikipedia.org/wiki/Strategy (accessed on June 2, 2012).

Notes

1 The abbreviated country codes stem from the ISO 3166-1 alpha-3 code set.

2 Lithuania mixed its vision with a set of SMART performance criteria.