Chapter 23
National Cybersecurity Strategies

Regner Sabillon
Universitat Oberta de Catalunya, Spain

ABSTRACT

This chapter studies the phases to unify our national cybersecurity strategy model (NCSSM) in any nation cyber strategy that is either under development or improvement stages. This methodology consists of developing international cybersecurity strategies, alliances, and cooperation with different stakeholders at all possible levels. The research evaluated the best practices of 10 leading countries and five intergovernmental organizations in terms of developing effective cybersecurity strategies and policies. The authors also assessed a series of cybersecurity best practices that can be aligned with cyber governance and cyber law when countries wish to develop or enhance national cyber strategies. Furthermore, they propose guidelines to audit the national cyber strategies by utilizing their cybersecurity audit model (CSAM). CSAM could be considered for conducting cybersecurity audits in any nation state in pursuance of reviewing and measuring the cybersecurity assurance, maturity, and cyber readiness and to detect the needs to increase cyber awareness to defend and protect critical cyber assets.

INTRODUCTION

A study from Luiijf et al. (2013) was conducted to research about the the structure, sections and elements of nineteen National Cybersecurity Strategies (NCSS) from these countries [Australia, Canada, Czech Republic, Estonia, France, Germany, India, Japan, Lithuania, Luxembourg, Romania, The Netherlands, New Zealand, South Africa, Spain, Uganda, The United Kingdom - UK (2009 and 2011) and The United States of America (USA)]. Most NCSS in this research, embraced a holistic approach for cyberspace, and all nations have considered international threats and risks in cyberspace. Most NCSS are focusing on societies, more specifically citizens, businesses, public sector and government. Subsequently, the authors proposed a structure for developing NCSS that encompasses an executive summary, an introduction, a strategic national vision on cybersecurituy, existing NCSS' relationships with other strategies

DOI: 10.4018/978-1-6684-3698-1.ch023

at the national and international level and legal frameworks, any guidance principles, the definition of cybersecurity objectives, an inventory of tactical actions and a glossary.

As reported by NATO (2013), cyber operations indicate the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace, and under international laws States may be responsible for the conduction of cyber operations by their organs including non-state actors.

For several years, there have been four notorious domains in warfare: Air, Sea, Space and Land. With the information era booming, a new domain was added which is now Cyberspace. Lemieux (2015) reserached several events that led to the consolidation of cyber domains as part of modern warfare studies. Network-Centric Warfare (NCW) was conducive during the US military dominance during the 1991 Gulf War, commanders took advantage of NCW to maintain their forces informed at all times regarding situational awareness, troop movement and always outmaneuvering enemy forces. Henceforth, these battlefield experiences were observed and explored by Russia and China for further acceptance into their own military operations.

The US Department of Defense - DOD (DOD, 1991) published the *Joint Publication 3-0: Operations* which included 'Information' as the fifth warfighting domain to join the existing Air, Sea, Space and Land domains. The DOD (1996) declassified the *National Military Strategy for Cyberspace Operations (NMS-CO)* where information was escalated to the cyberspace domain.

Many nations are straighten out their cyber capabilities in cyberspace by proposing, creating, implementing and continuously updating a National Cybersecurity Strategy, policy or programme. Sabillon et al. (2016) described a cybersecurity policy as the instrument developed by nations to communicate and express those aspects that want a state to protect in cyberspace. North Atlantic Treaty Organization - NATO (2019) introduced a repository with NCSS and legal documents for 81 countries [13 for Africa, 11 for Americas and The Caribbean, 19 for Asia and Oceania and 38 for Europe] and The European Union Agency for Cybersecurity (ENISA, 2019) maintains the ENISA NCSS map for the 28 member states of the European Union (EU) and for the 4 member states of the European Free Trade Association (EFTA) that lists the implementation date and the number of objectives of each NCSS . International Telecommunication Union (ITU) (2016) highlights that 72 out 193 member states have published a National Cybersecurity Strategy but the majority of countries now have a NCSS (ITU, 2019). According to the Global Cybersecurity Index GCI 2018 v3 (ITU, 2019), 58% of the United Nations members have a NCSS in place with Europe and countries from the Commonwealth of Independent States (CIS) with the highest numbers of nations with NCSS, while the Africa region has the lowest indicator (14 out of 44 countries with a NCSS).

NATIONAL CYBERSECURITY STRATEGIES (NCSS)

A cybersecurity policy is an instrument designed by nations to communicate and express selected aspects that want a state to protect cyberspace. It is a statement which embodies the stance of a nation to bind strongly to citizens, their rights and duties; now in a stage of the widespread reality of society where instant information, mobility and social networks are the norm of its operation. This perceptibility of cyberspace requires a renewed understanding of the relationships with others and with the nations. Given the background, cybersecurity in a state policy formalizes a decision that a country now declares as a digital territory – and it has extended where similarly will exercise sovereignty, knowing that virtual space is shared with other nations and possess a national synergy (Sabillon et al., 2016).