2016

Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy

Riza Azmi
University of Wollongong, ra873@uowmail.edu.au

William Tibben
University of Wollongong, wjt@uow.edu.au

Khin Than Win
University of Wollongong, win@uow.edu.au

Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy

Riza Azmi
School of Computing and Information Technology
University of Wollongong
Northfields Ave, Wollongong NSW 2522
Email: ra873@uowmail.edu.au

William Tibben
School of Computing and Information Technology
University of Wollongong
Northfields Ave, Wollongong NSW 2522
Email: wjt@uow.edu

Khin Than Win
School of Computing and Information Technology
University of Wollongong
Northfields Ave, Wollongong NSW 2522
Email: win@uow.edu

Abstract

Defining the factors that give rise to National Cyber Security Strategy (NCSS) has the potential to better understand information security in a global context. Considering the large number of countries that have developed NCSS, the paper seeks to define common motives that enable NCSS development to be understood as public policy phenomenon. In order to achieve this, the paper employs qualitative coding to review the NCSS of 54 countries. *Descriptive coding* is used to distill common motives, and then *pattern coding* is employed to develop themes as a way to explain the development and adoption of cyber security strategies by governments. The themes are *National Security*, *Jurisprudence*, and *Politics*. Enabling greater clarity in the motives that lead to cyber security strategies provides policymakers and scholars with additional insights into the development of initiatives that aim to take advantage of the opportunities presented by cyberspace while mitigating its security threats.

Keywords Cyber Space, Cyber Security, Cyber Security Strategy, Cyber Security Strategy Motives, National Cyber Security Strategy, Information Security.

1 Introduction

The socio-technical factors that shape the effectiveness or otherwise of security policies has been the focus of information systems (IS) research. Examples of this can be found in developing information security policy that seeks to define an effective information security policy requirement in an organisation (Flowerday and Tuyikeze 2016). One little-explored aspect to the social-technical dimensions of information security policies, however, are the effects that national policies play in shaping the information security environment. Described more generally as national cyber security strategy (NCSS) the factors that lead to its development are arguably a powerful shaping force that enables information security to be understood as a global phenomenon.

Given the pervasive nature of information and communication technology (ICT) throughout the world an ongoing issue for policy makers is to how best define cyber security strategy that works for the benefits of government, industry and civil society. An effective cyber security strategy seeks to balance accepted norms of a country with the opportunities presented by the internet. On the one hand, the internet, as a key enabler of cyberspace, is considered a disruptive technology that calls into question many accepted norms in military affairs, public policy, business and civil society (Lyytinen and Rose 2003). On the other hand, Government must balance this concern with the nature of the internet which is to preserve the openness and free flow of the information (Arsneault et al. 2005; OECD 2012). This condition may have considerable implications for country's future. While a strict security policy ensures stability, it may also reduce the potential benefits of the information age (Arsneault et al. 2005).

With the proliferation of NCSS it has become increasingly difficult to perceive an overall understanding of cyber security development as a public policy phenomenon. For example, the Cooperative Cyber Defence Centre of Excellence (CCDCOE 2015) and the European Network and Information Security Agency (ENISA 2013) note that there are more than 50 countries that have developed their own National Cyber Security Strategy (NCSS) (Klimburg 2012). Given the various motives and the range of NCCS, it is necessary for this research to pose the question "*why do countries create their National Cyber Security Strategy (NCSS)?*". To that end, the research strives to understand motives behind the creation of cyber security strategy to enable a better understanding of the NCSS as a shaping force in a nation's information security environment.

2 NCSS: Definition and Challenge

2.1 Definition

The history of the term "*cyberspace*" stretches back over many decades. The term "*cyber*" emerged seven decades ago (Ottis and Lorents 2010). Wiener (1948, pp. 144–154) coined the term "*cybernetics*" to describe "*interactions between humans (or animals) with a machine that can provide an alternative environment*". The term "*cyberspace*" was first used in early 1980's which described as "*a graphic representation of data abstracted from banks of every computer in the human system.*" (Gibson 1984). Since then, the term has entered common usage, including the study of information system's study (Ottis and Lorents 2010).

Often, the definition of *cyber security* and *information security* are used interchangeably (E. Luiijf et al. 2013, p. 6). However, von Solms and van Niekerk (2013) attempts to clarify differences between these two terms. *Information security* deals with the protection of information as an asset, in physical or non-physical form; whereas, *cyber security* deals with the protection of with both informational and non-informational assets through the ICT infrastructure (von Solms and van Niekerk 2013). From an information systems perspective, this division appears as a misleading one when considering the work of information systems professionals. This is because the information assets that von Solms and van Niekerk (2013) seek to distinguish from infrastructure is, in reality, part and parcel of such infrastructure. In much the same way information systems may be essential to running a banking enterprise such systems are also fundamental to ensuring the proper working of a dam or power station as amply demonstrated by the software worm Stuxnet that was used to disrupt the Iranian nuclear program (Shakarian et al. 2013).

Bearing in mind that the distinction that von Solms and van Niekerk makes does have some veracity, we define National Cyber Security Strategy (NCSS) as "*a careful plan or method of protection both informational and non-informational assets through the ICT infrastructure for achieving a particular national goals usually over a long period of time*" (E. Luiijf et al. 2013; Merriam-Webster 2016a; von Solms and van Niekerk 2013). Using this definition, it can be understood that the NCSS seeks to address a nation's goals which have implications for its government, businesses and civil society.

2.2 Challenges on Creating NCSS

The broader motivations for NCSS development appertain to a number of factors namely: the nature of the internet, stakeholder representation, cyberspace borders, and dynamic changes. While NCSS should seek to preserve the openness and free flow of information of the internet, it should not undermine the national interest (Klimburg 2012, pp. 35–42; OECD 2012). Inevitably, creating the NCSS requires issues of economics, politics, culture and international relations to be balanced with internet-age ideals of openness and free information flow (Arsneault et al. 2005; Klimburg 2012, pp. 35–42; OECD 2012). One does not need to look too far to find a nexus between cyber security and tensions in international relations. For example, the Stuxnet attack mentioned previously was judged to be a US state-sponsored attack designed to upset Iran's nuclear program as well as its leadership. Tension between Australia and Indonesia in 2013 over Australia's National Security Agency's monitoring of phone calls by Indonesian politicians and their families is another example. (Reddick et al. 2015). While countries that limit the free information flow attempts to ensure political stability, they potentially reduce benefits that can be gained in the information age (Arsneault et al. 2005).

Another challenge in defining cyber security strategy is how to achieve representation for all parts of society ranging from the private sector to government to civil society (Klimburg 2012; E. Luiijf et al. 2013). From a government's perspective, there are benefits in creating e-government services in the delivery of services as well as improving their government capacity (Stier 2015). Civil society has been an active user of cyber space to coordinate action leading to the slogan "*think globally, act locally*". The ability to maintain anonymity and confidentiality makes the Internet a potentially transformative medium (Seebruck 2015), such as in political activism (Al-Rawi 2014). The private sector's use of cyberspace to enable electronic transactions, promotes e-commerce, e-banking, and e-advertising (Porter 2001). Therefore, cyber security strategy needs to account for varied and legitimate use while ensuring criminal activity is kept in check (Souza 2013).

One key challenge in creating cyber security strategy is defining borders in cyber space. Borders are important in delineating jurisdictions in which law is enforced (Johnson and Post 1996). Depending on which lens is adopted different sets of boundaries are brought into focus, and, by implication, different perceptions of jurisdictions (Cottim 2008; Finklea 2012; Johnson and Post 1996; Motlagh 2015). Some argue that cyberspace should remain borderless in which no one should claim or rule cyberspace on the basis that no physical interactions take place (Barlow 1996; Johnson and Post 1996). However, globalisation and technology has fostered the change on viewing the jurisdiction and border not only based on the geographical boundary but across the national border (Finklea 2012). Therefore, several conventional jurisdictions, such as territorial jurisdiction, personality jurisdiction, extraterritorial jurisdiction, universal jurisdiction, and "*turf*" *boundary*", are proposed which may be applied in seeking the cyberspace jurisprudence (Cottim 2008; Finklea 2012; Tehrani and Manap 2013). Owing to these different interpretations cyber security strategy needs to deal with defining an appropriate context in which security can be effectively addressed.

The last challenge in developing cyber security strategy seeks to deal with changing environments. The internet, as a key enabler of cyberspace, is considered a disruptive technology (Lyytinen and Rose 2003) that calls into question many accepted norms in military affairs, public policy, business and civil society. Developing a strategy to address the uncertainty of innovation is not straightforward. There is a challenge of creating a good strategy within the uncertainty of disruptive technological change. Thus, the cyber security strategy needs to account for future innovations inside the cyberspace.

In summary, countries generally need NCSS to secure their national cyberspace. However, defining NCSS has challenges. First, there are various perspectives when defining cyber security (E. Luiijf et al. 2013). Second, some aspects need to be considered by the government, such as internal and external environment (GCSCC 2014; ITU 2012). Considering there are different challenges posed by every country, there is a need to better define the motives that lead to the creation of NCSS.

3 Methodology

This research uses the grounded theory paradigm to synthesise motives behind cyber security strategy throughout the world. Grounded theory aims to generalise concepts (and theory) from empirical results (Saldaña 2009; Scott and Glaser 1967). Figure 3-1 shows the steps taken in this paper to synthesise national cyber security strategy (NCSS) documents.

The first phase described our response to the research question: *why do countries create National Cyber Security Strategy (NCSS)?*, which was to collect the relevant literature using our defined search strategy (NVIVO 2015; Saldaña 2009). The search strategy included the keywords "National Cyber Security Strategy/Policy <Country>", "Information Security Strategy/Policy <Country>", "Digital

Security Strategy/Policy <Country>" followed by the Country specifics on the search engines Google and DuckDuckGo. The main source of NCSSs were found from CCDCOE's and ENISA's website (CCDCOE 2015; ENISA 2013). We applied inclusion and exclusion criteria in our literature classification. Primary documents that related to strategy documents referring to cyber space such as, for example, national security strategies and national security doctrines were included. Due to resource limitations we excluded literature that was not in English. The task of ensuring accurate translations of non-English documents into English was beyond available resources for this research.

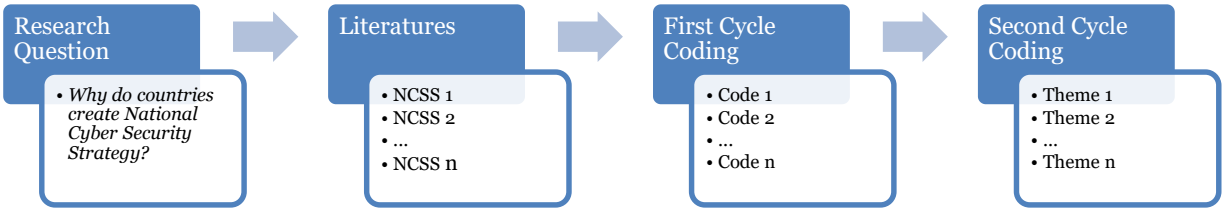

Figure 3-1 A Streamlined of the Research adapted from (NVIVO 2015; Saldaña 2009)

The application of the literature search yielded 64 NCSS from 54 countries (see Table 3-1). Literature classification sometimes yielded two different examples of NCSS from the one country (i.e. Austria, Netherland, Russia, United Kingdom, and the United States). Publication dates of these documents ranged from 2003-2015.

Table 3-1 List of Countries

Asia	Africa	Europe
Afghanistan (Wafa 2014) – AFG Bangladesh (BG 2014) – BGD Israel (PMO 2011) – ISR India (MCIT 2013a) – IND Japan (GoJ 2015) – JPN Jordan (MICT 2012) –JOR Pakistan (Syed 2014) –PAK Qatar (MICT 2013) –QAT Republic of Korea (MOND 2009) – ROK Russian Federation (MoD 2011; PRF 2000; RF 2013) – RUS Saudi Arabia (MCIT 2013b) – SAU Singapore (IDA 2013) – SGP Turkey (MTMAC 2013) –TUR	Egypt (MCIT 2012) – EGY Ghana (MOC 2014) – GHA Kenya (MICT 2014) – KEN Mauritius (MTCI 2015) – MUS Morocco (MCINET 2013) – MAR Nigeria (SSS 2014a, 2014b) – NGA South Africa (GoSA 2011) – ZAF Uganda (NITA-U 2014) –UGA **America** Brazil (MoD 2012b) – BRA Canada (GoC 2013; MPS 2010) – CAN Colombia (NCESP 2011) – COL Trinidad & Tobago (IMCCS 2012) – TTO United States of America (DoD 2015; WH 2003; WH 2011)– USA **Oceania** Australia (AG 2009) – AUS New Zealand (NZG 2011) – NZL	Austria (BKA 2012, 2013) – AUT Belgium (ACOS STRAT 2014) – BEL Czech Republic (NCKB 2015) – CZE Croatia (Skendžić 2014) – HRV Cyprus (OCECPR 2012) – CYP Estonia (MEAC 2014) – Lithuania (GoL 2011) – LTU Montenegro (GoM 2013) – MNE Netherlands (MoD 2012a; NCSC 2013) – NLD Norway (GARCIA 2012) – NOR Poland (MADISA 2013) – POL Serbia (MOD 2010) – SRB Slovakia (GoS 2008) – SVK Spain (DOND 2013) – ESP Sweden (GS 2015) – SWE Switzerland (DOD 2012) – CHE United Kingdom (HMG 2010) – GBR

To synthesise the information in these documents two phases of coding followed – *first cycle coding;* and the *second cycle coding*. Qualitative coding generally seeks to establish an analytic process with a progressive refinement that is transparent and repeatable (Saldaña 2009, p. 45). This study adopted an approach called "*descriptive coding*" for its first cycle coding method and "*pattern coding*" for its second cycle coding method (Saldaña 2009). Descriptive coding as a first cycle coding method is distinguished by the use of individual words (nouns) or short phrases from the literature to create topics that are used to characterise tracts of qualitative data (Saldaña 2009, p. 70). This process of coding is repeatable which is refined several times until codes describe the specific common concept. Pattern coding in the second cycle is distinguished by techniques that explain or infer an emergent theme in the data (Saldaña 2009, p. 152). It aims to transform understanding of contextual data into generalised concepts (Saldaña 2009). In order to synthesise a large amount of data into particular concepts, the research used NVIVO™. NVIVO™ is a software tool that assists in connecting concepts and perceived patterns that emerge.

4 Findings

Motives that lead to the creation of NCSS are arguably most fundamental to understanding why countries develop an NCSS. In this section, we describe our findings that synthesise the 64 documents from 54 countries. Findings are presented as two steps (Saldaña 2009). First cycle codes and their

definitions are presented using *descriptive codes* (Section 3.1). These codes will then be abstracted into themes using *pattern codes* (Section 3.2).

4.1 First Cycle Coding

Each of the reviewed NCSS documents generally describes a national cyber security vision, pre-requisite conditions, assumptions, and background that articulate unique attributes of each country's cyber security strategy. In seeking to develop codes that enable description of these diverse motives nine codes were advanced: *(1) Reducing Cyber Threats, (2) Economic Security, (3) Required by other policy instruments, (4) Strengthening National Resiliency, (5) Political Imperative, (6) Lawful Mandate, (7) Protecting State Secrets, (8) Strengthening Diplomacy,* and *(9) Increasing Country Image*. Table 4-1 summarises these codes, their definition and associated countries.

Table 4-1 Coding Summary and Definitions of Cyber Security Motives by Countries

Coding	Aims of Motive/Countries*	#
Reducing Cyber Threats	**Definition:** *reducing the malicious conduct exercised in cyberspace that has possibility of action, or capacity to produce a cyber-attack* (MOD 2013; NCESP 2011; PCM 2013).	46
	Countries: AFG, AUS, BGD, BEL, CAN, CZE, COL, CYP, EGY, EST, FIN, FRA, GEO, DEU, GHA, ISL, IND, IRL, ISR, ITA, JPN, JOR, KEN, LVA, LTU, MUS, MNE, NLD, NZL, NGA, NOR, PAK, POL, QAT, RUS, RWA, SAU, SRB, ZAF, PRK, CHE, TTO, TUR, UGA, GBR, USA	
Economic Security	**Definition:** *an act of ensuring the confidence and trust of digital transaction in cyber space, and protecting the structure of national economy in the digital realm* (AG 2009; MICT 2012; MPS 2010; NCKB 2015; SGDSN 2015; WH 2003)	35
	Countries: AFG, AUS, AUT, BGD, CAN, CZE, COL, HRV, CYP, FIN, FRA, DEU, GHA, ISL, IND, IRL, ITA, JPN, JOR, KEN, LVA, MNE, MAR, NLD, NZL, NGA, NOR, POL, QAT, RUS, ZAF, ESP, TUR, GBR, USA	
Required by other policy instruments	**Definition:** *an official order to do something, which may be derived based on previous national agenda such as National Security Strategy, National Roadmap, formal request, or assessment.*	23
	Countries: AUT, COL, CYP, FIN, ISR, ITA, JPN, KEN, NLD, NGA, POL, QAT, RUS, SAU, SVK, ZAF, PRK, ESP, CHE, TTO, TUR, UGA, USA	
Strengthening National Resiliency	**Definition:** *an act to maintain the integrity of the uninterrupted operation and resilience of vital ICT services that have major importance and devastating impact to public at national level* (BMI 2011; GARCIA 2012; IMCCS 2012; MEAC 2014; MOC 2014; MTMAC 2013; SA 2011)	17
	Countries: AUS, CZE, COL, HRV, FRA, GHA, JPN, NLD, NZL, RUS, RWA, SAU, SVK, ZAF, PRK, SGP, CHE, USA	
Political Imperative	**Definition**: *political imperative may be viewed as a broad rationale that incorporates the national interest (i.e. promoting national values, keeping country's prosperity) or political situation (asserting democratic values, guaranteeing human rights, or ensuring free flow of information).*	20
	Countries: AUS, AUT, BGD, CAN, CZE, COL, EST, FRA, ITA, JPN, KEN, LTU, NLD, NZL, QAT, RUS, RWA, TUR, GBR, USA	
Lawful Mandate	**Definition:** *a condition of having an authoritative legal mandate to enforce law in cyber space.*	10
	Countries: COL, GHA, IND, MUS, NZL, NGA, PAK, RUS, TTO, TUR	
Protecting State Secrets	**Definition:** *the national information whose unauthorised disclosure could endanger national security*, adapted from Merriam-Webster (2016b).	7
	Countries: CZE, COL, JPN, NLD, NZL, RWA, ESP	
Strengthening Diplomacy	**Definition:** *the art and practice of conducting negotiations between nations* (Merriam-Webster 2016c)	5
	Countries: BEL, GEO, NLD, RUS, USA	
Increasing Country Image	**Definition:** *an impression of country looks or might look that presents to public*	3
	Countries: GHA, JPN, TTO	

**Country abbreviation is based on three-letter country codes defined in ISO 3166-1*

Reducing Cyber Threats. A strong motivator to develop NCSS for the majority of countries is to address their vulnerability to cyber threats (N=46, see Table 4-1). The nature of these attacks may be sophisticated efforts sponsored by foreign governments or can be advanced by anonymous actors using cheap methods requiring little technical skills. Even so, these attacks can pose a great menace to a country, which is reflected in the high number of references to such cyber threats in country NCSS. These threats, can be categorized into two conditions: (1) stated-sponsored threat (i.e. cyber espionage, cyber terrorism, and cyber warfare), and (2) malicious activities (i.e. cyber-crime, hacktivism, large-scale attacks, mismatch technology, development and security) (DEA 2012; H. A. M. Luiijf et al. 2013; PCM 2013). Cyber-threats need not be limited to international terrorism but is often linked to internal political activities. For example, Kenya recognises the threat of hacktivism "*seeking to publicise*

political view" as a factor that may influence local political interactions (MICT 2014). Similarly, Qatar recognises the risks of cyber space in "*undermining social norms*" (MICT 2013).

Economic Security. As ICT has led to increasing growth in the digital economy (Jin and Cho 2015; Jorgenson and Vu 2016) issues of the national economy become entangled with cyber security. Therefore, most NCCS cite economic factors and the need to avoid potential disruptions to economic growth (N=35, see table 4-1). The protection of the digital economy includes factors, for example, such as: (1) ensuring the confidence and trust of digital transaction in cyber space, and (2) protecting the structure of national economy in the digital realm (AG 2009; MICT 2012; MPS 2010; NCKB 2015; SGDSN 2015; WHO 2003). Generating trust and confidence in cyberspace protection, may attracts potential investors to the country (DCENR 2015; MCIT 2013a). Another reason is to sustain and enhance an efficient and secure digital environment is to promote stable economic growth and development which has significant implications for a country's future prosperity (MPS 2010).

Required by Other Policy Instruments. The creation of NCSS is often required by other social policy instruments (N=23, see Table 4-1). For example, national security strategies often identify the need to develop NCSS given the threats that cyber space poses to national security (DOD 2012; MOND 2009). Other policy instruments are required by National Roadmaps to extend national plan in cyberspace such as ICT Master Plan, and National Development Plan (IMCCS 2012; MICT 2013, 2014; NCESP 2011; OCECPR 2012; WHO 2003). In both cases, it can be seen that there is a desire to align NCSS with security and national development plans. A third source from which NCSS is mandated is official reviews. Official reviews are often carried out as a risk mitigation exercise strategy against known security breaches. For example, the Polish government partly based their periodic reviews of incidents reported by Poland's Computer Emergency Response Team (CERT) (MADISA 2013). Finally, the development of NCSS can also be invoked from of a formal request from legislation, resolution or presidential decree (GoJ 2015; GoS 2008; MCIT 2013b; MOD 2013; PCM 2013)).

Strengthening National Resiliency. Strengthening resilience in cyber space is intended to maintain credible deterrents to cyber-attacks on national critical information infrastructure (CII). The CII represents a key enabler of vital ICT services that can have considerable knock-on effects should a cyber-attack prove successful (BMI 2011; GARCIA 2012; IMCCS 2012; MEAC 2014; MOC 2014; MTMAC 2013; SA 2011). Hence cyber-attacks on CII can have major national impacts leading this to become a significant motive for the creation of NCSS (N=18, see Table 4-1). In some countries, strengthening resiliency is aligned explicitly to improving defence capability representing a new area of military focus along with land, sea, and air. This is particularly evident in the NCSS of Belgium (ACOS STRAT 2014). Some countries use NCSS to address regional security tensions. For example, the Government of Georgia established their cyber security strategy after the Russian-Georgian war as a means to better engage military support for protection in cyberspace (DEA 2012). Similarly, South Korea and Japan demonstrate the use of NCSS to address regional tension in East Asia by creating rival cyber defence units (MOND 2009, pp. 18, 57).

Political Imperative. Political imperatives were discovered as a motive in the creation of NCSS in some countries (N=20, see Figure 4-1). These political imperatives seek to establish a political agenda for nations in cyberspace. For example, some countries outline an agenda that asserts the personal freedoms of citizens to enjoy access to information, freedom of expression as well as protection of human rights. For example, France seeks to establish national values and within cyber space in its NCSS (SGDSN 2015). Similar sentiments are expressed by other countries such as Japan, Russia, United States (GoJ 2015; WHO 2003).

Lawful Mandate. NCSS is used by countries to create a legal mandate in cyber space (N=10, see Figure 4-1). The underlining assumption is that cyberspace represents an extension in 'space' that requires protection. Therefore, the NCSS is aiming to provide a policy framework that enables legal authorities to take action such as monitoring suspicious activity, gathering evidence and prosecuting (MICT 2013).

Protecting State Secrets. While some governments see merit in developing ICT infrastructure to enhance public service through e-government initiatives, there is recognition that this also poses risks in protecting sensitive information assets (N=7, see Figure 4-1). Thus, NCCS functions to guide the development of technical standards as well as align technological systems. Two motivations are found to dominate: those seeking to make e-government service more accessible (GoM 2013; MoD 2012a; NCESP 2011) and another which seeks to protect valuable government information from stated-sponsored agency (i.e. cyber espionage), or from malicious activities (i.e. hacktivism) (GoJ 2015; GoR 2011; MED 2011).

Strengthening Diplomacy. Creating cyber security strategy can become a control centre for national diplomacy and security in cyberspace. Some countries see cyberspace as opening up new

opportunities for cyber diplomacy (BKA 2012; MoD 2012a) (N=5, see Figure 4-1). Cyber diplomacy aims to promote the peaceful use of the digital domain, strengthening partner relationship, or for conflict resolution (BKA 2012; NCSC 2013; WHO 2003). However, in other countries, having the NCSS is intended to create the cyber deterrence. Aligning military function with the cyber security strategy is envisioned to strengthen the military diplomacy (MOND 2009; WH 2011, p. 4).

Promoting Country Image. Similar to increasing diplomacy, sometimes the creation of NCSS is intended to promote a country's image (N=3, see Figure 4-1). Japan's (ISPC 2013) NCSS is partly designed to show an image of Japan's advanced cyberspace capabilities as well as being secure to attract investors and promote trust .While some seek to promote their image others seek to counter a negative image through a NCSS. The notorious image of Ghana as a source for cybercrime and money laundering, is countered through their adoption of a NCSS (FATF 2015; MOC 2014).

By synthesising NCCS into several codes an understanding of the factors that have led to various NCSS can be seen. However, the range of codes now need to be distilled into themes, so that motives for NCS can be more generally understood. To provide this broad perspective of NCSSs, the next section will provide second cycle coding which uses "*pattern coding*".

4.2 Second Cycle of Coding: Themes of Cyber Security Strategy Motives

Second cycle of coding seeks to reorganise and reanalyse data from first cycle coding, by further synthesising data by fitting one category with another (Saldaña 2009). In this section we develop themes which are derived from codes defined in Section 4.1. We group codes by its common concept and its similarity of concept using pattern coding (Saldaña 2009). Figure 4-1 presents the themes of NCCS motives. The cyber security strategy motives may be explained in themes *National Security, Legal Remedy*, and *Politic*.

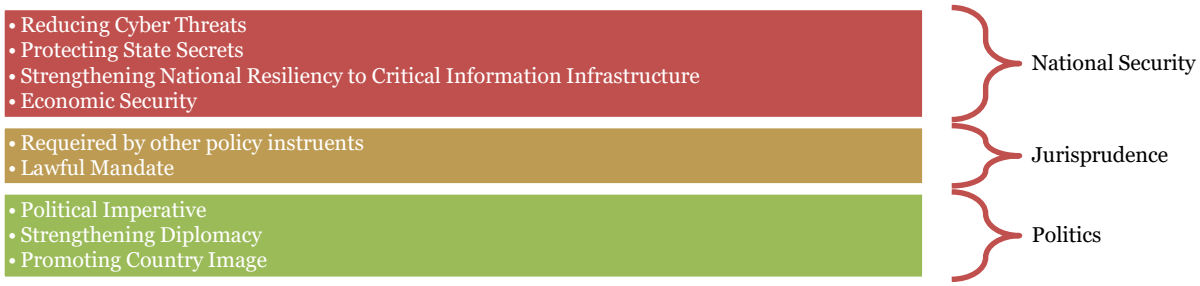

Figure 4-1 Coding Result – Cyber Security Motives, from Codes to Themes

issue of national security. The codes of *Reducing Cyber Threats*, *Protecting State Secrets*, *Strengthening National Resiliency*, and *Economic Security* all can be grouped together because the intention of NCSS is to protect the safety, economic interests and the well-being of citizens and national institutions both public and private.

Jurisprudence. The theme of jurisprudence addresses the need to create a credible legal foundation for governments to operate in cyberspace. The two codes of "*required by other policy instruments*" and "*Lawful Mandate*" both seek to define an appropriate legal context that enables legal authorities to reduce or eliminate actions in cyberspace that are harmful to a nation's interests through the use courts of law, international tribunals and the like.

Politics. The remaining motives of political imperative, strengthening diplomacy, and promoting country image, can be grouped under the theme of politics. Here it can clearly be seen that cyber security strategy is used to promote a political vision and philosophy at the strategic and leadership level. Cyberspace is viewed in this context as a way to communicate national values to a wider international context.

5 Discussion and Conclusion

5.1 NCCS Motives: from National Security, to Jurisprudence, to Politic

A wide spectrum of motives leading to the creation of NCSS has been recognized. Interestingly, these motives encompass more than the just obvious ones of national protection in cyberspace, but also jurisprudence and political will. Firstly, it is clear that for the great majority of countries the creation of NCSS underpins national security by countering cyber threats, protecting state secrets, strengthening national resiliency, or consolidating economic security. This motive is understandable since the internet is recognised for not only bringing advantages but also introducing distinguishable risks.

Accordingly, strengthening national security in cyberspace requires governments to deal with the nature of Internet technologies. This requires more than just dealing with currently known vulnerabilities but to also account for future innovations inside cyberspace.

The theme of jurisprudence outlines an important role for governments in regulating cyberspace. In view of the risks, governments view cyberspace as an extended jurisdictional space along with land, air, and sea which needs to be regulated to preserve national sovereignty. Jurisprudence in cyber space can take the form of the stand-alone laws or may be associated with other areas of policy such as in e-commerce, e-government and e-health. Inevitably, seeking jurisprudence is fraught with complexities, due to two reasons. *First,* defining borders and jurisdiction in cyberspace is the subject of multiple interpretations. While some argue that cyberspace should remain borderless (Barlow 1996), others argue that cyberspace is an extension of national sovereignty (Cottim 2008; Finklea 2012; Tehrani and Manap 2013). *Second,* cyberspace is intertwined with realities of life within countries meaning that internet-age ideals of openness and free information flow clash with the realities of economics, politics and culture when defining appropriate laws and regulations (Klimburg 2012, pp. 35–42; OECD 2012).

This leads to the third motive of the creation of cyber security strategy which are political ones. Political motives tend to develop from the perceptions of decision-makers and policy-makers which can change in response to prevailing circumstances, particularly perceived threats (Klimburg 2012, p. 50). NCSS development in this context needs careful consideration of implications that flow from NCSS to the national interest. Politics is therefore perceived as an overarching motive that influences other areas of NCSS.

In conclusion, the paper has outlined codes and themes of motives emerged from national cyber security strategies. Within the literature, the strategy becomes apparent: *national cyber security strategy* covers various perspectives on defining cyber security that are based on internal and external environment of the country called cyber security motives. Cyber security motives are the factors that lead to the creation of a nation's cyber security vision and include pre-requisite conditions, assumptions, and background that generates the unique attributes of cyber security strategy.

5.2 Limitation of Study

Although this study seeks to clarify the range of factors that motivate the creation of cyber security strategy, the findings should be considered tentative. Codes and themes were collected and developed from existing NCSSs. While done in accordance with Scott & Glaser's (1967) grounded methodology, the reliability of these themes becomes the subject for future research.

References

ACOS STRAT (Belgian Joint Staff, Strategy & International Relations Department). 2014. *Cyber Security Strategy for Defence*, Brussel, Belgium, Belgium: Belgian Joint Staff, Strategy & International Relations Department.

AG (Attorney General's Department of Australia). 2009. *Cyber Security Strategy*, Canberra, ACT: Attornet General's Department of Australia.

Al-Rawi, A. K. 2014. "Cyber warriors in the Middle East: The case of the Syrian Electronic Army," *Public Relations Review* (40:3), Elsevier Inc., pp. 420–428 (doi: 10.1016/j.pubrev.2014.04.005).

Arsneault, S., Northrop, A., and Kraemer, K. L. 2005. "Taking Advantage of the Information Age: Which Countries Benefit?," in *Handbook of Public Information Systems*G. D. Garson (ed.) (Second Edi.), Singapore: Taylor & Francis Ltd.

Barlow, J. P. 1996. "A Declaration of the Independence of Cyberspace," *EFF* (available at https://projects.eff.org/~barlow/Declaration-Final.html; retrieved December 5, 2015).

BG (Bangladesh Government). 2014. *The National Cybersecurity Strategy of Bangladesh*, Dhaka, Bangladesh: Bangladesh Government.

BKA (Bundeskanzleramt Austria). 2012. *National ICT Security Strategy Austria* (H. Markhardt, ed.), Vienna, Austria: Federal Chancellery of the Republic of Austria.

BKA (Bundeskanzleramt). 2013. *Austrian Cyber Security Strategy*, Vienna, Austria: Federal Chancellery of the Republic of Austria (BKA).

BMI (Bundesministeriums des Innern). 2011. *Cyber Security Strategy for Germany*, Berlin: Federal Ministry of the Interior (available at www.bmi.bund.de).

CCDCOE (Cooperative Cyber Defence Centre of Excellence). 2015. "Cyber Security Strategy Documents," *Cooperative Cyber Defence Centre of Excellence* (available at https://ccdcoe.org/strategies-policies.html; retrieved November 11, 2015).

Cottim, A. A. 2008. "Cybercrime , Cyberterrorism and Jurisdiction : An Analysis of Article 22 of the COE Convention on Cybercrime," *European Journal of Legal Studies* (17:3), pp. 81–103.

DCENR (Department of Communications, Energy & Natural Resources - Republic of Ireland). 2015. *National CyberSecurity Strategy 2015-2017: Securing our Digital Future*, Dublin, Ireland: Department of Communications, Energy & Natural Resources - Republic of Ireland.

DEA (Data Exchange Agency). 2012. *Cyber Security Strategy of Georgia 2012 - 2015*, Tbilisi, Georgia: Data Exchange Agency (DEA) - Georgia.

DOD (Federal Department of Defence Civil Protection and Sport DDPS National). 2012. *National strategy for the protection of Switzerland against cyber risks*, Switzerland: Federal Department of Defence, Civil Protection and Sport DDPS National - Switzerland.

DoD (Department of Defence). 2015. *The DoD Cyberstrategy*, Washington: Department of Defence - United States of America (doi: 10.1017/CBO9781107415324.004).

DOND (Department of National Defence). 2013. *National Cyber Security Strategy*, Madrid, Spain: Department of National Defence - Kingdom of Spain.

ENISA (European Union Agency for Network and Information Security). 2013. "National Cyber Security Strategies (NCSSs) Map," *European Union Agency for Network and Information Security* (available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/; retrieved November 11, 2015).

FATF (Financial Action Task Force). 2015. *International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations*, Paris, France: Financial Action Task Force (available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf).

Finklea, K. M. 2012. "the Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement.," *Journal of Current Issues in Crime, Law & Law Enforcement* (5:1/2), pp. 29–67.

Flowerday, S. V., and Tuyikeze, T. 2016. "Information security policy development and implementation: The what, how and who," *Computers & Security* (61), Elsevier Ltd, pp. 169–183 (doi: 10.1016/j.cose.2016.06.002).

GARCA (Government Administration Reform and Church Affairs). 2012. *Cyber Security Strategy for Norway*, Oslo, Norway: Norwegian Ministry of Government Administration Reform and Church Affairs.

GCSCC (Cyber Security Capacity Centre). 2014. *Cyber Security Capability Maturity Model (CMM)* (Version 1.), Oxford: Global Cyber Security Capacity Centre, University of Oxford (available at http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM Version 1_2_0.pdf).

Gibson, W. 1984. *Neuromancer* (T. Carr, ed.), New York: Ace Books.

GoC (the Government of Canada). 2013. *Action Plan 2010-2015 for Canada's Cyber Security Strategy*, Ottawa, Canada: the Government of Canada (available at http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf).

GoJ (the Government of Japan). 2015. *Cybersecurity Strategy (Provisional Translation)*, Tokyo, japan: The Government of Japan (available at http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf).

GoL (the Government of Republic of Lithuania). 2011. *Resolution No 796 of the Government of the Republic of Lithuania: The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-201*, Vilnius, Lithuania: The Government of The Republic of Lithuania.

GoM (the Government of Montenegro). 2013. *National Cyber Security Strategy*, Podgorica, Montenegro: The Government of Montenegro (available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS_ESen.pdf).

GoR (the Government of Rwanda). 2011. *National ICT Strategy and Plan NICI III* (2011-2015, ed.), Rwanda: the Government of Rwanda.

GoS (the Government of Slovak Republic). 2008. *National Strategy for Information Security in the Slovak Republic* (T. G. of T. S. R. (GoS), ed.), Slovak: the Government of The Slovak Republik.

GoS (the Government of Sweden). 2015. *Sweden's Defence Policy 2016 to 2020*, Stockholm, Sweden: the Government of Sweden.

GoSA (the Government of Republic of South Africa). 2011. *A National Cybersecurity Policy Framework for South Africa* (GoSA, ed.), the Government of Republic of South Africa.

HMG (the Her Majesty's Government). 2010. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, London: Her Majesty's Government (doi: Cm 7953).

IDA (Infocomm Development Authority). 2013. *National Cyber Security Masterplan 2018*, Singapore: Infocomm Development Authority of Singapore (doi: 10.1017/CBO9781107415324.004).

IMCCS (Inter-Ministerial Committee for Cyber Security). 2012. *Government of the Republic of Trinidad & Tobago National Cyber Security Strategy*, Trinidad & Tobago: Inter-Ministerial Committee for Cyber Security - the Republic of Trinidad & Tobago National.

ISPC (Information Security Policy Council of Japan). 2013. *Cybersecurity Strategy: Towards a World-Leading, Resilent and Vidorous Cyberspace*, Tokyo: Information Security Policy Council of Japan.

ITU (International Telecommunication Union). 2012. *ITU National Cybersecurity Strategy Guide* (F. Wamala, ed.), Geneva: International Telecommunication Union (available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs//ITUNationalCybersecurityStrategyGuide.pdf).

Jin, S., and Cho, C. M. 2015. "Is ICT a new essential for national economic growth in an information society?," *Government Information Quarterly* (32:3), Elsevier Inc., pp. 253–260 (doi: 10.1016/j.giq.2015.04.007).

Johnson, D. R., and Post, D. 1996. "Law And Borders: The Rise of Law in Cyberspace," *Stanford Law Review* (48:5), pp. 1367–1402.

Jorgenson, D. W., and Vu, K. M. 2016. "The ICT revolution, world economic growth, and policy issues," *Telecommunications Policy* (40:5), Elsevier, pp. 383–397 (doi: 10.1016/j.telpol.2016.01.002).

Klimburg, A. (Ed.). 2012. *National Cyber Security Framework Manual The NATO Science for Peace and Security Programme*, Tallin: NATO Cooperative Cyber Defence Centre of Excellence (doi: 9789949921119).

Luiijf, E., Besseling, K., and de Graaf, P. 2013. "Nineteen national cyber security strategies," *International journal of critical ...* (July 2015), pp. 2–31 (doi: 10.1504/IJCIS.2013.051608).

Luiijf, H. A. M., Besseling, K., Spoelstra, M., and De Graaf, P. 2013. "Ten national cyber security strategies: A comparison," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 6983 LNCS), pp. 1–17 (doi: 10.1007/978-3-642-41476-3_1).

Lyytinen, K., and Rose, G. M. 2003. "The disruptive nature of information technology innovations: The case of internet computing in systems development organizations," *MIS Quarterly: Management Information Systems* (27:4), pp. 557–595 (available at http://www.scopus.com/inward/record.url?eid=2-s2.0-9744227977&partnerID=tZOtx3y1).

MADISA (Ministry of Administration and Digitisation, Internal Security Agency). 2013. *Cyperspace Protection Policy of the Republic of Poland*, Warsaw, Poland: Ministry of Administration and Digitisation, Internal Security Agency - Republic of Poland.

MCINET (Ministry of Industry, Trade and New Technologies). 2013. *The National Strategy for Information Society and Digital Economy*, Rabat, Morocco: Ministry of Industry, Trade and New Technologies - Kingdom of Morocco.

MCIT (Ministry of Communication and Information Technology). 2012. *National ICT Strategy 2012-2017: Towards Digital Society and Knowledge-based Economy*, Cairo, egypt: Ministry of Communication and Information Technology - Arab Republic of Egypt.

MCIT (Ministry of Communication and Information Technology). 2013a. *National Cyber Security Policy 2013 (NCSP-2013)*, India.

MCIT (Ministry of Communication and Information Technology). 2013b. *Developing National Information Security Strategy for the Kingdom of Saudi Arabia* (NISS Draft.), Riyadh, Saudi Arabia: Ministry of Communication and Information Technology - Kingdom of Saudi Arabia.

MEAC (Ministry of Economic Affairs and Communication). 2014. *Cyber Security Strategy (2014-2017)*, Tallin, Estonia: Ministry of Economic Affairs and Communication - Republic of Estonia.

MED (Ministry of Economic Development). 2011. *New Zealand'S Cyber Security Strategy*, Wellington: Ministry of Economic Development - New Zealand.

Merriam-Webster. 2016a. "Definition of Strategy," (available at http://www.merriam-webster.com/dictionary/strategy; retrieved May 17, 2016).

Merriam-Webster. 2016b. "Definition of Secret," (available at http://www.merriam-webster.com/dictionary/secret; retrieved July 8, 2016).

Merriam-Webster. 2016c. "Definition of Diplomacy," (available at http://www.merriam-webster.com/dictionary/diplomacy; retrieved July 8, 2016).

MICT (Ministry of Information and Communications Technology). 2012. *National Information Assurance and Cyber Security Strategy (NIACSS)*, Jordan: Ministry of Information and Communications Technology - Jordan.

MICT (Ministry of Information and Communications Technology). 2013. *National Cyber Security Strategy* (Ministry of Information and Communications Technology - Kingdom of Qatar, ed.), Qatar: Ministry of Information and Communications Technology - Kingdom of Qatar.

MICT (Ministry of Information and Communications Technology). 2014. *Cybersecurity Strategy*, Nairobi, Kenya: Ministry of Information Communications and Technology - Republic of Kenya.

MOC (Ministry of Communication). 2014. *Ghana National Cyber Security Policy and Strategy*, Accra: Ministry of Communication - Republic of Ghana.

MoD (Ministry of Defence). 2010. *White Paper on Defence of The Republic of Serbia*, Belgrade, Serbia: Ministry of Defence - Republic of Serbia (doi: 10.1007/s13398-014-0173-7.2).

MoD (Ministry of Defence). 2011. *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (Unofficial Translation by CCDCOE)* (CCDCOE, ed.), Moscow, Russia: Ministry of Defence of the Russian Federation.

MoD (Ministry of Defence). 2012a. *The Defence Cyber Strategy*, Amsterdam, Netherland: Ministry of Defence (MoD) - Kingdom of the Netherlands.

MoD (Ministry of Defence). 2012b. *Defense White Paper*, Brasilia: Ministry of Defense - Federative Republic of Brazil.

MoD (Ministry of Defence). 2013. *Finland's Cyber security Strategy*, Helsinki, Finland: Secretariat of the Security and Defence Committee - Finland.

MOND (Ministry of National Defense). 2009. *2014 Defense White Paper*, Seoul, Korea: Ministry of National Defense - Republic of Korea.

Motlagh, H. 2015. "Border Management of Cyberspace , First Step of Cyber Defense," (5:1), pp. 16–24.

MPS (Ministry of Public Safety). 2010. *Canada ' s Cyber Security Strategy*, Ottawa: Ministry of Public Safety.

MTCI (Ministry of Technology, Communication and Innovation). 2015. *National Cyber Security Strategy 2014-2019: For Resilent and Secure Mauritius*, Port Louis, Mauritius: Ministry of Technology, Communication and Innovation - Republic of Mauritius.

MTMAC (Ministry of Transport, Maritime Affairs and Communications). 2013. *National Cyber Security Strategy and 2013-2014 Action Plan*, Istambul, Turkey: Ministry of Transport, Maritime Affairs and Communications - Republic of Turkey.

NCESP (National Council on Economic and Social Policy). 2011. *Policy Guidelines on Cybersecurity and Cyberdefense*, Bogotá, Colombia: National Council on Economic and Social Policy - Republic of Colombia.

NCKB (National Cyber Security Centre). 2015. *National Cyber Security Centre of The Czech Republic for the Periode from 2015 to 2020*, National Cyber Security Centre - The Czech Republic.

NCSC (National Coordinator for Security and Counterterrorism). 2013. *National Cyber Security Strategy 2* (National Coordinator for Security and Counterterrorism - Kingdom of Netherland, ed.), Den Haag, Netherland: National Coordinator for Security and Counterterrorism - Kingdom of Netherland.

NITA-U (National Information Technology Authority - Uganda). 2014. *National Information Security Policy* (National Information Technology Authority - Uganda, ed.), Uganda: National Information Technology Authority - Uganda.

NVIVO. 2015. "Choosing the Best Approach for Your Project," *NVivo 11 for Windows Help* (available at http://help-nv11.qsrinternational.com/desktop/concepts/choosing_the_best_approach_for_your_project.htm; retrieved February 9, 2016).

NZG (the New Zealand Government). 2011. *New Zealand's Cyber Security Strategy* (N. Z. G. (NZG), ed.), Wellington: New Zealand Government.

OCECPR (Office of the Commisioner of Electronic Communication and Postal Regulation). 2012. *Cybersecurity Strategy of the Republic of Cyprus: Network and Information Security and Protection of Critical Information Infrastructures*, Nicosia, Cyprus: Office of the Commisioner of Electronic Communication and Postal Regulation - Republic of Cyprus.

OECD (Organisation for Economic Co-operation and Development). 2012. *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*. *OECD Digital Economy Papers* (No.322 ed., Vol. 211), OECD Publishing (doi: http://dx.doi.org/10.1787/5k8zq92vdgtl-en).

Ottis, R., and Lorents, P. 2010. "Cyberspace: Definition and Implication," in *Proceeding of the 5th International Conference Information Warfare and Security*, Ohio, USA: The Air Force Institute of Technology, pp. 267–269.

PCM (Presidency of the Council of Ministers). 2013. *The National Plan for Cyberspace Protection and ICT security*, Rome, Italy: Presidency of the Council of Ministers - Italian Republic.

PMO (Prime Minister's Office). 2011. *Advancing National Cyberspace Capabilities: Resolution No. 3611 of the Government of August 7, 2011* (Vol. 2002), Jerusalem, Israel: Prime Minister's Office of Israel.

Porter, M. E. 2001. "Strategy and the Internet," *Harvard Business Review* (March 2001), pp. 63–78 (available at https://hbr.org/2001/03/strategy-and-the-internet/ar/1).

PRF (President of the Russian Federation). 2000. "President of the Russian Federation: Information Security Doctrine of the Russian Federation," *2008* (available at http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument; retrieved May 17, 2016).

Reddick, C. G., Chatfield, A. T., and Jaramillo, P. A. 2015. "Public opinion on National Security Agency surveillance programs: A multi-method approach," *Government Information Quarterly* (32:2), pp. 129–141 (doi: 10.1016/j.giq.2015.01.003).

RF (the Russian Federation). 2013. "Basic Principle for State Policy of the Russian Federation in the field of International Information Security to 2020 (Unofficial Translation)," (available at http://en.ambruslu.com/highlights-in-russia/basic-principles-for-state-policy-of-the-russian-federation-in-the-field-of-international-information-security-to-2020.html).

Saldaña, J. 2009. *The Coding Manual for Qualitative Researchers* (First Edit.), Singapore: SAGE Publications.

Scott, J. C., and Glaser, B. G. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. *American Sociological Review* (2006th ed., Vol. 36), New Brunswick (doi: 10.2307/2094063).

Seebruck, R. 2015. "A Typology of Hackers: Classifying Cyber Malfeasance using a Weighted Arc Circumplex Model," *Digital Investigation* (14:14), Elsevier Ltd, pp. 36–45 (doi: 10.1016/j.diin.2015.07.002).

SGDSN (Secrétariat Général de la Défense et de la Sécurité Nationale). 2015. *French National Strategy Digital Security Strategy*, Paris: Secrétariat Général de la Défense et de la Sécurité Nationale.

Shakarian, P., Shakarian, J., and Ruef, A. 2013. "Attacking Iranian Nuclear Facilities: Stuxnet," in *Introduction to Cyber-Warfare: A Multidisciplinary Approach*, Sydney: Syngress, pp. 223–239.

Skendžić, A. 2014. "Security Policy and Wireless Computer Networks in Educational Institutions in The Republic of Croatia," *Anali Poslovne Ekonomije* (7:10), pp. 69–81 (doi: 10.7251/APE1410066S).

von Solms, R., and van Niekerk, J. 2013. "From information security to cyber security," *Computers & Security* (38), Elsevier Ltd, pp. 97–102 (doi: 10.1016/j.cose.2013.04.004).
Souza, P. de. 2013. "National Cyber Defense Strategy," in *Strategic Intelligence Management National Security Imperatives and Information and Communications Technologies*, Butterworth-Heinemann, pp. 224–228 (doi: 10.1016/B978-0-12-407191-9.00001-6).
SSS (State Security Service). 2014a. *Nigeria's National Cybersecurity Policy*, Abuja, Nigeria: The State Security Service - Federal republic of Nigeria.
SSS (State Security Service). 2014b. *Nigeria's National Cybersecurity Strategy*, The State Security Service (SSS) - Federal republic of Nigeria.
Stier, S. 2015. "Political determinants of e-government performance revisited: Comparing democracies and autocracies," *Government Information Quarterly* (32:3), Elsevier Inc., pp. 270–278 (doi: 10.1016/j.giq.2015.05.004).
Syed, M. H. 2014. "National Cyber Security Council Bill 2014," Pakistan (available at http://www.senate.gov.pk/uploads/documents/1397624997_197.pdf).
Tehrani, P. M., and Manap, N. A. 2013. "A rational jurisdiction for cyber terrorism," *Computer Law and Security Review* (29:6), pp. 689–701 (doi: 10.1016/j.clsr.2013.07.009).
Wafa, Z. 2014. *National Cyber Security Strategy of Afghanistan (NCSA)* (2nd ed.), Kabul, Afganistan: Ministry of Communications and IT - Islamic Republic of Afghanistan.
WH (the White House Washington). 2003. *The National Strategy to Secure Cyberspace*, Washington: The White House Washington.
WH (the White House Washington). 2011. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington: The White House Washington.
Wiener, N. 1948. *Cybernetics: Control and Communication in the Animal and the Machin* (second edi.), Cambridge, Massachusetss: The M.I.T Press.

Acknowledgements

The first author would like to acknowledge the Indonesia Endowment Fund for Education (Lembaga Pengelola Dana Pendidikan - LPDP), Ministry of Finance, The Republic of Indonesia as its support for the scholarship funding.

Copyright