CENTRE FOR SECURITY STUDIES

DEFENCE WHITE PAPER PROJECT

SPAIN'S NATIONAL CYBER SECURITY STRATEGY 2013

GITIKA GUPTA

EDITED BY: DIVYASHREE JHA

About the author

Gitika Gupta is a Post graduate student at the Jindal School of International Affairs.

About the Centre for Security Studies

The Centre for Security Studies (CSS) was established in 2020 as the Jindal School of International Affairs' first student-run research centre under the aegis of Prof Dr Pankaj K Jha. Researchers at CSS – through in-depth analysis briefs and events, reports, policy briefs and print publications – explore both regional and thematic topics in the broader field of international security studies. The concept of international security has been expanded to reflect not merely the study of state security, but also include topics like ethnic, sectarian and religious conflict; civil wars and state failure; cyber and space warfare; resource related security issues; the proliferation of weapons of mass destruction; defence economics and also the role of ethics or morality in the formulation of security policies. The complexity of these matters is what the Centre for Security Studies attempts to unfold. Please refer to www.cssjsia.com for further details, and follow the Centre's social media platforms for critical news and research updates:


www.linkedin.com/company/jindal-centre-for-security-studies/


www.instagram.com/css_jsia/


https://twitter.com/Css_Jsia

Get in touch with us through email: css@jgu.edu.in

Important Disclaimer

WD2207007

Introduction

"Cyber security is a man-made ecosystem." - Lehto, Martti.[1]

As the world is rapidly moving towards higher levels of globalisation and the use of international common spaces such as cyberspace is becoming increasingly common, not just for corporations and private individuals, but also public administrative services in different countries of varying levels of globalisation, it raises concerns regarding threats and risks pertinent in the global cyberspace where there are no natural borders and jurisdiction can be difficult to execute. In Spain the issue of cyber security was first dealt with through the National Security Strategy, Estrategia de Seguridad Nacional, ESN of 2011. But it only dealt with it in a minor way, and Spain was lagging behind many of its European and Western peers[2]. The National Security Department, Departamento de Seguridad Nacional, DSN, was formed in July 2012 under the Prime Minister's office and it reviewed the ESN 2011, and released an improved and more comprehensive ESN in 2013. ESN 2013 described cyber security as one of the twelve priority work areas, defining cyberspace as a global common space[3]. This led to the subsequent development of the National Cybersecurity Strategy of 2013 by the Spanish government whose area of jurisdiction, objectives and subsequent work is explored critically in this report[4].

[1] Martti Lehto, "The Ways, Means and Ends in Cyber Security Strategies," in *Proceedings of the 12th European Conference on Information Warfare and Security*, ed. Rauno Kuusisto and Erkki Kurkinen (University of Jyvaskyla, Finland: Academic Conferences and Publishing International Limited, 2013), 182–90, https://www.google.co.in/books/edition/Proceedings_of_the_12th_European_Confere/CrIVBAAAQBAJ?hl=en&gbpv=1.
[2] Alexander Cendoya, "National Cyber Security Organisation: Spain," ed. Kadri Kaska (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016).
[3] "National Security Strategy" (Spain: Gobierno De España, 2013).
[4] "Spanish National Security Strategy," www.oecd.org, accessed May 3, 2022, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/spanishnationalsecuritystrategy.html

Cyberspace and Cybersecurity

The term cyber-security was first popularised in mainstream media in 2009 by the then U.S. president Barack Obama[5]. Previously the use of terms such as computer security and information security was more popular in general discourse. The previous terms had an advantage in terms of clarity because it is easier to gauge the meaning of what one means when they use the term "Information technology", as compared to the ambiguity of the term "cyber security".

In modern day conversations, cyber security is interchangeably used with terms such as internet security or information security. For strategic documentation and policy initiatives, the ambiguity in the use of the term cyber security is problematic because it creates uncertainty regarding what all areas in the cyber domain should be considered while formulating security strategies. There is little consensus universally, when it comes to defining what cyber security is. This can possibly create a problem for collaborations between different nation-states and formation of international treaties and arms control agreements. The general perception of cyber security in the West is of creating a "cyber security prism" but because of the lack of commonality between governments when it comes to definition, there is a lack of cohesion when it comes to governance of the cyberspace.

A proposed academic definition for cyber security that can be used for the analysis of various national cyber security strategies is "The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyberspace. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users."[6]

The Spanish national cyber security strategy, i.e., the Spanish NCSS, defines cyberspace as a dynamic and global domain that has come into existence with the development of Information and Communication technologies (ICTs) over the decades[7]. Cyberspace consists of critical infrastructures of information technology, the internet, networks and information and telecommunications systems. Because of the

[5] Schatz, Daniel, Rabih Bashroush, and Julie Wall. "Towards a More Representative Definition of Cyber Security." *The Journal of Digital Forensics, Security and Law* 12, no. 2 (2017): 53–74. https://doi.org/10.15394/jdfsl.2017.1476.

[6] Schatz, Daniel, Rabih Bashroush, and Julie Wall. "Towards a More Representative Definition of Cyber Security." *The Journal of Digital Forensics, Security and Law* 12, no. 2 (2017): 53–74. https://doi.org/10.15394/jdfsl.2017.1476.

[7] "National Cyber Security Strategy" (Spain: Gobierno De España, 2013).

unprecedented globalisation seen in the 21st century, cyberspace is a highly globalised platform where the area of influence and control of different nations is intermingled with each other and has led to the conception of new opportunities and threats, not just for Spain, but for the whole world[8].

Subsequently, NCSS is defined as a "strategic document that provides the Spanish Government with a basis for developing the provisions of the National Security Strategy on the protection of cyberspace in order to implement cyber threat prevention, defence, detection, response and recovery actions against cyber threats."[9]

Threats to cyber security

An important aspect in defining the motivations of governments in developing the NCSS, is understanding the risks and threats faced by a government through cyberspace. The European Network and Information Security Agency (ENISA) has defined a cyber-threat model, according to which a threat agent can be any person or thing which acts in a way that causes, carry, transmit or support a threat[10]. ENISA also narrows down some of the biggest threat agents in the 21st century - corporations, cybercriminals, employees, hacktivists, nations and terrorists. The threat model ENISA has developed defines threats as different types of cyber-attacks and techniques, in addition to malware and physical attacks.

Cyber-attacks and techniques	Malwares	Physical threats
Drive-by Exploits	Exploit Kits	Physical Theft/Loss/Damage
Code Injection Attacks	Worms/Trojans	Rogue certificates
Botnets	Rogueware/Scareware	
Denial of service	Spam	
Phishing		
Compromising confidential information		
Targeted Attacks		
Identity Theft		
Abuse of Information Leakage		
Search Engine Poisoning		

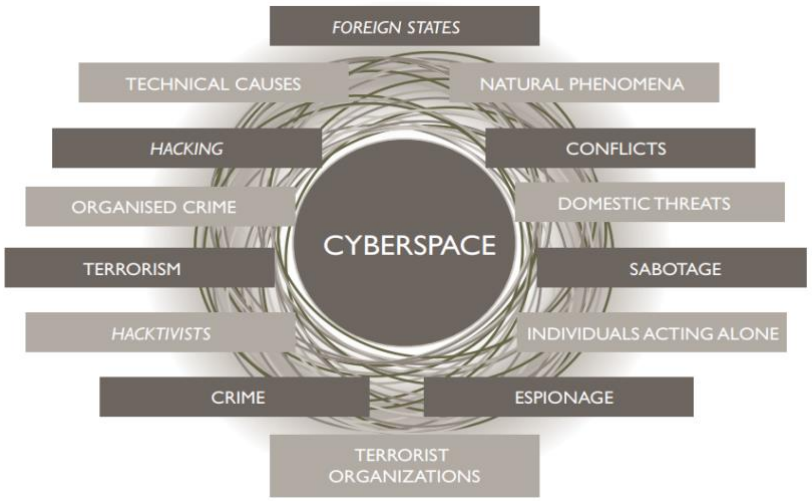
[11]

[8] Riza Azmi, William Tibben, and Khin Than Win, "Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy," *Australasian Conference on Information Systems*, 2016.
[9] "National Cyber Security Strategy" (Spain: Gobierno De España, 2013).
[10] Lehto, Martti. "The Ways, Means and Ends in Cyber Security Strategies." In *Proceedings of the 12th European Conference on Information Warfare and Security*, edited by Rauno Kuusisto and Erkki Kurkinen, 182–90. University of Jyvaskyla, Finland: Academic Conferences and Publishing International Limited, 2013. https://www.google.co.in/books/edition/Proceedings_of_the_12th_European_Confere/CrIVBAAAQBAJ?hl=en&gbpv=1.

[11] Lehto, Martti. "The Ways, Means and Ends in Cyber Security Strategies." In *Proceedings of the 12th European Conference on Information Warfare and Security*, edited by Rauno Kuusisto and Erkki Kurkinen, 182–90.

For Spain, cyber-attacks share the similar characteristics of low cost, ubiquity and ease of execution, effectiveness and impact, and reduced risk for the attacker[12]. The Spanish government acknowledges that in the 21st century, a country's stability and prosperity is highly dependent on the security and the reliability of cyberspace. Technical causes, natural phenomena and deliberate aggressions are all considered a threat to the resilience of Spanish cyberspace.

The Spanish government considers the following as threats and risks to the Spanish cyberspace:



[13]

Motives Behind the Creation of NCSS

A NCSS provides a strategic framework to a country to improve the security and sustainability of the cyberspace of the country consisting of information instruction, public administration, internet, etc[14]. A commonality found in different countries' NCSS is the strategic importance given to protecting government information and national defence, in addition to critical infrastructures and protecting civilian information.

University of Jyvaskyla, Finland: Academic Conferences and Publishing International Limited, 2013. https://www.google.co.in/books/edition/Proceedings_of_the_12th_European_Confere/CrIVBAAAQBAJ?hl=en&gbpv=1.

[12] "National Cyber Security Strategy" (Spain: Gobierno De España, 2013).

[13] "National Cyber Security Strategy" (Spain: Gobierno De España, 2013).

[14] Riza Azmi, William Tibben, and Khin Than Win, "Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy," *Australasian Conference on Information Systems*, 2016.

In forming their NCSS, states come to view cyberspace as a jurisdictional space similar to land, air and sea. According to policymakers, cyberspace too, is an important area that requires regulation to preserve national sovereignty. It is difficult to regulate cyberspace because of the fact, it is difficult to establish borders or even a cohesive understanding of cyber security among different states. Additionally, in the highly globalised and "open" world we live in, the free flow of information regarding economics, politics and culture may result in leaking of state-secrets creating a need for laws and regulations[15]. Political motivations are also important for consideration when we discuss the procedure and aim of policy-making. Politicians, who are the ultimate policy-makers responding to the environment of the state, especially any experienced and/or perceived threats[16]. The NCSS align with the national interest and politics is therefore, intermingled with the motives that influence the formation of NCSS.

The general guidelines for the development of policy initiative, regarding cybersecurity, in Spain is guided by the principles as defined in its constitution and the provisions of the Charter of the United Nations on peacekeeping and international security, along with the initiatives developed in Europe, internationally and/ or regionally[17]. Furthermore, In context of cyber security, economic security, protection of state secrets and requirements defined by the other policy instruments are important motivations for the conception of NCSS 2013. The NCSS is built on shared principles with the National Security Strategy of Spain, 2013. The principles guiding the strategic document are as follows- National leadership and coordination efforts; shared responsibility; proportionality, rationality and efficiency; and international cooperation[18]. The ultimate aim for the same, as defined by NCSS, 2013, is to strengthen and respect the protection and fulfilment of the fundamental freedoms as described in the Spanish Constitution and in international doctrines such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms.

[15] Riza Azmi, William Tibben, and Khin Than Win, "Review of Cybersecurity Frameworks: Context and Shared Concepts," *Journal of Cyber Policy* 3, no. 2 (May 4, 2018): 258–83, https://doi.org/10.1080/23738871.2018.1520271.
[16] Martti Lehto, "The Ways, Means and Ends in Cyber Security Strategies," in *Proceedings of the 12th European Conference on Information Warfare and Security*, ed. Rauno Kuusisto and Erkki Kurkinen (University of Jyvaskyla, Finland: Academic Conferences and Publishing International Limited, 2013), 182–90, https://www.google.co.in/books/edition/Proceedings_of_the_12th_European_Confere/CrIVBAAAQBAJ?hl=en&gbpv=1.
[17] Alexander Cendoya, "National Cyber Security Organisation: Spain," ed. Kadri Kaska (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016).
[18] "National Cyber Security Strategy" (Spain: Gobierno De España, 2013).

Overview of the Objectives NCSS, Spain 2013

The NCSS, Estrategia Nacional de Ciberseguridad, ENCS, was adopted by the Kingdom of Spain in December, 2013, is considered the foundational document for cyber security strategy in the country. ENCS is responsible for providing the basis for establishing guidelines for cyberspace security with the cooperation of all public administrations, private sector and the larger population[19].

The underlying objective of ENCS is to ensure that Spain uses ICT systems in such a manner that is responsible for strengthening prevention, defence, detection and response capabilities of the country's government and administration, in response to cyber-attacks[20]. Though, a policy issue is that the document doesn't clearly define what risks and threats in cyberspace mean. The overall objective is further defined into the following objectives:

1. Ensuring the ICT systems used by the Public Authorities of the country are protected and are resilient through the implementation of a comprehensive and cohesive framework that includes not just policies, but also procedures and technical standards, applicable to all public administrations. The aim is to ensure the protection of public information and public administrative systems, along with tits supporting networks. This will require public administrations and the general technological level of the country to continue to evolve and adapt to the new risks and threats faced within cyberspace.

2. Ensuring the security and resilience of ICT systems of importance in the business sector, especially of the operators of Critical Infrastructures. It will require the public administrations to maintain continuous and close relationships with private sector companies and firms important for the protection and continued existence of the critical infrastructure, along with ensuring easy exchange of knowledge to facilitate coordination and understanding between public and private cyberspace.

3. Improving the prevention, detection, reaction, analysis, recovery, response, research and coordination capabilities of public administrations in combating terrorist activities and crime in cyberspace. It is important to facilitate international judicial and police cooperation. It also includes the establishment of necessary instruments for international cooperation and exchange of information, along with national legislation that aligns with international agendas.

[19] Alexander Cendoya, "National Cyber Security Organisation: Spain," ed. Kadri Kaska (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016).
[20] "National Cyber Security Strategy" (Spain: Gobierno De España, 2013).

4. Raising awareness among citizens, professionals, companies and Spanish Public Authorities about the risks in cyberspace. A major step in this direction is to promote a cyber security culture that ensures that the all described actors have the necessary awareness and confidence when it comes to utilising the benefits of the information society to the maximum and minimise their exposure to risks and threats in cyberspace by using reasonable measures to guarantee protection of data and secure connection of systems and equipments.

5. Gaining and maintaining knowledge, skills, experience and technological abilities Spain needs to achieve all the cyber security objectives defined. A basic requirement for that is the availability of qualified personnel and to ensure the continuous flow of R&D&I activities important for cyber security.

6. Improving cyber security in the international sphere. It requires developing a coordinated cyber security system with various international organisations such as European Defence Agency (EDA), the European Union Agency for Network and Information Security (ENISA), the European Cybercrime Centre attached to EUROPOL, the United Nations (UN), the Organisation for Security and Cooperation in Europe (OSCE), the North Atlantic Treaty Organisation (NATO), and the Organisation for Economic Cooperation and Development (OECD), etc[21].

The strategy document goes further on to list and describe 8 lines of Action response to carry out the above defined objectives of the Kingdom of Spain in a systematic manner. These lines of Action include - an institutional ability to detect, prevent, respond and recover from cyber threats; ensure the security of ICT systems important for public administration, and critical infrastructure; capacity to investigate and prosecute cybercrime and cyberterrorism; ensuring the security and resilience of ICT systems of the private sector; developing knowledge, skills and R&D&I in the country through training professionals and etc.; developing a cyber security culture in the country; and committing to developing an international cyberspace[22].

[21] "National Cyber Security Strategy" (Spain: Gobierno De España, 2013).
[22] "National Cyber Security Strategy" (Spain: Gobierno De España, 2013).

Cyber Security Infrastructure in Spain

The ESN 2013 is responsible for the formation of the National Cybersecurity Council or Consejo Nacional de Ciberseguridad (NCC), a collegiate body that supports the functions of the National Security Council (NCS), the Government's Delegate Commission for National Security. The framework of the relationship between the two councils is laid out by Law 50/1997, of November 27, of the Government. The National Cybersecurity Council was created by Agreement of the National Security Council of December 5, 2013 as per the objectives discussed in the ESN 2013. The National Cyber Security Council is a part of the specialised committees in the NSC[23].

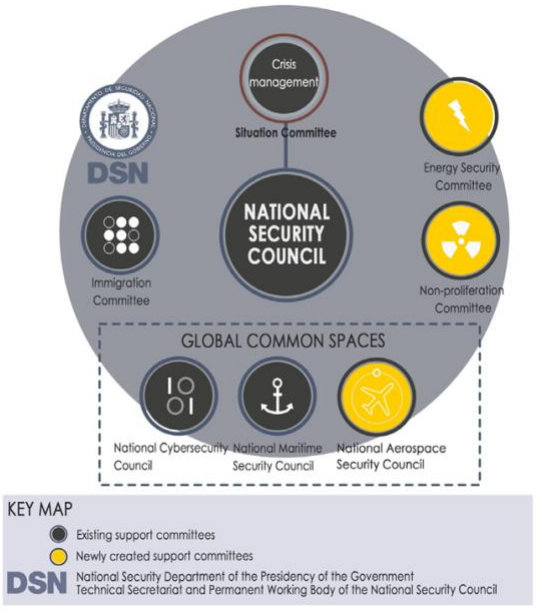
The objective of the NCC is to strengthen coordination, collaboration and cooperation between various public administrations in the country, along with the other public and private sector actors. This relationship is important to facilitate the decision-making of the NCC through analysis, study and proposal of national and international initiatives. The NCC is the technical secretariat and a permanent body of the NSC, and is supported by the Department of National Security[24]. The council consists of the Deputy Prime Minister, relevant State Secretaries, the Director of the Prime Minister's Office, and other members of the Spanish government. NCS holds regular meetings on a bi-monthly basis or as many times as required, that are chaired by the Prime Minister, unless the King of Spain is in attendance. The NSC is responsible for assisting the Prime Minister for the purpose of coordination and management of the National Security Policy, on cybersecurity issues, both national and international[25].

The ESN 2013 also facilitates the formation of a Specialised Situation Committee, Comité Especializado de Situación, which is responsible to provide assistance to the NSC during crisis situations relating to cybersecurity matters that cannot be channelled through the conventional response mechanisms already in place either because of their severity or their nature[26]. It supports CSN in its mandate to perform specific and effective responses through a single governing body. Duties of the committee include formulating political-strategic guidelines for managing crisis situations; ensuring optimum use of the available

[23] "El Consejo de Seguridad Nacional | DSN," www.dsn.gob.es, accessed May 3, 2022, https://www.dsn.gob.es/es/sistema-seguridad-nacional/consejo-seguridad-nacional.
[24] "National Cyber Security Strategy" (Spain: Gobierno De España, 2013).
[25] Alexander Cendoya, "National Cyber Security Organisation: Spain," ed. Kadri Kaska (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016).
[26] "National Cyber Security Strategy" (Spain: Gobierno De España, 2013).

resources; promoting international cooperation; studying and analysing crisis situations; and convening sessions for the CSN during crises[27].

28



29

Furthermore, The Spanish National Cybersecurity Institute M.P., S.A., (INCIBE) is an institution under the Ministry of Economic Affairs and Digital Transformation through the State Secretariat for Digitalization and Artificial Intelligence[30]. It is responsible for the development of cybersecurity and digital trust among Spanish citizens, academic and research networks and companies in sectors of strategic importance. It is responsible for leading cyber security in Spain on a national and international level. INCIBE-CERT is the security incident response centre of reference for citizens and private actors in Spain, under the jurisdiction of the National Institute of Cybersecurity. It is also responsible for coordination between national and

[27] Alexander Cendoya, "National Cyber Security Organisation: Spain," ed. Kadri Kaska (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016).
[28] "National Cyber Security Strategy" (Spain: Gobierno De España, 2013).
[29] "National Security Strategy" (Spain: Gobierno De España, 2017).
[30] "What Is INCIBE," INCIBE, January 27, 2016, https://www.incibe.es/en/what-is-incibe.

international teams to improve the efficiency of cybersecurity and information networks and ensuring public security.

The Cybersecurity Environment of Spain

The Global cybersecurity index, published December, 2014, ranked Spain as 9th worldwide, with an index of 0.588, whereas Spain's overall regional ranking was 6 at 0.5882. The index is described through certain categories and performance indicators. Spain's index corresponding to these measures was as follows- legal, 1.0000; technical, 0.6667; organisational, 0.6250; capacity building, 0.6250; and cooperation, 0.2500[31].

Furthermore, Spain is ranked 6th among the top 20 countries to have the highest rates of cybercrime. There are 6 contributing factors to this ranking- share of malicious computer activity out of all computer activities, 4%; malicious code rank, 10; spam zombies rank, 8; phishing web-site hosts rank, 13; bot rank, 3; and attack origin rank, 6. Among the developed countries of the world, Spain was ranked at 9, at par with France[32].

The ENCS 2013 classifies cyberspace only as internet and internet connected ICT devices and the responsible authority for dealing with cybersecurity is a new coordinating body in the form of NCC as described above[33]. Based on the ambiguity in the definition of cyberspace and the lack of any description regarding a public-private partnership plan in the ENSC 2013, the strategy of the country overlooks certain critical aspects of building a sound and reliant cybersecurity system.

[31] "Global Cybersecurity Index" (New York, USA: ABI Research, December 9, 2014).
[32] "Top 20 Countries Found to Have the Most Cybercrime," EnigmaSoft, n.d., https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/.
[33] Narmeen Shafqat and Ashraf Masood, "Comparative Analysis of Various National Cyber Security Strategies," *International Journal of Computer Science and Information Security (IJCSI)S* 14, no. 1 (January 2016).

Conclusion

Spain is very much committed to developing a national system and facilitating international cooperation when it comes to its cybersecurity needs. Raising awareness regarding cyber threats, and developing the resilient system of security in the society continue to be an important component of the response mechanism to cyber threats and risks faced by the country[34]. Furthermore, establishment of government institutions and CSIRT/CERT teams open to the private sector, and regional CERTs has proved to be essential to build trust and cohesion in the Spanish cybersecurity community[35]. The 2013 strategy was revised in 2017 in the National Security Strategy, where the Spanish government further illustrates the lines of action and concepts proposed in the 2013 document[36]. It also illustrates the need to adapt policy, instruments and state resources in context to the dynamic environment of cyberspace. One major policy requirement for further initiatives and development of cybersecurity in Spain requires a detailed definition of cyberspace and the jurisdictional area within the cyberspace for the country. It will not only facilitate better functioning and resilience of the cybersecurity infrastructure of Spain, but also facilitate better cohesion in international governance of the global cyberspace.

[34] "Spanish National Security Strategy," www.oecd.org, accessed May 3, 2022, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/spanishnationalsecuritystrategy.htm.
[35] Rubén Arcos, "Securing the Kingdom's Cyberspace, Cybersecurity and Cyber Intelligence in Spain," ed. Scott N. Romaniuk and Mary Manjikian, *Routledge Companion to Global Cyber Security Strategy*, 2021, 11–25.
[36] "National Security Strategy" (Spain: Gobierno De España, 2017).

Bibliography

Arcos, Rubén. “Securing the Kingdom’s Cyberspace, Cybersecurity and Cyber Intelligence in Spain.” Edited by Scott N. Romaniuk and Mary Manjikian. *Routledge Companion to Global Cyber Security Strategy*, 2021, 11–25.

Azmi, Riza, William Tibben, and Khin Than Win. “Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy.” *Australasian Conference on Information Systems*, 2016.

———. “Review of Cybersecurity Frameworks: Context and Shared Concepts.” *Journal of Cyber Policy* 3, no. 2 (May 4, 2018): 258–83. https://doi.org/10.1080/23738871.2018.1520271.

Cendoya, Alexander. “National Cyber Security Organisation: Spain.” Edited by Kadri Kaska. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016.

digital-agenda-data.eu. “Digital Scoreboard - Data & Indicators,” n.d. https://digital-agenda-data.eu.

www.dsn.gob.es. “El Consejo de Seguridad Nacional | DSN.” Accessed May 3, 2022. https://www.dsn.gob.es/es/sistema-seguridad-nacional/consejo-seguridad-nacional.

“Global Cybersecurity Index.” New York, USA: ABI Research, December 9, 2014.

Lehto, Martti. “The Ways, Means and Ends in Cyber Security Strategies.” In *Proceedings of the 12th European Conference on Information Warfare and Security*, edited by Rauno Kuusisto and Erkki Kurkinen, 182–90. University of Jyvaskyla, Finland: Academic Conferences and Publishing International Limited, 2013. https://www.google.co.in/books/edition/Proceedings_of_the_12th_European_Confere/CrIVBAAAQBAJ?hl=en&gbpv=1.

“National Cyber Security Strategy.” Spain: Gobierno De España, 2013.

“National Security Strategy.” Spain: Gobierno De España, 2013.

“National Security Strategy.” Spain: Gobierno De España, 2017.

Schatz, Daniel, Rabih Bashroush, and Julie Wall. “Towards a More Representative Definition of Cyber Security.” *The Journal of Digital Forensics, Security and Law* 12, no. 2 (2017): 53–74. https://doi.org/10.15394/jdfsl.2017.1476.

Shafqat, Narmeen, and Ashraf Masood. “Comparative Analysis of Various National Cyber Security Strategies.” *International Journal of Computer Science and Information Security (IJCSI)S* 14, no. 1 (January 2016).

www.oecd.org. “Spanish National Security Strategy.” Accessed May 3, 2022. https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/spanishnationalsecuritystrategy.htm.

EnigmaSoft. “Top 20 Countries Found to Have the Most Cybercrime,” n.d. https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/.

INCIBE. “What Is INCIBE,” January 27, 2016. https://www.incibe.es/en/what-is-incibe.