National Cyber Security Strategies: Global Trends in Cyberspace

Regner Sabillon[1], Victor Cavaller[2] and Jeimy Cano[3]

[1] Network and Information Technologies, Universitat Oberta de Catalunya (UOC), Barcelona, Spain

[2] Information and Communication Studies, Universitat Oberta de Catalunya (UOC), Barcelona, Spain

[3] Law Faculty, Universidad de los Andes (Uniandes)

[1]regners@athabascau.ca, [2]vcavaller@uoc.edu, [3]jcano@uniandes.edu.co

ABSTRACT

Nations must define priorities, objectives, goals and scope when formulating a national strategy that covers cyberspace, cybersecurity, stakeholder engagement, capacity building, cyber governance, cybercrime and cyber defense. The goal of this article is to propose a National Cybersecurity Strategy Model (NCSSM) based on key pillars in order to tackle the completion of all the requirements in a national strategy. This approach aims to develop international cybersecurity strategies, alliances and cooperation. Our research is focused on a comparative analysis of ten leading countries and five intergovernmental organizations cybersecurity strategies. It includes eleven cybersecurity frameworks aligned with cyber governance and cyber law.

Keywords: *National cybersecurity strategy, cybersecurity, cyber law, cyber governance, international cybersecurity strategy, cyber policy.*

1. INTRODUCTION

One lesson we cannot forget is that talking about cybersecurity should not be limited to reflections in the context of information technology, but the understanding of the challenges and impacts imposed by cyberspace as a platform where the relationship between states and citizens now happens.

A cybersecurity policy is an instrument developed by nations to communicate and express those aspects that want a state to protect cyberspace. It is a statement which embodies the stance of a government 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.

In this context, economic variables related to the movement of capital and investment are affected, since banks are more flexible and promote such interaction with increasingly personalized and electronic services, encouraging an online flow of financial assets, conditions that require permanent protection, safety practices thus control where customers and the bank interact.

On the other hand, there are psychological implications of these new interactions of citizens in cyberspace; where the motivations, orientations and actions are presented in accordance with trends and patterns of actions that are defined by emerging realities of informatics relationships between different actors - they may induce positive, negative or neutral behaviors which manifest a supranational consciousness that is present not in a visible, but immersed in the social fabric assisted by information networks and communication context.

Since this new reality of virtual and real interaction mobilizes communities and relationships outside the domain and contours of a country, behaviors and social expressions demand a whole different order. In this sense, legal science finds a new challenge of regulation on a scenario that is uncertain and unpredictable, to try to conceptualize and propose solutions versus those situations categorized as reprehensible conducts, which articulated with information technology, become more volatile against possible forms of punishment and control.

This reality 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.

This article analyzes comparatively national security strategies in ten countries from five different continents, study policy-making considerations from five global intergovernmental organizations and describe the most current cybersecurity frameworks. The research has six parts. Part I discusses national cybersecurity strategies in Australia, Canada, Israel, Japan, Malaysia, Norway, South Africa, The Netherlands, The United Kingdom and The United States of America. Part II examines the national security strategy perspectives from intergovernmental organizations like UN, ITU, EU, OECD and NATO. Part III highlights eleven cybersecurity frameworks that are in use globally. Part IV introduces a proposal of the National Cybersecurity Strategy Model (NCSSM) and all its components. And finally, part V reviews the international cooperation and knowledge transfer of the existing national strategies.

2. Part I: National CyberSecurity Strategies

We have selected ten nations that have demonstrated a steady leadership when dealing with cybercrime; establishing cyberdeterrence and implementing a national cybersecurity strategy. A previous study [1] compared national cybersecurity strategies, and then our research is based on main components of a national strategy, goals, action plans, involved agencies and future developments to consolidate and expand the strategies [1].

2.1 Australia

Australia's cyber strategy is included in their *Strategy for National Security* and also on the *Defence White paper*. This strategy has been ratified since 2013.

Along with their national security strategy, Australia wants to secure their assets and infrastructure by identifying national security risks like malicious cyber activity, organized crime activities and pervasive technology threats.

One of the long term priorities is to integrate cyber policy and operations to enhance the defense of the Australian digital networks. The National security strategy highlights that cyber strategy is a fundamental pillar for Australia's future. Their national law and enforcement agencies are focused on protecting citizen's privacy and their cyber environments.

They have identified that cyber threats like identity theft, denial of services and cyber espionage can affect government agencies, businesses and citizens. Australia's cybersecurity expenditure in the 2011-12 period included AU $ 480 million[2]. Their approach enclosed forming alliances with 125 countries on intelligence to fight cyber threats and by implementing cyber initiatives between the government and the industries. The Australia-United States alliance is their most important security relationship [2]. They are focused on protecting Australia's cyberspace and in terms of cyber resilience, by constantly increasing integrated cyber security operations. The Australian Cyber Security Operations Centre (CSOC) provides different capabilities like Cyber Security Operations, Computer Emergency Response Team (CERT), Cyber Espionage and High-Tech Crime. The Australia's military is regularly adding cyber capabilities to protect and remediate critical information networks and systems [3].

The *Australian Defence* signed an AU $ 1.1 billion contract with Telstra, to upgrade telecommunication technology in order to protect against cyber attacks[3].

For future development, they want to strengthen cooperation with allies like UN, APEC, G20, Seoul Conference and the Council of Europe's Convention on Cybercrime.

2.2 Canada

Canada relies on their Cyber Security Strategy and on the Action plan 2010-15 as well. Both policies have been approved since 2010.

The Cyber Security strategy protects citizens, industry and government from cyber threats; it enforces the National *Strategy and Action Plan for Critical Infrastructure* policy. *And* it implements a plan to protect digital infrastructure in conjunction with the Throne, provinces, territories and the private sector.

The Cyber Security strategy is based on three pillars[4] - protecting governments systems, creating partnerships outside the federal habitat and protecting Canadians in cyberspace [4].

Clear federal roles and responsibilities have been designated to federal agencies like the Public Safety Canada, Industry Canada, Defence Research and Development Canada, Canadian Radio Telecommunications Commission, Justice Canada, Privy Council Office, Canadian Cyber Incident Response Centre, Communications Security Establishment Canada, Canadian Security Intelligence Service, Royal Canadian Mounted Police, Shared Services Canada, Treasury Board Secretariat, Foreign Affairs and International Trade Canada, Department of National Defence and the Canadian Forces.

The Action Plan states the implementation steps to support the national cybersecurity to strengthen cybersecurity at all levels, protect assets from cyber

[1] Greiman, Virginia, *Cyber Security and Global Governance*, Proceedings of the 14th European Conference on Cyber Warfare & Security (Hattfield: University of Hertfordshire 2015), 1-4

[2] Australian Government, *Strong and Secure: A Strategy for Australia's National Security* (Canberra: Department of the Prime Minister and Cabinet, Commonwealth of Australia 2013) Ch 3, 15

[3] Australian Government, *Strong and Secure: A Strategy for Australia's National Security* (Canberra: Department of the Prime Minister and Cabinet, Commonwealth of Australia 2013) Ch 8, 81

[4] Canadian Government, *Canada's Cybersecurity Strategy for a Stronger and More Prosperous Canada* (Ottawa: Her Majesty the Queen in Right of Canada 2010), 7-8

threats, improve the response to cyber incidents, to engage with international partners, to improve the citizen's cyber awareness and to fight cybercrime. It also promotes Academia involvement with cyber security research and development projects.

Public cyber awareness campaigns have included Get Cyber Safe and STOP.THINK.CONNECT[1]. In the fight against cyber criminality, Canada established the Cyber Crime Fusion Centre and included a Cyber Crime Strategy including Anti-spam legislation and Safeguarding Canadian's Personal Information Act.

Canada works jointly to enhance their Cyber security capacities with the United Kingdom, New Zealand, NATO, G8 and UN agencies [5].

2.3 Israel

The Israel's National Cyber Bureau (INCB)[2] was established in 2011 as an advising agency for the Prime Minister, the Israel government and all its committees to recommend the national cyber field policy [6].

The INCB operates based on the National Security Council Framework; the INCB also works in close cooperation with the National Council for Research and Development (NCRD).

Israel owns a world renowned cyber defense and is constantly exporting cyber-related product and services second to the United States.

The Israel's cybersecurity policy was established to position Israel on the top five list of global superpower nations, by adopting the *National Cyber Initiative*, by defending the nation from cyber attacks, that Israel becomes the core for Information Technology and lastly by strengthening cooperation between the government, academia, industry, private sector and the security community.

Israel recently incorporated its Military – The Israel Defense Forces (IDF) to protect their cyberspace. They established the IDF Cyber Command; this new unit will work together with the C41 Telecommunications Directorate and the Military Intelligence Directorate (DMI)[3].

Other agencies involved with the Israeli cybersecurity policy encircle the Cyber Authority, the General Security Service of Israel (GSS) and the Mossad [7].

2.4 Japan

Japan's National Cybersecurity Strategy was ratified in 2012; the strategy is based on the *Japan's Cybersecurity Strategy: Towards a World Leading, Resilient and Vigorous Cyberspace policy.*

The strategy comes to support the previous efforts in the national information security area. The ultimate goal of their strategy is to become a cybersecurity nation with a world-leading, resilient and vigorous cyberspace.

Their strategy involves cyber environmental change, the national policy, areas of effort and promotion of systems.

Japanese agencies like the National Information Security Center (NISC), Japan CERT, Cyber Attacks Analysis Council and the Information Security Center Council (ISCP) are responsible for managing national cybersecurity operations, deterrence of cyber threats and remediation.

The Information Security Center Council (ISCP) is operating on three strategies[4] that have been set on middle to long term plan [8]:

First Strategy: At this stage, information security is the national goal to guarantee a sustained economic development. Furthermore, this strategy clarifies roles and responsibilities for all stakeholders including government agencies, critical infrastructure vendors and corporations.

The Second National Strategy on Information Security: This strategy shows escalation from the previous one by hardening capacities, providing rapid response to avoid business disruptions.

Information Security Strategy for Protecting the Nation: While maintaining the preceding strategies, this strategy manages security and crisis, respond to cyber threats and handle large-scale cyber attacks on Japan's soil or internationally.

The Japan Cyber strategy aims to improve government cybersecurity, critical infrastructure, involvement with corporations and academia; to promote cyber space awareness for business and citizens; to implement cybercrime countermeasures and cyberspace defense. They intend to construct a 'Vigorous' cyberspace by activating the country's cybersecurity industry, by improving cybersecurity research and development, to develop the cyber security personnel and the improvement of the cyberspace literacy.

Japan follows common cyber security goals from allies like USA, the European Union, United Kingdom, France, Germany and South Korea.

[1] Canadian Government, *Action Plan 2010-2015 for Canada's Cybersecurity Strategy* (Ottawa: Her Majesty the Queen in Right of Canada 2013), 12

[2] Benoliel, D. *Towards a Cyber Security Policy Model: Israel National Cyber Bureau (INCB) Case Study* (Haifa: The University of Haifa 2014), 6-8

[3] Elran, M. and Siboni, G., 'Establishing an IDF Cyber Command', *The Institute for National Security Studies Insight*, No 719, (July 2015), 1.

[4] Japanese Government, Japan's *Cybersecurity Strategy: Towards a World Leading, Resilient and Vigorous Cyberspace* (Tokio: Information Security Policy Council 2013), 13-14

2.5 Malaysia

The National Cyber Security Policy was approved in 2006. The policy was based on the National Cyber Security Framework, areas like legislation, stakeholder cooperation, technology, institutional and universal acceptance were considered since its inception [9].
The national policy encircles eight pillars and are also identified as Thrust First-Eighth[1]:

- THRUST 1: Effective Governance
- THRUST 2: Legislative & Regulatory Framework
- THRUST 3: Cyber Security Technology Framework
- THRUST 4: Culture of security and Capacity Building
- THRUST 5: Research & Development Towards Self-Reliance
- THRUST 6: Compliance and Enforcement
- THRUST 7: Cyber Security Emergency Readiness
- THRUST 8: International Cooperation

It plans to protect the Critical National Information Infrastructure (CNII) for the most critical sectors of Malaysia:

- National Defence and Security
- Banking and Finance
- Information and Communications
- Energy
- Transportation
- Water
- Health Services
- Government
- Emergency services
- Food and Agriculture

CyberSecurity Malaysia[2] is the government agency responsible for cyber security emergency services, security quality management, InfoSecurity professional development and cyber security strategic engagement and research [10]. The agency manages cyber security strategic policy research, cyber technology research, the malware research centre and the Critical National Information Infrastructure (CNII)[3] portal.

2.6 Norway

Norway cyber security strategy has been active since 2009. The current strategy is based on the *National Security Authority's 2009 Cyber Security Strategy. Four Norwegian Ministries participated to create the national cyber security strategy: The Ministry* of Justice and Public Security, The Ministry of Defence, The Ministry of Transport and Communications and The Ministry of Government Administration, Reform and Church Affairs. Their first national security strategy was implemented back in 2003.
The Cyber Security strategy is focusing on four specific goals [11]:

1 Better coordination and common understanding for information security
2 Robust and secure ICT infrastructure for Norway
3 Good ability to handle adverse ICT threats
4 High level of competence and security awareness for everyone

Special considerations were implemented in order to prevent, detect and fight cybercriminality. Government supports top level national cyber security research and development – Some research initiatives include VERDIKT (Core Competence and Value Creation in ICT), The European Union Seventh Framework Programme for Research and Technological Development and Horizon 2020.
The government agencies that are involved with the strategy are The Norwegian National Security Authority (NSM), NorCERT, The Norwegian Post and Telecommunications Authority (PT), The Norwegian Centre for Information Security (NorSIS), Norwegian Directorate for Civil Protection (DSB), Kripos (National Criminal Investigation Service), Norwegian Intelligence Service (NIS), Norwegian Police Security Service (PST) and The Norwegian Data Protection Authority (DT).

2.7 South Africa

South Africa's Cyber Security policy has been operating since 2010; it is based on the *National Cybersecurity Policy Framework (NCPF)* that was created from National Cybersecurity Strategies like Australia, Japan, Malaysia, United Kingdom and Germany.

[1] Malaysia Government, *National Cyber Security* (Purtrajaya: Minister of Science, Technology and Innovation. ICT Policy Division 2006), 4-5
[2] Malaysia Government, *Cyber Security Malaysia* (The Mines Resort City: Minister of Science, Technology and Innovation 2013),1
[3] http://cnii.cybersecurity.my

The South African Cybersecurity policy intends to involve the government, public and private sectors, society and special interest groups to protect cyberspace from cybersecurity threats. The Framework was supported by the National Cybersecurity Implementation Plan [12].

The Framework was created to address specific areas like cybersecurity measures to fight cyber threats, promotion of a cybersecurity culture, intelligence strengthening to face cybercrime, cyber terrorism and cyber warfare, to protect national critical information infrastructure, to build cybersecurity partnerships and to ensure proper cyber governance for South Africa's cyberspace[1].

The Justice Crime Prevention and Security Cluster (JCPS) is the government agency responsible of the national cyber security strategy by coordinating other government clusters. The National Cyber Security Coordinating Centre and the Computer Security Incident Response Team (CSIRT) exist to support the national cyber security policy.

Other participating South African agencies are The State Security Agency (SSA), The Department of Communications (DoC), The State Information Technology Agency (SITA), The Department of Justice and Constitutional Development (DOJ&CD), The National Prosecution Agency (NPA), The South African Police Service (SAPS), The Department of Defence and Military Veterans (DoD&MV) and The Department of Science and Technology (DST).

2.8 The Netherlands

The Netherlands published their first National Cybersecurity Strategy in 2011, their most current version *National Cyber Security Strategy (NCSS)2: From awareness to capability* updated in 2014 has five strategic objectives[2]:

1. The Netherlands is resilient to cyber attacks and protects its vital interests in the digital domain.
2. The Netherlands tackles cybercrime.
3. The Netherlands invests in secure ICT products and services that protect privacy.
4. The Netherlands builds coalitions for freedom, security and peace in the digital domain.
5. The Netherlands has sufficient cyber security knowledge and skills and invests in ICT innovation to attain cyber security objectives.

The current strategy has an aggressive action plan aligned with the aforementioned strategic objectives. The cybersecurity strategy highlights the importance of cybersecurity, the fight against cyber threats and future challenges to overcome in cyberspace. National and International Vision, Approach and a structured 2014-16 action programme are also part of the new Dutch cybersecurity strategy [13].

The Dutch Cyber Security Council (Nederlandse Cyber Security Raad, CSR) is the national and strategic advisory body responsible for the implementation and development of the national cybersecurity strategy.

2.9 United Kingdom (UK)

The UK has been fighting cyber attacks based on their *National Security Strategy* since 2010. Then the UK Cyber Security strategy was implemented in November 2011 [14].

The National Cyber Security Programme (NCSP) is managed by the Office of Cyber Security and Information Assurance in the Cabinet Office, under the Cabinet Office. The UK has invested in their cyber security strategy **£** 860 million since its inception. The strategy has four key objectives[3]:

1. The UK to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace
2. The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace
3. The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies
4. The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives

Government agencies to support the strategy include intelligence agencies and Ministry of Defence, The Government Communications Headquarters (*GCHQ*), The Defence Cyber

[1] South Africa Government, *South Africa National Cyber Security Policy Framework* (Pretoria: Minister of State Security 2012), 3-16

[2] Netherlands Government, *National Cyber Security Strategy (NCSS)2: From awareness to capability* (Den Haag: National Coordinator for Security and Counterterrorism, Minister of Security and Justice 2014), 7-9

[3] United Kingdom Cabinet Office, *The UK Cyber Security Strategy - Report on progress and forward plans – December 2014* (London: UK Cabinet Office 2014), 8

Operations Group, The Global Operations and Security Control Centre, The Centre for the Protection of National Infrastructure, The Government Office for Science, The Serious Organised Crime Agency (SOCA), The Ministry of Justice, The Home Office, The National Crime Agency (NCA), The Child Exploitation and Online Protection (CEOP), The Metropolitan Police's Police Central E-crime Unit, The National Fraud Intelligence Bureau, UK Computer Emergency Response Team, The Public Services Network (PSN) and The Defence Cyber Protection Partnership (DCPP).

The UK implemented the *Military Cyber Reserves*[1] in 2013, to increase the cadre of cyber security specialists.

With respect to cybersecurity awareness, the UK launched the Cyber Essentials and Cyber Streetwise programmes [2] to improve awareness for organizations and small and medium size businesses; likewise working with ISPs to cyber educate citizens using the Internet Service Providers (ISPs) Guiding Principles publication [15].

And in terms of scientific research, 11 UK universities have joined the 'Academic Centres of Excellence' in the cyber research area[3].

2.10 United States of America (USA)

The US National cyber security strategy has been active since 2003, it is part of the *National Strategy for Homeland Security and complemented by the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. The* Department of Homeland Security (DHS) oversees the National strategy [16].

The cyber strategy includes five national priorities[4]:

1. A National Cyberspace Security Response System
2. A National Cyberspace Security Threat and Vulnerability Reduction Program
3. A National Cyberspace Security Awareness and Training Program
4. Securing Governments' Cyberspace
5. National Security and International Cyberspace Security Cooperation

The priorities have identified a total of 31 major actions and initiatives. The main objectives of this strategy encircle to prevent cyber attacks against their critical infrastructures; to reduce their national vulnerabilities to cyber attacks; and to minimize the damage and recovery time from cyber attacks that do occur.

Some Federal agencies and departments involved with this strategy are Department of the Treasury, Department of Health and Human Services, Department of Energy, Environmental Protection Agency, Department of Agriculture, Department of Agriculture, National Cyberspace Security Response System, National Communications System, the National Infrastructure Protection Center's analysis and warning functions, the Federal Computer Incident Response Center, the Office of Energy Assurance, the Critical Infrastructure Assurance Office, FBI, and the U.S. Secret Service.

Nowadays, The USA is the only country in the world that established a formal international strategy to promote cybersecurity in cyberspace [17].

3. PART II: GLOBAL INTERGOVERNMENTAL ORGANIZATIONS

In this section, we analyze the cybersecurity policies and guidelines that major global governance organizations have implemented. The analysis includes actions, programmes and strategies developed by the United Nations (UN), the *International Telecommunication Union* **(**ITU), the Organisation for Economic Co-operation and Development (OECD), the European Union (EU) and the North Atlantic Treaty Organization (NATO).

3.1 United Nations (UN)

According to the UN, national cybersecurity efforts are categorized in two areas: the first one that only includes national agencies like the law and communication ministries and the last one, where the military holds some kind of a cybersecurity responsibility.

In 2011, 68 out of the 113 UN member states had cybersecurity programmes; 32 states integrated cyberwarfare in their Defense planning and the rest named civilian agencies to be in charge of the national cybersecurity. By 2012, the new UN study showed that 114 states were already considering cybersecurity

[1] United Kingdom Cabinet Office, *The UK Cyber Security Strategy - Report on progress and forward plans – December 2014* (London: UK Cabinet Office 2014), 22

[2] United Kingdom Cabinet Office, *The UK Cyber Security Strategy - Report on progress and forward plans, 7-12*

[3] United Kingdom Cabinet Office, *The UK Cyber Security Strategy - Report on progress and forward plans, 23*

[4] United States of America Government, *The National Strategy to Secure Cyberspace* (Washington D.C.: The White House 2003), 2-4

programmes; 47 states assigned the role to their military forces and 67 were managed by civilian agencies[1].

States in all world regions are implementing or have implemented a national cybersecurity programme. 39 states in Asia, 38 states in Europe, 16 states in the Americas, 18 states in Africa and 3 states in Oceania [18].

The UN Charter puts emphasis in Cyberspace and remarks the need to create confidence building measures and norms. The UN Charter also contains rules on how the work of the member organizations shall be carried out and how the states should behave [19].

China, Russia, Tajikistan, Uzbekistan, Kyrgyzstan and Kazakhstan jointly submitted an inter-national conduct code for information security to the UN general assembly, to seek international norms and to strengthen international coopera-tion[2].

3.2 International Telecommunication Union (ITU)

Due to the fact that cybersecurity covers social, national security and economic activities of any nation, ITU recommends involving as many agents as possible in the policy making of the national cybersecurity strategy. These stakeholders are executive branch, legislative branch, critical infrastructure owners and operators, the judiciary, law enforcement, intelligence community, vendors, academia, international partners and citizens [20].

Once the participants are identified, ITU introduces the strategy elaboration process which includes five stages: Direct and Coordinate Elaboration, Define and Issue Strategy, Sector or Global Cybersecurity Agenda (GCA) Pillar-specific Strategies, Implement Cybersecurity Strategy and Report on Compliance and Efficacy.

ITU highlights that cybersecurity is no longer a computer security issue but rather a national policy matter. They have created a reference model that can be used to elaborate national cybersecurity strategies and it also strengthens capacity building to implement the national cybersecurity strategy and utilize all the resources to mitigate risks.

ITU also presents the Global Cybersecurity Agenda (GCA)[3] which is a holistic framework for coordinating, developing and implementing a powerful global cybersecurity culture. The GCA is based on five pillars: legal measures, technical and procedural measures, organisational structures, capacity building and international cooperation.

In addition, they have drafted a national cybersecurity strategy, which is presented as a reference model for national administrators seeking advice on policy making to create or to improve their national cybersecurity policy.

3.3 The Organisation for Economic Co-operation and Development (OECD)

The OECD completed a comparative analysis study related to national cyber security strategies in 2012. The scope of the research included ten countries which eight have already adopted a national strategy at the time (Australia, Canada, France, Germany, Japan, Netherlands, the UK and the USA) and two countries which were developing their cybersecurity strategy (Spain and Finland). Non-governmental stakeholders like the Business and Industry Advisory Committee to the OECD (BIAC), Civil Society Internet Society Advisory Council (CSISAC) and the Internet Technical Advisory Committee (ITAC) were engaged in the study. The OECD strongly believes that security in cyberspace is a key driver for social development and economic prosperity [21].

The study highlights that cybersecurity is now a national priority, Internet and ICT are crucial for country development thus the complexity of cyber threats are continually growing.

Cyber security strategies must be directed by the government and an integrated approach is required. Cybersecurity policy is a matter of national priority; the engagement of public and private institution cooperation is highly advisable; international cooperation ought to improve and strategies have to place the highest levels of respect to freedom of speech, privacy and free flow of information.

The research also discovered emerging trends on sovereignty in cybersecurity policy making that covers national and international security, defense, military and intelligence; the flexibility when approaching cybersecurity policy making; the importance of economic factors for strategies and the benefits of involving multiple stakeholders[4].

Action plans of the national cybersecurity strategies are reinforced and broadened in the government security,

[1] UN Institute for Disarmament Research, *The Cyber Index: International Security Trends and Realities* UNIDIR/2013/3 (Geneva: UNIDIR 2013), 1-3

[2] UN General Assembly, *Group of Governmental Experts on Developments in the field of Information and Telecommunications in the Context of Internal Security* A/69/723. (New York: UN General Assembly 2015), 1

[3] *International Telecommunication Union, ITU National Cybersecurity Strategy Guide (*Geneva**:** *Edited by Frederick* Wamala 2012), Ch.4, 19-21

[4] The Organisation for Economic Co-operation and Development, Cybersecurity *Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy* (Paris: OECD Publishing 2012), 14-16

the protection of critical information infrastructures, cybercrime fight, awareness raising, education, cyber attacks response and research and development areas (R&D).

The conclusions established that international cooperation must improve, cross-border interdependencies of critical information infrastructures are barely addressed and that cybersecurity policy making have to be redefined according to new levels of maturity of the existing strategies by facing higher levels of complexity.

3.4 The European Union (EU)

The EU has implemented a cybersecurity strategy for its members. It was proposed by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy including cybersecurity vision, clarifying roles and setting out the action plan to make the EU's cyberspace the safest worldwide. The EU wants to guarantee that the core values in cyberspace are ensuring to the citizens: Protection of fundamental rights, freedom of speech, privacy, personal data and Internet for all. And to fight cybercrime and to promote cyber resilience the EU Commission established the European Network and Information Security Agency (ENISA) in 2004 [22].

In *Figure 1* the EU introduced and organized all different agencies in order to prevent and respond to cyber threats, the level of coordination between EU and National agencies are based on cybersecurity, law enforcement and defence divisions.

Nevertheless, ENISA is responsible for creating the guides for Member States to managing the national cybersecurity strategies [23]. According to ENISA a national cybersecurity strategy is *'A tool to improve the security and resilience of national information infrastructures and services. It is a high-level, top-down approach to cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe. As such, it provides a strategic framework for a nation's approach to cyber security.'* [1]

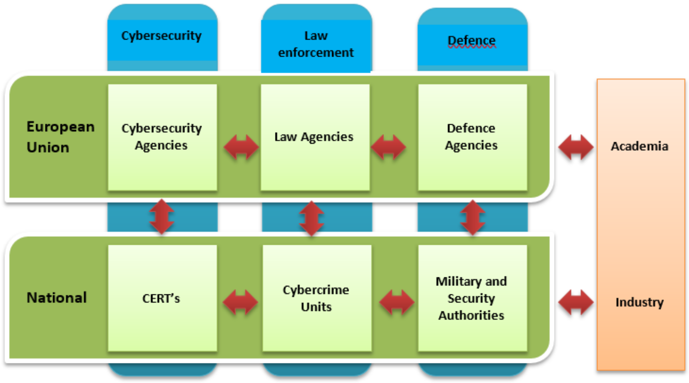

Fig. 1. Coordination between EU and National Agencies

ENISA also provides a national cybersecurity strategy lifecycle that in its foundation includes developing and executing the cyber strategy and afterwards, following an assessment and adjustment of the strategy.

3.5 The North Atlantic Treaty Organization (NATO)

NATO proposes a National Cybersecurity Strategy (NCS) framework that contains three pillars which are mandates, dimensions and dilemmas[2].

Five mandates which will need a proper management of incident cycle [24]:

1. Cyber Diplomacy & Internet Governance
2. Critical Infrastructure & Crisis Management
3. Intelligence & Counter-Intelligence
4. Military Cyber
5. Counter Cyber Crime

The Three Dimensions are different stakeholder groups that ought to be considered on any NCS strategy's nation. One of the biggest challenges is somehow bring into play the lessons learned from any security policy and successfully implement them through public policy to the NCS:

1. Government
2. National actors
3. International and Transnational groups

[1] European Network and Information Security Agency, *National Cyber Security Strategies: Practical Guide on Development and Execution* (Heraklion: ENISA 2012), 2

[2] North Atlantic Treaty Organization, *National Cybersecurity framework manual* (Tallin: Edited by Alexander Klimburg, NATO CCD COE Publication 2012), Ch.1, 29-43

And the Five Dilemmas that try to balance between costs and benefits that will have repercussions on citizen freedoms, economic growth and NCS requirements:

1. Stimulate the economy versus improve national security
2. Infrastructure modernisation versus critical infrastructure protection
3. Private sector versus public sector
4. Data protection versus information sharing,
5. Freedom of expression versus political stability

NATO concludes that creating a NCS strategy cannot be put in practice as a unique model for every country; the bottom line is how to address the cyber challenges of any modern state and by means of conceiving them at all government levels.

4. PART III: CYBERSECURITY FRAMEWORKS

This section provides a general overview of the major cybersecurity frameworks[1] that have been established in different industries and sectors like government, military, critical infrastructure, health, information security, information technology, credit card and security [25].

4.1 (ISC)^2 CBK

The Common Body of Knowledge was created by the International Information Systems Security Certification Consortium (ISC)$^{2.}$
It contains ten security domains:

1) Access Control
2) Telecommunications and Network Security
3) Information Security Governance and Risk Management
4) Software Development Security
5) Cryptography
6) Security Architecture and Design
7) Security Operations
8) Business Continuity and Disaster Recovery Planning
9) Legal, Regulations, Investigations and Compliance
10) Physical Security

4.2 ISO 27032:2012[2]

The International Organization for Standardization 27032:2012 was prepared by the Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*. The international standard provides guidance to fight cybersecurity risks like social engineering attacks, hacking, malware proliferation and unwanted software. It includes controls like cyberattack preparedness, detection and monitoring of attacks thus responsiveness to cyber threats.
The standard provides a definition of stakeholders, describing their roles in cybersecurity, guidance to address cybersecurity issues and a framework to activate stakeholder participation on resolving cyber issues.

4.3 NIST SP800-53

Revisions 3 and 4 were created by the US National Institute of Standards and Technology (NIST). The document contains security controls for US federal computer systems. Revision 4 covers 224 controls categorized in 18 families:

1) Access control
2) Awareness and training
3) Audit and accountability
4) Security assessment and authorization
5) Configuration management
6) Contingency planning
7) Identification and authentication
8) Incident response
9) Maintenance
10) Media protection
11) Physical and environmental protection
12) Planning
13) Personnel security
14) Risk assessment
15) System and services acquisition
16) System and communications protection
17) System and information integrity
18) Program management

[1] Donaldson, S. and Siegel, S., *Enterprise cybersecurity: How to build a successful cyberdefense program against advanced threats* (New York: Apress 2015) Appendix B, 297-309

[2] https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

4.4 NIST Cybersecurity Framework (2014)

This cybersecurity framework was established to comply with US executive order 13636, while it complements NIST SP800-53; it is more oriented towards cybersecurity operations and response process. The framework is organized in five functions, 22 categories and 98 subcategories.
The main functions include Identify, Protect, Detect, Respond and Recover to cybersecurity threats.

4.5 DHS Cyber Resilience Review (CRR)

The US Department of Homeland Security (DHS) conceived the Cyber Resilience Review (CRR) framework to assess cybersecurity capabilities thus cyber resilience within critical infrastructure and crucial resources sectors.

The CRR is assembled in ten domains:

1. Asset management
2. Controls management
3. Configuration and Change management
4. Vulnerable management
5. Incident management
6. Service continuity management
7. Risk management
8. External dependency management
9. Training and awareness
10. Situational awareness

4.6 Council on Cybersecurity Critical Security Controls

The Center for Internet Security (CIS) recently introduced CIS Controls for Effective Cyber Defense Version 6.0
The CIS controls are a collection of internal cyber hygiene measures to be implemented in order to protect IT networks.
The framework is divided in 20 Critical Security Controls:

1. Inventory of authorized and unauthorized devices
2. Inventory of authorized and unauthorized software
3. Secure configurations for hardware and software
4. Continuous vulnerability assessment and remediation
5. Controlled use of administrative privileges
6. Maintenance, monitoring and analysis of audit logs
7. Email and web browser protections
8. Malware defences
9. Limitation and control of network ports
10. Data recovery capability
11. Secure configurations of network devices
12. Boundary defense
13. Data protection
14. Controlled access based on the need to know
15. Wireless access control
16. Account monitoring and control
17. Security skills assessment and appropriate training to fill gaps
18. Application software security
19. Incident response and management
20. Penetration tests and red team exercises

4.7 Australian Defense Signals Directorate (DSD) to mitigate targeted cyber intrusions

This is published by the Australian Defense Signals Directorate (DSD) and its last revision is from 2014. The top four strategies are mandatory for all Australia Government agencies. There are 35 existing controls to mitigate cyber intrusions:

1) Application whitelisting
2) Patch applications
3) Patch operating system vulnerabilities
4) Restrict administrative privileges
5) User application configuration hardening
6) Automated dynamic analysis
7) Operating system generic exploit mitigation mechanisms
8) Host-based Intrusion Detection/Prevention System
9) Disable local administrator accounts
10) Network segmentation and segregation
11) Multi-factor authentication
12) Software-based application firewall, blocking incoming network traffic
13) Software-based application firewall, blocking outgoing network traffic
14) Non-persistent virtualised sandboxed trusted operating environment

15) Centralised and time-synchronised logging of successful and failed computer events
16) Centralised and time-synchronised logging of allowed and blocked network events
17) Email content filtering
18) Web content filtering
19) Web domain whitelisting for all domains
20) Block spoofed emails
21) Workstation and server configuration management
22) Antivirus software using heuristics and automated internet-based reputation ratings
23) Deny direct internet access from workstations
24) Server application security configuration hardening
25) Enforce a strong passphrase policy
26) Removable and portable media control
27) Restrict access to Server Message Block (SMB) and NetBIOS services
28) User education
29) Workstation inspection of Microsoft Office files
30) Signature-based antivirus software
31) TLS encryption between email servers
32) Block attempts to access web sites by their IP address
33) Network-based Intrusion Detection/Prevention System
34) Gateway blacklisting
35) Capture network traffic

4.8 PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is the global standard that ensures payment card data security.
The Global standard version 3.1 covers six areas and 12 requirements:

Build and maintain a secure network and systems

1) Install and maintain a firewall configuration to protect cardholder data
2) Do not use vendor-supplied defaults for system passwords and other security parameters

Protect cardholder data

3) Protect stored cardholder data
4) Encrypt transmission of cardholder data across open, public networks

Maintain a vulnerability management program

5) Protect all systems against malware and regularly update anti-virus software or programs
6) Develop and maintain secure systems and applications

Implement strong access control measures

7) Restrict access to cardholder data by business need to know
8) Identify and authenticate access to system components
9) Restrict physical access to cardholder data

Regularly monitor and test networks

10) Track and monitor all access to network resources and cardholder data
11) Regularly test security systems and processes

Maintain an Information Security Policy

12) Maintain a policy that addresses information security for all personnel

4.9 HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule specifies US standards for protecting the confidentiality, integrity and availability of the Electronic Protected Health Information (EPHI) for health plans, clearinghouses and healthcare providers.
22 cybersecurity standards are organized in five different areas:

Administrative Safeguards

1) Security management process
2) Assigned security responsibility
3) Workforce security
4) Information access management
5) Security awareness and training
6) Security incident procedures
7) Contingency plan
8) Evaluation
9) Business associate contracts and other arrangements

Physical Safeguards

10) Facility access controls
11) Workstation use
12) Workstation security
13) Device and media controls

Technical Safeguards

14) Access controls
15) Audit controls
16) Integrity
17) Person or entity authentication
18) Transmission security

Organizational Requirements

19) Business associate contracts or other arrangements
20) Requirements for group health plans

Policies, Procedures and Documentation Requirements

21) Policies and procedures
22) Documentation

4.10 HITRUST Common Security Framework (CSF)

The Health Information Trust Alliance (HITRUST) created the CSF to normalize the security requirements for healthcare institutions, US federal agencies, US State legislation, industry frameworks and the industry-specific to improve critical infrastructure cybersecurity.
The HITRUST CSF is made of 13 control categories, 42 control objectives and 135 control specifications.
These are the main security control areas:

1) Information security management program
2) Access control
3) Human resources security
4) Risk management
5) Security policy
6) Organization of information security
7) Compliance
8) Asset management
9) Physical and environmental security
10) Communications and operations management
11) Information systems acquisition, development and maintenance
12) Information security incident management
13) Business continuity management

4.11 NERC CIP Cybersecurity Version 5

The North American Electric Reliability Corporation (NERC) introduced the Critical Infrastructure Protection (CIP) Cybersecurity version 5 in 2013. This version is oriented towards a major progress in mitigating cyber threats to the bulk power system.
The NERC CIP version 5 contains ten areas with 32 cybersecurity requirements:

1) CIP-002 Critical cyber assets
2) CIP-003 Security management controls
3) CIP-004 Personnel and training
4) CIP-005 Electronic security
5) CIP-006 Physical Security
6) CIP-007 Systems security management
7) CIP-008 Incident reporting and response planning
8) CIP-009 Recovery plans for Bulk Electric System (BES) cyber assets
9) CIP-010 Configuration changes and vulnerability assessments
10) CIP-011 Information protection

5. PART IV: MAIN COMPONENTS OF A NATIONAL CYBERSECURITY STRATEGY

In this section, we present a National CyberSecurity Strategy Model (NCSSM) that is based on our research. The NCSSM (Figure 2) contains eight pillars that are in constant interaction and it includes certain input features to become effective. As a result, specific outcomes are in need to be assessed continually due to the changing nature of cyberspace.
Our Model is based on the recommendations that the ITU, NATO, OECD and EU introduced to include key aspects, stakeholders, components and pillars of any NCSS.

Input

This section requires a clear definition of the scope of the national cybersecurity strategy. Ideally, a clear understanding in terms of protecting critical information infrastructure must be achieved.
Mission, Vision, Objectives and Goals of the national cybersecurity strategy are identifiable at this stage.

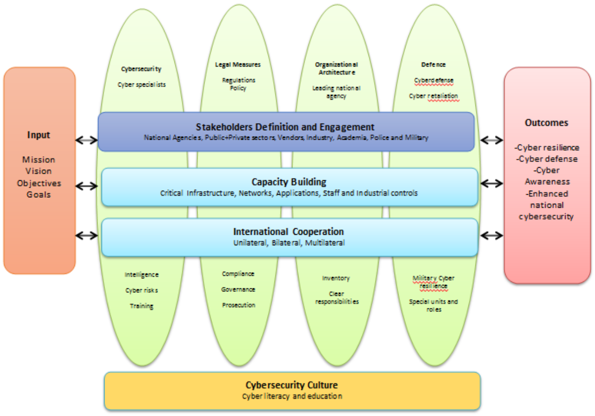
Cybersecurity
Cyber specialists
Legal Measures
Regulations
Policy
Organizational Architecture
Leading national agency
Defence
Cyberdefense
Cyber retaliation
Input
Mission
Vision
Objectives
Goals
Stakeholders Definition and Engagement
National Agencies, Public+Private sectors, Vendors, Industry, Academia, Police and Military
Capacity Building
Critical Infrastructure, Networks, Applications, Staff and Industrial controls
International Cooperation
Unilateral, Bilateral, Multilateral
Outcomes
-Cyber resilience
-Cyber defense
-Cyber Awareness
-Enhanced national cybersecurity
Intelligence
Cyber risks
Training
Compliance
Governance
Prosecution
Inventory
Clear responsibilities
Military Cyber resilience
Special units and roles
Cybersecurity Culture
Cyber literacy and education

Fig. 2. The National CyberSecurity Strategy Model (NCSSM)

The Pillars

1. Cybersecurity Culture is the main pillar that supports the other pillars. How citizens and society apply the use of cyber security measures

2. Stakeholders definition and engagement: A national agency will be in charge of the NCSS creation and implementation. All stakeholders must be identified with clear roles and responsibilities.
3. Capacity Building: All necessary measures must be taken to ensure protection from cyber threats, risks and vulnerabilities. Baseline security requirements for each sector must be defined including a minimum set of cyber security measures. Specific cybersecurity standards and frameworks are selected. A cadre of cybersecurity professionals must be recruited.
4. International Cooperation: Countries need to be involved with the cybersecurity policy making leaders including developed nations and intergovernmental organizations due to the international nature of cyber threats.
5. Cybersecurity: This pillar helps to achieve a strong cybersecurity framework and work in harmony with all different stakeholders to ensure jurisdiction. Procedural measures include accountability, risk management, security policing, compliance and assurance. Lastly, the technical measures are aligned with core systems and networks in terms of administration, identifying cyber threats, inspections, IT health monitoring and audits.
6. Legal Measures: Countries must engage in creating modern laws, policies to fight and prosecute cybercrime. Develop cyberlaw capacity including police, private sector, judicial and legislative branches.
7. Organizational Architecture: This pillar is fundamental to define the NCCS coordinator and the different agencies that participate at the national level. Participating agencies are responsible to lead cybersecurity activities in all industries and sectors. A National CERT is defined
8. Defense: Military forces and national security agencies are prepared to develop some kind of military cyber capability in protecting defense networks, cyber warfare activities, enabling network centric warfare or manage cyber warfare strategies.

Outcomes

Valid outcomes of NCSS must be continually evaluated using key performance indicators and objective performance metrics.
Cyber defense, Awareness, Cyber resilience and Enhancement of national cybersecurity output are the main components in this final phase.

6. PART V: CYBERSECURITY STRATEGY KNOWLEDGE TRANSFER TO OTHER COUNTRIES

Despite the fact, that many nations have already implemented or are planning to implement a national cybersecurity strategy, very little efforts are targeted towards the contribution of international cybersecurity standardization, defining jurisdiction in international cyberspace or the contribution from developed nations to help developing countries to establish an initial cybersecurity programme, policy or strategy.
There are just a few exceptions that can initiate the knowledge transfer, international cooperation and lessons learn sharing in these areas.
Hence, existing national cybersecurity strategies include very little details for international cooperation in cybersecurity matters but in most cases this topic is inexistent or country leaders in cybersecurity topics are not interested in this kind of international cooperation. Nowadays, many countries are joining to fight back the Islamic State of Iraq and the Levant (ISIL). The global coalition mostly counters strikes when a terrorist attack did afflict a nation. A very similar approach must be taken to defining a broader international cooperation to fight cybercrime, coordinate cybersecurity efforts and initiate a more aggressive approach for cyber governance and cybersecurity policy-making.
Countries like the USA, the UK and the Netherlands have a more consistent approach to international cooperation in cybersecurity matters.
The United States developed the *International Strategy for Cyberspace* that consists on core principles to

support cyberspace operations like fundamentals freedoms, respect for property, safeguard privacy, protection from cybercrime and the right of cyber self-defense[1]. The strategy intends to provide knowledge transfer to build cybersecurity capacity, to continually develop and share cybersecurity best practices, to enhance the ability to fight cyber criminality and to develop relationships with policy makers.[2]

The UK promoted an international dialogue at the London Conference on Cyberspace for the sake of developing international norms in cyberspace and The Netherlands through their national Cyber Security Council wish to collaborate with other countries to strengthen its international orientation. The Dutch Cyber Security Council wishes to expand the international network collaboration to develop national views.

6. CONCLUSION

This paper has focused on analyzing leading countries and intergovernmental institutions perspectives regarding the creation, policy making, structure, implementation and sustaining national cybersecurity strategies.

The content of the national strategies varies widely and each country structures the strategy based on their needs related to fight cybercrime, critical infrastructure protection, stakeholders engagement, cybersecurity awareness, cyber resilience, cyber intelligence gathering, cyber attacks alertness and eradication, cyber incident response, cybersecurity research and development, cyber police organization, communication, military involvement, law and judiciary collaboration, cyber governance and international cooperation.

As a result of our research, we present ‘The National CyberSecurity Strategy Model (NCSSM)’ that contains eight pillars: Cybersecurity Culture, Stakeholders definition and engagement; Capacity Building; International Cooperation; Cybersecurity; Legal Measures; Organizational Architecture; and Defense. The Model requires specific input features and the outcome is measured in terms of cyber defense, cyber awareness, cyber resilience and national cybersecurity.

We also included an overview of the major cybersecurity frameworks that are instrumental to support national cybersecurity strategies.

Some countries have a higher level of maturity than others when dealing with cyberspace, cybersecurity and national cybersecurity strategy policy-making.

These leading countries have to recognize the importance of international cooperation, alliance developent to fight cybercrime, rule cyberspace and knowledge transfer of cybersecurity strategy matters.

Future research will need to focus on the development of international standards and regulations to tackle cybercrime, to expand international cooperation in cybersecurity and national strategies. The challenges to overcome are to secure nations and global cyberspace while creating dynamic cybersecurity strategies.

REFERENCES

[1] Greiman, Virginia, Cyber Security and Global Governance, Proceedings of the 14th European Conference on Cyber Warfare & Security, Hattfield: University of Hertfordshire, 2015

[2] Australian Government, Defence white paper 2013, Canberra: Department of Defence, Commonwealth of Australia, 2013

[3] Australian Government, Strong and Secure: A Strategy for Australia’s National Security, Canberra: Department of the Prime Minister and Cabinet, Commonwealth of Australia, 2013

[4] Canadian Government, Canada’s Cybersecurity Strategy for a Stronger and More Prosperous Canada, Ottawa: Her Majesty the Queen in Right of Canada, 2010

[5] Canadian Government, Action Plan 2010-2015 for Canada’s Cybersecurity Strategy, Ottawa: Her Majesty the Queen in Right of Canada, 2013

[6] Benoliel, D. Towards a Cyber Security Policy Model: Israel National Cyber Bureau (INCB) Case Study, Haifa: The University of Haifa, 2014

[7] Elran, M. and Siboni, G., ‘Establishing an IDF Cyber Command’, The Institute for National Security Studies Insight, No 719, July 2015, pp. 1-3.

[8] Japanese Government, Japan’s Cybersecurity Strategy: Towards a World Leading, Resilient and Vigorous Cyberspace, Tokio: Information Security Policy Council, 2013

[9] Malaysia Government, Cyber Security Malaysia, The Mines Resort City: Minister of Science, Technology and Innovation, 2013

[10] Malaysia Government, National Cyber Security, Purtrajaya: Minister of Science, Technology and Innovation. ICT Policy Division, 2006

[11] Norway Government, Cyber Security Strategy for Norway, Oslo: The Ministry of Government Administration, Reform and Church Affairs, 2013

[12] South Africa Government, South Africa National Cyber Security Policy Framework, Pretoria: Minister of State Security, 2012

[13] Netherlands Government, National Cyber Security Strategy (NCSS)2: From awareness to capability, Den Haag: National Coordinator for Security and

[1] United States of America Government, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington D.C: The White House 2011), Ch. 1, 5

[2] United States of America Government, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, 10-15*

Counterterrorism, Minister of Security and Justice, 2014

[14] United Kingdom Cabinet Office, The UK Cyber Security Strategy - Protecting and promoting the UK in a digital world, London: UK Cabinet Office, 2011

[15] United Kingdom Cabinet Office, The UK Cyber Security Strategy - Report on progress and forward plans, London: UK Cabinet Office, 2014

[16] United States of America Government, The National Strategy to Secure Cyberspace, Washington D.C.: The White House, 2003

[17] United States of America Government, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, Washington D.C: The White House, 2011

[18] UN Institute for Disarmament Research, The Cyber Index: International Security Trends and Realities, Geneva: UNIDIR, 2013

[19] UN General Assembly, Group of Governmental Experts on Developments in the field of Information and Telecommunications in the Context of Internal Security A/69/723, New York: UN General Assembly, 2015

[20] International Telecommunication Union, ITU National Cybersecurity Strategy Guide, Geneva: Edited by Frederick Wamala, 2012

[21] The Organisation for Economic Co-operation and Development, Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy, Paris: OECD Publishing, 2012

[22] European Union, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels: European Commission, 2013

[23] European Network and Information Security Agency, National Cyber Security Strategies: Practical Guide on Development and Execution, Heraklion: ENISA, 2012

[24] North Atlantic Treaty Organization, National Cybersecurity framework manual, Tallin: Edited by Alexander Klimburg, NATO CCD COE Publication, 2012

[25] Donaldson, S. and Siegel, S. Enterprise cybersecurity: How to build a successful cyberdefense program against advanced threats, New York: Apress, 2015.

AUTHOR PROFILES:

Regner Sabillon, C|CISO, ITIL, CGEIT, CRISC, ISO 27001 LA, I.S.P., ITCP, MBA, M.Sc.
Ph.D. Candidate at Universitat Oberta de Catalunya (UOC), Spain, Canadian researcher in Cybersecurity, Cyber law, Cyberforensics and Cybercrime areas. Instructor at Athabasca University, Canada and ICT specialist with more than 20 years of experience.

Victor Cavaller, Ph.D., M.Sc.
He is a Professor in the Department of Information and Communication Sciences at the Open University of Catalonia (UOC) and in the Faculty of Business at the Universitat Abat Oliva CEU, Spain.

Jeimy Cano, Ph.D, CFE.
Dr. Jeimy Cano is a Law Faculty Distinguished Professor at Universidad de los Andes (Uniandes) in Bogota- Colombia, a researcher and founder member of Research Group on electronic commerce, telecommunications and computing.