Global Network of Interdisciplinary Internet & Society Research Centers
NoC Internet Governance Case Studies Series

TOWARDS A CYBER SECURITY POLICY MODEL: ISRAEL NATIONAL CYBER BUREAU (INCB) CASE STUDY

By: Daniel Benoliel
Haifa Center of Law and Technology (HCLT)
The University of Haifa Faculty of Law

July 2014

ABSTRACT

Design and implementation of a cyber security legal policy model is an ambitious endeavor. This policy brief offers primary guidelines focusing on the national level. It uses Israel's recently established National Cyber Bureau (INCB) cyber command funneled by its national cyber policy as a case in point. In so doing the brief offers a cross-section comparison between leading cyber security national policies of the United States, United Kingdom, Canada, Japan and the Netherlands.

It further introduces comparable policies including the balancing of cyber security with civil liberties, cyber crime policy, adherence to international law and international humanitarian law, forms of regulation (technological standards, legislation, courts, markets or norms) and prevalent forms of cooperation (intra-governmental, regional, public-private platform (PPP) and inter-governmental cooperation).

Ultimately this brief could facilitate academic-government cooperation over the design of an archetypical cyber security policy model for countries henceforth.

Table of Contents:

Introduction

Recent revelations about the United States National Security Agency's (NSA) clandestine mass electronic surveillance data mining projects raised a public debate worldwide over the legality of governmental compliance with democratic principles.[1] From a legal policy perspective designing the nooks and crannies of cyber security is challenging for two decisive reasons. At a start, the field is largely shrouded with much secrecy and over classification. In addition, the traditional major stakeholders in the field are national defense and intelligence organs.

This excessive secrecy in the Israeli case and elsewhere is already burdensome in current policy initiatives.[2] Not surprisingly, the original attempts to regulate cyber security for the private sector started and are still predominantly restricted to technological standard setting and governmental-industry cooperation thereof. To date four such endeavors are much prevalent. These are the highly popular International Organization for Standardization (ISO)'s ISO 27001 as early as 2005,[3] and 27002[4] -

[1] A key example is the PRISM project. Prism gathers Internet communications derived from demands made to Internet companies such as Yahoo! Inc. It does so under Section 702 of the FISA Amendments Act of 2008 in order to yield any data that counterparts court-approved search terms. *See* Barton Gellman and Ashkan Soltani, NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, The Washington Post (30 October 2013).

[2] Lior Tabansky, The Chair of Cyber Defense, Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University, Israel, January 2013 - Article n° III.12, available at: http://sectech.tau.ac.il/sites/default/files/publications/article_3_12_-_chaire_cyberdefense.pdf, at 2. In an interview with Mr. Tal Goldstein from the Israeli National Cyber Bureau (21 September 2014) it was further emphasized that to a large extent commercial enterprises themselves withhold their cooperation with INCB cyber defense organs due to commercially-related secrecy concerns. *Id.* (file with author).

[3] ISO, An Introduction To ISO 27001 (ISO27001), at: http://www.27000.org/iso-27001.htm (labelled as "*specification for an information security management system (ISMS)*").

[4] ISO, Introduction To ISO 27002 (ISO27002), at: http://www.27000.org/iso-27002.htm (offering *"guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.*")

two cyber security standards offering ISO/IEC voluntary certifications for complying businesses. In addition, one should mention the Information Security Forum's (ISF) Standard of Good Practice for Information Security (SoGP) covering a spectrum of information security arrangements to keep business risks associated with information systems,[5] the Software Assurance Maturity Model (SAMM) best practices in software security,[6] and lastly the Cloud Security Alliance (CSA) best practices for cloud computing.[7] In the backdrop of this technical orientation towards cyber security, the focus has thus gradually been shifting onto other stakeholders interested in internet governance-related policy. Such stakeholders typically preside within academia, international non-governmental initiatives and governments.

To date, numerous governments have already taken on this initiative whilst offering the most advanced sets of cyber security policies. These are noticeably the United States,[8] the United Kingdom,[9] Canada,[10] Japan,[11] Germany,[12] the

[5] See The Information Security Forum's (ISF) Standard of Good Practice for Information Security (SoGP), at https://www.securityforum.org/tools/sogp/.

[6] *See* The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security. *See* Common Assurance Maturity Model (CAMM) Software Assurance Maturity Model: A guide to building security into software development Version - 1.0, available at: http://www.opensamm.org/downloads/SAMM-1.0.pdf, at 3. The building blocks of the model are the three maturity levels defined for each of the twelve security practices. *Id*. These define a wide variety of activities in which an organization could engage to reduce security risks and increase software assurance. *Id*.

[7] *See* Cloud Security Alliance (CSA), Security Guidance for Critical Areas of Focus in Cloud Computing (3rd ed., 2011), at https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf. (CSA's best practices cover potential legal issues when using cloud computing. These include protection requirements for information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements, international laws, etc.) at 35-37.

[8] See generally, Barak Obama. Executive Order – Improving Critical Infrastructure Cybersecurity, February 12, 2013; The White House, Presidential Policy Directive – Critical Infrastructure and Resilience, February 12, 2013 (PDD-21); H.R. 3696, 13TH Congress 1st Session., *National Cybersecurity and Critical Infrastructure Protection Act of 2013;* U.S Department of Homeland Security, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience; Barak Obama, International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World, The White House (May 2011); National Infrastructure Advisory Council, Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations (October 14, 2008); The White House, Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (December 17, 2003) (HSPD-7); The White House, Presidential Decision Directive/NSC-63, (May 22, 1998); White House, Presidential Decision Directive 63: Policy on Critical Infrastructure Protection (Washington, DC: U.S, Government Printing Office, 1998); The President's Commission on Critical Infrastructure Protection (PCCIP), Critical Foundations: Protecting America's Infrastructures, Washington, October 1997. PCCIP does not exist today. Its functions have been reallocated per HSPD-7.

[9] For Great Britain's 2009 policy initiative, see, UK Cabinet Office, Cyber Security Strategy of the United Kingdom: Safety, security and resilience in cyber space (London: The Cabinet Office, CM 7642, June 2009), at: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf.

[10] *See* Government of Canada, Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada, (2010), at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

[11] Information Security Strategy for protecting the nation (2013). See, earlier the Japanese Information Security Policy Council released the Information Security Strategy for Protecting the Nation, (May 11, 2010), at: http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf.

[12] *See* Federal Ministry of the Interior, Cyber Security Strategy for Germany (February 2011), at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile.

Netherlands,[13] or Israel's establishment of an Israel National Cyber Bureau (INCB) in 2011. These national initiatives have also served to construct cyber security threats as predominantly national instead of merely global or international.[14] This policy brief focuses on the national level within this natural regulatory flow.

Other stakeholders have also begun initiating equivalent policies. To mention but a few, the NetMundial platform noticeably offers a vibrant bottom-up NGO-based alternative.[15] This perceptible platform directly indicates as one of its seven principles for internet governance: *"Security, stability and resilience of the internet should be a key objective"* and elsewhere *"Effectiveness in addressing risks and threats to security and stability of the Internet depends on strong cooperation among different stakeholders."*[16] Similarly, the Organization for Security and Cooperation in Europe (OSCE) has been discussing cyber security issues for numerous years, offering yet another multinational discussion platform. To illustrate, at the OSCE Summit held in 2010, in Astana, Kazakhstan the Heads of State and Government of the 56 participating States of the OSCE underlined that ‘‘*greater unity of purpose and action in facing emerging transnational threats*” must be achieved, whilst offering for an international "*security community"*.[17] The *Astana Commemorative Declaration* significantly mentions cyber threats as one of these emerging transnational threats abridging the north-south divide between developed and developing countries.[18] Yet in vie with the NetMundial platform, OSCE's Summit has not yielded more concrete cyber security recommendations to date.

Lastly, a landmark decision recently has taken place at the United Nations (UN). For the first time in 2013 a group of governmental experts from fifteen member states have agreed to acknowledge the full applicability of international law and state responsibility to state behavior in cyberspace.[19] That is, by extending traditional transparency and confidence-building measures, and by recommending international

---

[13] *See* National Cyber Security, Strategy 2: From awareness to capability (2013). Beforehand see also Ministry of Science and Justice, The National Cyber Security Strategy (NCSS), The Ministry of Security and Justice, the Netherlands (2011).

[14] Brigid Grauman, Cyber-Security: The Vexed Question of Global Rules: An Independent Report on Cyber-Preparedness around the World, edited by Security & Defence Agenda (SDA) and McAfee Inc. Brussels: Security & Defence Agenda (SDA), 2012 [hereafter, 'the Security & Defence Agenda (SDA) report'], at 66-67.

[15] The NetMundial platform is a voluntary bottom-up, open, and participatory process involving thousands of people from governments, private sector, civil society, technical community, and academia worldwide on Internet governance ecosystem. *See* http://giplatform.org/events/netmundial.

[16] NetMundial Multi stakeholder Statement (April, 24th 2014), at: http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf, at 5 (defined as one of NetMundial's seven principles, titled: "*Security and stability and resilience of the internet*"). The statement is a result of NetMundial's first conference held in Sao Paulo, Brazil between 23-24 April 2014.

NetMundial's "*Roadmap for the Further Evolution of the internet governance ecosystem*" Part (2)III(1)(a) (titled: "*Security and stability*") in part (2) dealing with specific internet governance topics - further reiterates international cooperation "*on topics such as jurisdiction and law enforcement assistance to promote cyber security and prevent cybercrime."* See http://content.netmundial.br/contribution/roadmap-for-the-further-evolution-of-the-internet-governance-ecosystem/177.

[17] The Astana Commemorative Declaration: Towards a Security Community (3 December 2010), at: http://www.osce.org/cio/74985?download=true.

[18] *Id*. Article 9.

[19] *See*, UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, June 24, 2013.

cooperation making information and communications technology (ICT) infrastructure more secure against cyber threats worldwide. Be that as it may, the decision has not yet become costmary international law and is still nonbinding within public international law.

The issue of information security surely has been on the United Nations agenda in view of the fact that the Russian Federation in 1998 first introduced a draft resolution in the First Committee of the UN General Assembly.[20] Since then there are annual reports by the Secretary-General to the General Assembly with the views of UN member states. There have also been three Groups of Governmental Experts (GGE) that have reviewed present and future cyber threats and cooperative measures.[21]

In the backdrop of these surfacing initiatives, this policy brief offers a comparable review of Israel's National Cyber Bureau (INCB) established in 2011. The brief may ultimately assist in constructing a comprehensive national cyber security policy model partially based on Israel's example as well as those of the United States, United Kingdom, Canada, Japan and the Netherlands.

A question remains: why Israel? Two significant reasons come to mind. First, Israel's cyber defense apparatus is world renowned and is considered a top leading one. To illustrate, an international comparative study of twenty-three developed countries put by a Brussels' security and defense think-tank within a Security & Defense Agenda's (SDA) cyber-security initiative, recently awarded Israel with a top grade on 'cyberdefense', alongside Sweden and Finland.[22] Yet unlike these two benevolent Scandinavian countries, Israel sees approximately one-thousand cyber-attacks within a hierarchy of threats every minute.[23] A second reason follows. According to Israel's National Cyber Bureau, Israeli remarkably exports cyber-related products and services more than all other nations combined apart from the United States.[24] Both its technological prominence funneled by global market dominance has turned Israel into a global leader in the field and a precious evolving working example.

Part A introduces the Israeli National Cyber Bureau initiative and the Israeli government's underlying recommendations. Part B then maps the main cyber security themes in reflection of the Israeli initiative. It opens with cyber security definitions including the range of cyber threats, types of cyber security risks and types of practices not designated as cyber security risks. In addition, the brief reviews models of cooperation over cyber security, including inter-governmental, public-private platform (PPP) and regional cooperation. Lastly, the brief considers specific cyber

[20] The General Assembly Resolution was adopted without a vote as A/RES/53/70.

[21] A first successful GGE report was issued in 2010 (A/65/201). In 2011 the General Assembly unanimously approved a resolution (A/RES/66/24) calling for a follow-up to the last GGE. See, The UN Office for Disarmament Affairs (UNODA), Fact sheet, Developments in the Field of Information and Telecommunications in the Context of International Security, at: http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf.

[22] The Security & Defense Agenda (SDA) report, Cyber-Security: The Vexed Question of Global Rules (30 January 2012), at 66-67.

[23] *Id*., at 66. In fact, different to the experience of most countries with advanced cyber security policies, Israel's one did not evolve in response to civil threats i.e., cyber crime but instead it reacted mostly to national security considerations due to the country's notable geo-political security challenges. See, Interview with Mr. Tal Goldstein from the Israeli National Cyber Bureau, supra note 2, *Id*.

[24] See, Barbara Opall-Rome, DefenseNews, Israel Claims $3B in Cyber Exports; 2nd Only to US (Jun. 20, 2014), at: http://www.defensenews.com/article/20140620/DEFREG04/306200018/Israel-Claims-3B-Cyber-Exports-2nd-Only-US (last year Israel sales reached $3 billion which make approximately 5 percent of the global market).

security-related legal topics, including cyber security aspects in international law referring to cyber attacks and international humanitarian law, cyber treaties and international treaty law, national responsibility for cyber attacks and state responsibility, cyber crimes and cyber security, international human rights law, privacy law, cyber security and telecommunications law and cyber security and contractual obligations. Part C then offers a cross-section policy comparison between five leading national cyber security policies of the United States, United Kingdom, Canada, Japan and the Netherlands. The Conclusion part then lists primary recommendations with the prospect of facilitating academia-government cooperation in designing a cyber security policy model for countries worldwide.

A. Mission and Function

Israeli cyber security policy was established based on two major official milestones. The first of two has been the 2010 "National Cyber Initiative", aiming for Israel to become a top five global cyber superpower by 2015.[25] The second milestone, coming after years of acknowledged departmentalized activities in various branches, was the Government of Israel's Government Resolution No. 3611 as of August 7, 2011 adopting recommendations for the "National Cyber Initiative".[26] At the core of these two initiatives stood the establishment of the Israel National Cyber Bureau (INCB) in the Prime Minister's office, reporting directly to the Prime Minister.[27] The Bureau's mission henceforth has been to serve as an advisory body for the Israeli Prime Minister, the government and its committees over national policy in the cyber field and to promote its implementation.[28]

---

[25] *See* National Cyber Initiative - Special Report for the Prime Minister (The State of Israel, Ministry of Science and Technology, the National Council on Research and Development and the Supreme Council on Science and Technology, eds.) 2011 (Hebrew).

[26] In this backdrop the Israeli government has sought to establish a national cyber policy as soon as 2002. In the same year Israel drew a list of 19 major infrastructures incorporating power production, water supply or banking, held as either public and private with purpose of standardizing core, albeit effectively limited legal and technological protection thereof. *Id*., at 67. Until the establishment of the Israeli National Cyber Bureau in 2011, Israel based its rather fragmented policies on Special Resolution B/84 on '*The responsibility for protecting computerized systems in the State of Israel'* by the ministerial committee on national security of December 11, 2002, launched the national civilian cyberdefense policy. In balance, it has been the latter Special Resolution that catalyzed the establishment of the Israeli Cyber Bureau. See Lior Tabansky, supra note 1, at 2. Israel undertook numerous other steps to address cyber threats. In 2002 a government decision established the State Authority for Information Security (Shabak unit). The Authority is accountable for the specialized guidance of the bodies under its accountability in terms of essential computer infrastructure security against threats of terrorism and sabotage. To illustrate, when the instigation of the biometric database in Israel led to a enormous public dispute, a recent law was enacted in 2009 and consequently the State Authority for Information Security received a defensive role in prevention of cyber attacks on the biometric database.

[27] Government of Israel passed Government Resolution No. 3611, titled: Advancing National Cyberspace Capabilities, Resolution No. 3611 of the Government of August 7, 2011, at: http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf (for the non-official English version). See generally, also the State of Israel Prime Minister's Office - The National Cyber Bureau, at: http://www.pmo.gov.il/.

[28] Addendum A, section 1 (titled "*Bureau Mission*") states: "*The Bureau functions as an advising body for the Prime Minister, the government and its committees, which recommends national policy in*

The National Cyber Bureau's mandate is threefold. The first is to defend national infrastructures from cyber attack.[29] This aspect surely has not been restricted to traditional law enforcement reactive deterrence dialectics, as it considers also a preventive outlook.[30] The second mandate is advancing Israel as a world leading center of information technology based on the country's high technological advantage.[31] The third mandate is to encourage cooperation between academia, industry and the private sector, government offices and the security community, respectively.[32]

These broad policies were further detailed within the Israel's government Resolution No. 3611 threefold. The Resolution's first mentioned decision and its raison d'être is officially establishing a National Cyber Bureau in the Prime Minister's Office.[33] The resolutions further calls on regulating responsibility for dealing with the cyber field albeit broadly.[34] Addendum B to the Resolution offers a model description of responsibilities incorporating a Head Bureau position,[35] Steering committee,[36] and related administrative working procedures.[37] The third decision set by the Resolution has been to advance defensive cyber capabilities in Israel and advance research and development in cyberspace and supercomputing.[38] Numerous concrete policies are then further detailed by the Resolution. Albeit part of a rather broad and monolithic

---

the cyber field and promotes its implementation, in accordance with all law and Government Resolutions." *Id.*

[29] *Id*., Resolution No. 3611, at 1 ("*To improve the defense of national infrastructures which are essential for maintaining a stable and productive life in the State of Israel and to strengthen those infrastructures, as much as possible, against cyber attack*"), *Id*.

[30] On the immense challenges facing a traditional law enforcement reactive cyber security deterrence, see National Research Council, Proceedings of a Workshop on Deterring Cyberattacks (Washington, DC: National Academies Press, 2010); Martin C. Libicki, Cyberdeterrence and Cyberwar (Santa Monica, CA: RAND, 2009). *But see*, Derek E. Bambauer, Privacy Versus Security, Journal of Criminal Law and Criminology, Vol. 103(3) (2013) (cyber security policy must focus on mitigating breaches rather than preventing them)).

[31] Resolution No. 3611, supra note 27 ("*[a]dvancing Israel's status as a center for the development of information technologies*"), *Id.* Thus two years after the establishment of the Israeli National Cyber Bureau, the Prime Minister, the Mayor of the southern metropolitan of city Beer-Sheva and the President of Ben Gurion University announced the establishment of a national cyber complex in Beer-Sheva, to be named CyberSpark, where INCB's command center also presides. See, Ben-Gurion University of the Negev, Prime Minister Benjamin Netanyahu announces Creation of CyberSpark in Beer-Sheva (27 January 2014), at: http://in.bgu.ac.il/en/Pages/news/CyberSpark.aspx. Two giant international companies - Lockheed Martin and IBM have said to join Deutsche Telekom and EMC in setting up their research activities in the park. *Id.*

[32] *Id*. ("*[e]ncouraging cooperation among academia, industry and the private sector, government ministries and special bodies.*"), *Id.*

[33] *Id*. section 1, at 2.

[34] *Id*., section 2, at 2.

[35] Addendum B (titled: "*Regulating Responsibilities for Dealing with the Cyber Field*"), section A, *Id*.

[36] *Id*., section B.

[37] *Id*., sections C-H.

[38] *Id*., section 3 at 2. Two subsidiary decisions follow. The fourth is a budgetary decision has been made in section 4, *Id*., stating: "*The budget to implement this Resolution will be determined by the Prime Minister in consultation with the Minister of Finance, and will be submitted to the government for approval*"'. *Id*. The fifth decision upheld in section 5, at 2 excludes archetypical "*Special bodies*" from the mandate of the Bureau. Section D in the Definition part defines these as follows: "*Special Bodies" – the Israel Defense Forces, the Israeli Police, Israel Security Agency ("Shabak"), the Institute for Intelligence and Special Operations ("Mossad") and the defense establishment by means of the Head of Security of the Defense Establishment (DSDE).*" *Id*.

list of such nineteen policy recommendations, these could be categorized as educational recommendations, policy compliance-related recommendations and strategic ones.

To begin with, the Bureau's recommendations labeled educational proactively identify and mitigate specific cyber security intimidations. The Bureau is consequently said to devise "*national education plans*",[39] commonly aimed at "*increasing public awareness*" to cyber threats.[40] Similar to the North Atlantic Treaty Organization (NATO),[41] the United States Pentagon's cyber-command (USCYBERCOM),[42] Germany,[43] United Kingdom,[44] or Finland,[45] the Israeli Cyber Bureau is said to respectively coordinate national and international exercises[46] as well as cooperation with parallel bodies abroad.[47]

Secondly, the Resolution sets numerous recommendations over policy compliance. These recommendations essentially proffer a tailored edition of low-latency policy checkpoints. The Bureau henceforth is set to determine a yearly "*national threat of reference,*"[48] publish comparable ongoing "*warnings*"[49] and "*preventive practices*".[50]

A national cyber situation room was put in charge of the bureau's early warning apparatus. The facility constructs ongoing national assessment among various essential civil and security & defense organizations whilst constituting a firsthand national defensive layer for the entire country's administration. The national cyber situation room directly reports to INCB's central command. One telling occasion sets a case in point concerning the cyber situation room's contribution. During Operation *Pillar of Defense* launched by Israel on 14 November 2012 against the Hamas-governed Gaza Strip, a massive-scale overseas cyber attack was carried out against Israel. It had targeted distributed denial of services, the defacement of Israeli websites and the publication of citizens' data.[51] As INCB later announced during the attack and much owing to the newly initiated cyber situation room, no publication of leaked data on any notable or potentially highly damaging scale has occurred.[52]

The National Cyber Bureau is said to further advance coordination and cooperation between governmental bodies, the defense community, academia, industrial bodies, business and other bodies relevant to the cyber field.[53] Numerous ongoing projects set a series of cases in point. To date, INCB conveniently categorizes its projects

---

[39] *Id*., Recommendation 14.

[40] *Id*., Recommendation 12. Recommendation 14 similarly calls for the "*formulation of and the wise use of cyberspace*." *Id.*

[41] The Security & Defense Agenda (SDA) report, supra note 22, at 71.

[42] *Id*., at 83.

[43] *Id*., at 64.

[44] *Id*., at 80.

[45] *Id*., at 61.

[46] *Id*., Recommendation 9. In particular, Recommendations 10 and 11 offers to assemble intelligence picture from all intelligence bodies and similarly reiterate a "*national situation status*" concerning cyber security, respectively. *Id*.

[47] *Id*., Recommendation 15. Substantive international cooperation is still deemed questionable by INCB, as discussed in Part C.2, infra. See, Interview with Mr. Tal Goldstein from the Israeli National Cyber Bureau, supra note 2, *Id.*

[48] *Id*., Recommendation 5.

[49] *Id*., Recommendation 13.

[50] *Id*., Recommendation 13.

[51] *Id*.

[52] *Id*.

[53] *Id*., Recommendation 16.

leniently as threefold. These are the development of national cyber security infrastructure, the development of human capital and finally the development of cyber defense per the abovementioned national cyber security situation room. At a start, INCB has thus far initiated three national security-related projects: with Israel's Office of the Chief Scientist (OCS), the Israeli Ministry of Defense and surely also with Israeli academia. All pertain to a multi stakeholders apparatus albeit local and largely nationally preferential. The first of three is INCB's cooperation with Israel's Office of the Chief Scientist (OCS) in the Ministry of Economy. In a project called KIDMA (per the initials of the term "*the promotion of cyber security R&D*" in Hebrew) the Chief Scientist has adopted preferential policy for INCB's R&D projects henceforth. In compliance with INCB's commitment to the promotion of cyber security R&D, the KIDMA is officially aimed at promoting entrepreneurship within this field while preserving and increasing Israeli competitive edge in cyber security world markets.[54] In a program that started in 2013, the Chief Scientist endowed 80 Million New Israeli Shekels (Approximately $22 Million Dollars (U.S.)) for 2013-2014).[55] A second national cyber security infrastructure project initiated by INCB follows. In this case it has been a 2012-2013 two year collaboration with the local national security apparatus. Thus, together The Israeli Ministry of Defense's Research Authority, Development of Ammunition and Technological Infrastructure (MAFAT) the two institutions have allocated a sum of 10 Million New Israeli Shekels (Approximately $3.5 Million Dollars (U.S.)) in a project labeled MASAD (per the initials of the term "*Dual Cyber R&D*" in Hebrew).[56] This civil-security project thus approaches the cyber security challenge from this dual standpoint. It similarly has endowed 32 Million New Israeli Shekels (Approximately $10 Million Dollars (U.S.)) for the years 2012-2014 and is specifically aimed at fostering academic research in the field.

A third national cyber security infrastructure project has been with academia based on university cyber security research centers. In practice, INCB has to date partnered two Israeli universities in the establishment of two university research centers. These are the Ben-Gurion University of the Negev with research emphasis on technology and applicative sciences and the Tel-Aviv University with a broader interdisciplinary emphasis including political sciences or law.[57]

---

[54] Israel National Cyber Bureau publications, the Inauguration of the KIDMA - Promotion of R&D in Cyber Security program (13 November 2013), at: http://www.pmo.gov.il/MediaCenter/Spokesman/Pages/spokeKidma131112.aspx (in Hebrew). See, also, Israel's Office of the Chief Scientist (OCS), Newsletter 02-2012 (21 Nov. 2012), at: http://www.moital.gov.il/NR/rdonlyres/89646959-5455-4A5A-99FD-C4B07D07E8E5/0/syber122012_3.pdf (in Hebrew). The program includes upgraded funding for cyber security startups operating in technological incubators, a higher finance percentile in related venture capital funds, a fastened application examination process, etc. *Id.*

[55] *Id.*

[56] Israel National Cyber Bureau publications, Announcement concerning the establishment of the joint The Israeli Ministry of Defense's Research Authority, Development of Ammunition and Technological Infrastructure (MAFAT)-INCB MASAD project, at: http://www.pmo.gov.il/MediaCenter/Spokesman/Pages/spokemasad311012.aspx (in Hebrew).

[57] See, e.g., Major Cyber Security Center Launched at Tel Aviv University (16 September 2014), at: http://english.tau.ac.il/blavatnik_cyber_center. Two additional university research centers are presently being discussed. See, Interview with Mr. Tal Goldstein from the Israeli National Cyber Bureau, supra note 2, *Id*.

The underlying dual proposition upheld by INCB continuously has been that not only is academic research lagging behind the industry; but that this lag is in fact is cross disciplinary, including non-technological fields and particularly social sciences and law.[58] In continuation, lately, on May 2014 INCB's has published with the Israeli Ministry of Science a novel grant program which as part of its broad and interdisciplinary appeal approaches not only scientists and engineers but also political scientists or lawyers.

INCB has further developed a detailed program for promoting what it deems as the development of human capital. INCB initiated cyber security advanced studies programs in numerous leading technological high schools and post-graduate academic programs. One such notable endeavor focuses on high schools from the country's socio-economically fairly weaker periphery. In a project labeled "Magshimim Leumit" ("*Nationally Achieving*" in Hebrew)) in cooperation with the Israel's Ministry of Education this 2013-2016 three year program thus focuses on educating and developing professional skills amongst outstanding high school students ranging 16-18 years old. The program was founded under the assumption that cyber security is yet just another policy avenue for the promotion of qualitative human capital within archetypical broader distributive justice dialectics.[59]

The Bureau ultimately is said to regularly advise the Prime Minister, the government and its committees regarding cyberspace.[60] It is further said to consolidate its administrative aspects,[61] and advance legislation and regulation in the cyber field.[62] As of 2012 INCB declared that the first ongoing regulatory stage would incorporate four types of regulation and accompanying objectives. These are the promotion of cyber security for organizations, the industrial and civil sectors, market regulation and lastly cyber security regulation through standard setting.[63] On that account Israel's INCB has declared that it plans on leading the process of establishing recommendations for the government.[64] As of July 2012 such a process was initiated incorporating open consultation with multi stakeholder experts regularly. This process took until October 2012 while focusing on rather confined cyber law needs to date.[65]

---

[58] *Id*.

[59] The Israeli Prime Minister's Office, Announcement about the inauguration of the "Magshimim Leumit" project (21 Dec. 2012), at: http://www.pmo.gov.il/MediaCenter/Events/Pages/eventmagshimim311212.aspx (in Hebrew).

[60] *Id*., Recommendation 1. Notwithstanding the Bureau's overarching mandate, in matters of foreign affairs and security, the advice provided to the government, to its committees and to the ministers, will be provided on behalf of the Bureau by means of the Israeli National Security Council. *Id.* Recommendation 19 offers that the Bureau carry out any other role in the cyber field determined by the Prime Minister. *Id.*

[61] *Id*., Recommendation 2. The Bureau will also offer supporting cross agency coordination thereof. *Id*. Recommendation 4 further adds that the Bureau will "*inform all the relevant bodies, as needed, about the complementary cyberspace-related policy guidelines*". *Id*.

[62] *Id*., Recommendation 17. Recommendation 18 adds that the Bureau will serve as a regulating body regulating body in fields related to cyber security. *Id*.

[63] See, INCB's Public Consultation with multi stakeholders in preparing cyber security regulation (in Hebrew) (last visited 10 September 2014), at: http://www.pmo.gov.il/sitecollectiondocuments/pmo/cyber.doc.

[64] *Id.*

[65] *Id.* It included four stages. at a start, INCB collected and processed expert testimonies. Soon after a public advisory committee was established. Then a series of open consultations as well as particular consultations took place. Lastly, INCB generated a list of recommendation which were at first open for public commentary soon to pass as INCB final regulation recommendation for the Israeli government consideration.

Lastly and more pertinently are three archetypical strategic propositions focused on establishing a measurable regulatory legal-related framework. The first strategic proposition handily solicits recommendations to be made "*to the Prime Minister and government regarding national cyber policy*".[66] The Israeli government and the Israeli Prime Minister's office thus assert themselves as direct dialogue associates for a cyber security policy model initiative such as the one the Network of Centers (NoC) may entail. The second and third more thematic albeit overly-general strategic recommendations are to "*promote research and development in cyberspace and supercomputing,*"[67] and *devise a "national concept" for coping with "emergency situations in cyberspace*",[68] respectfully. These three policies also underlay this brief's legal positive framework.

B. The Positive Framework

This part maps the cyber security themes which constitute national cyber security policies worldwide. This part introduces and discusses these fields of law with the prospect of identifying the main legal concerns any national cyber security policy should entail in reference to the Israeli example. First to be discussed are cyber security definitions including the range of cyber threats, types of cyber security risks and types of practices not designated as cyber security risks. In addition, models of cooperation over cyber security are reviewed including inter-governmental, public-private platform (PPP) and regional cooperation. Lastly, the brief considers specific fields of law for examination, including cyber security and international law, cyber attacks and international humanitarian law, cyber treaties and international treaty law, national responsibility for cyber attacks and state responsibility, cyber crimes and cyber security, cyber attacks ad international human rights law, privacy and cyber security, cyber security and telecommunications law and cyber security and contractual obligations.

1. *Cyber security definitions*

A cyber security policy model should adhere to three categories of definitions as these are repeatedly present in leading national cyber policies.

See, also, interview with Mr. Amit Ashkenazi from the Israeli National Cyber Bureau (18 September 2014) (file with author) (adding that it is clear that adapted legislation is needed yet the intention is not to opt for an overarching statute but modular and proportional set of statutory frameworks for separate cyber threats), *Id.*

[66] Addendum A, section 2 (titled "*Bureau Goals*"), Recommendation 3 ("*[t]o guide the relevant bodies regarding the policies decided upon by the government and/or the Prime Minister; to implement the policy and follow-up on the implementation*."), *Id.*

[67] *Id.*, Recommendation 6. Such emblematic *'research and development'* should be promoted by what remain undefined "*professional bodies*", *Id.*

[68] *Id.*, Recommendation 8. There remains yet a fourth trade policy-related recommendation which albeit seminal in the Israeli Cyber Bureau's mandate, is nevertheless limited to advancement of the local economy. Recommendation 7 thus flatly calls upon the Bureau to "*work to encourage the cyber industry in Israel*," Recommendation 7. *Id.* This important yet only loosely irrelevant to cyber security policy, will remain outside the scope this policy brief.

a. *Defining the range of cyber threats*; ranging from deliberate attacks for military or political advantage through the forms of cyber crime and cyber warfare and cyber terror against civil and military objects.

b. *Defining types of cyber security risks*; ranging from concealment (Trojan horse), infectious malware and malware for profit (vector, control, maintenance and payload), Botnets, cybercrime business models (advertising, theft, support) and chokepoints (anti-malware, registrars, payments, site takedown and blacklisting).

c. *Defining types of practices not designated as cyber security risks;* including joke software, hoaxes, scams, spam and internet cookies)

2. *Models of cooperation over cyber security*

A cyber security policy model ought to map the possibilities and limitations regarding the creation of cooperative international arrangements, involving governments and civil society to reduce risks to cyber security. At the outset, INCB to date still witnesses only a limited degree of international cooperation. Two pivotal reasons clarify this actuality. Firstly, as a matter of a fact, few countries practice cyber security policies. A lesser number of countries actually have standing traditions of cyber industries funneled by policy making mechanisms and cyber security administrative organs. Secondly, it is further questionable to which extent international consensus could be achieved, in the backdrop of regional and even narrower bilateral alternatives.[69] Notwithstanding these regulatory constraints, numerous cooperative avenues offer preside across countries.

a. Inter-governmental cooperation

1) *The European Union* - The EU Cyber Security Strategy '*Protection of an open and free internet and opportunities in the digital world*' (February 2013) and associated draft directives: *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union* (February 2013) set the framework at the European Union for cyber security. The 2013 EU Cyber Security Strategy is gradually implemented by EU member states with the purpose of minimizing policy fragmentation among member states.

The EU's policy resonates the 2009 EU Commission's issuance of a communication on *Critical Information Infrastructure Protection (CIIP)*, entitled "*Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*".[70] In much

[69] See, Interview with Mr. Tal Goldstein from the Israeli National Cyber Bureau, supra note 2, *Id.*

[70] See EU Commission, Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience (2009), at: http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf.

resemblance to the Israeli case, the EU Commission has recently noted that the upcoming challenges for Europe are broadly fourfold. First the uneven and uncoordinated national approaches by EU member states. Second is the need for a new European governance model for critical information infrastructures. Third is the limited European early warning and incident response capability, and lastly is the prospective need for appropriate international cooperation. Collaboration with non-European national cyber security policies such as the Israeli one could be upheld. That is, given the European Commission's call to engage the global community to develop a set of principles reflecting European core values for the net's resilience.

Moreover, a cyber security policy model could reflect on the cooperative extent of the *European Programme for Critical Infrastructure Protection* set forth in a Directive EU COM(2006) 786. The program obliges all member states to the European Economic Area (EEA) to adopt the components of the Programme into their national statutes.[71] In the Israeli case, Israel and the EU are continually discussing EEA's integration based on a direct association agreement with Israel so that the prospect of a harmonized edition of a cyber security policy brief may be particularly timely.

Lastly, there remains the *European Union Agency for Network and Information Security (ENISA)* operating for the EU institutions and member states. ENISA serves as the EU's coordinative response to cyber security issues of the European Union and offers yet another platform for inter-governmental cooperation over cyber security in the EU.[72]

2) *The United States* - A cyber security policy model could further borrow from the case of the 2009 *Comprehensive National Cyber-security Initiative (CNCI)* put forward by the United States government funneled by the 2011 *International Strategy for Cyberspace (White House, May 2011).*[73] The details of this policy surely will be discussed in Part C.

Equally, most elements of the United States policy focus on federal government's cyber-security house in order instead of on the state level. In balance, however, in resemblance to the Israeli case, the United States has still not firmly decided what should be the regulatory authority of the federal government in protecting critical infrastructures owned and operated by the private sector. Be that as it may, the United States' designated priority policies include (1) economics, (2) protecting our networks, (3) law enforcement, (4) military, (5) internet governance, (6) international development, (7) internet freedom, as will be discussed in Part C, infra.

[71] European Programme for Critical Infrastructure Protection set forth in a Directive EU COM(2006) 786, at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.

[72] For ENISA's policy, see also, European Network and Information Security Agency (ENISA), National Cyber Security Strategies: Practical Guide on Development and Execution, (December 2012).

[73] The White House, President Barak Obama, The Comprehensive National Cybersecurity Initiative, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

b. *Regional cooperation*; a regional or inter-regional cyber security initiative incorporating future national examples could borrow from the constituting case of Asia-Pacific's regional cooperation over cyber security in National Computer Emergency Response Teams (CERT) by (APCERT). This initiative already facilitates regional cooperation and coordination amongst CERTs and Computer Security Incident Response Teams (CSIRTs).[74]

Another regional initiative which could shed light on regional or inter-regional cooperation is the comparable Organization of American States' (OAS) portal aimed at augmenting cyber-security and regional responses to cybercrime.[75] This rather early-stage portal was created primarily to facilitate and streamline cooperation and information exchange among government experts from OAS member states.

c. *Public-private platform (PPP)* - The business sector has taken on technological standardization initiatives since the early days of cyber security. Technological standardization has been advanced to increase the security of products, services and networks. One such important initiative came from the Internet Corporation for Assigned Names and Numbers (ICANN). Its successful effort to promote development and adoption of security extensions for the domain name system (DNSSEC) illustrates how a private-sector led initiative backed by government participation can significantly enhance the net's security.[76]

Another important example for governmental cooperation with commercial enterprises and educational institutions, albeit with a technical orientation are Computer Emergency Response Teams (CERTs). They are intended to promote information sharing and better coordination among government agencies and the private sector against cyber-attacks and identify and correct cyber-vulnerabilities.[77] The lessons from CERTs are still rather preliminary and necessitate further technical testing.

d. *Economics of information security considerations;* Evaluation of incentives for multiple stakeholders to align over cyber security should further incorporate adherence to efficiency considerations.[78] Thus cyber security policy may offer not only direct regulation, but also indirect regulation aimed at incentivizing efficient behavior by end-users. To name but a few suggestions these range from optimal security enhancing incentives such as tax subsidies for compatible standards to incentivizing whistle blowing against hazardous internet users or even against risky corporate espionage.

[74] Council for Security Cooperation in the Asia Pacific (CSCAP), Memorandum No. 20, Ensuring A Safer Cyber Security Environment (May 2012).

[75] See, Inter-American Cooperation Portal on Cyber-Crime, at, http://www.oas.org/juridico/english/cyber.htm.

[76] See, European Network and Information Security Agency (ENISA), Good Practices Guide for Deploying DNSSEC) at http://www.enisa.europa.eu/act/res/technologies/tech/gpgdnssec.

[77] See, the Forum of Incident Response and Security Teams, at: http://www.first.org. The European Government CERTs (EGC) Group (http://www.egc-group.org) has 11 member organizations.

[78] Tyler Moore, Introducing the Economics of Cybersecurity: Principles and Policy Options, National Research Council, Proceedings of a Workshop (2010).

e. *Administrative responses to cyber crises* offer additional possibilities regarding the creation of a cyber security policy model. Such are the Israeli Bureau call for defining *emergency cyber situations* in Recommendation 8 to the INCB's recommendations, or the Bureau's called for definition for *cyber warnings* in Recommendation 13 to the INCB's recommendations. This issue is surely discussed in Part C, infra.

f. *Linking international cyber security policy to domestic law.* Attention should be given to information asymmetries and principle-agent constraints when applying international cyber security regulation to national ones.[79] Such legal adaptations generally uphold the need to preserve separate national discretion, realistic and even lenient regulatory time tables, administrative safe harbors and even restrained judicial discretion while evaluating local differentiated security risks and challenges.

3. Cyber security and international law

a. *Cyber attacks and international humanitarian law* introduces discussion over most key definitions within international humanitarian law. These include a reassessment of the use of non-physical and non-military force, the definition of an cyber armed conflict alongside its intensity dialectics, the classification of cyber combatants and unlawful combatancy, cyber terror and its consistency with asymmetric war argumentation, collective security and self-defense in the midst of immediate and even anonymous cyber attacks, and even the definition of the all-out aggressive cyber war.[80] These issues already arise in a variety of forums and should be incorporated, at least in part, into a cyber security policy model. Recently, to illustrate, the North Atlantic Treaty Organization (NATO) issued an experts report, "*NATO 2020: Analysis and recommendations of the group of experts on a new strategic concept for NATO*" which included preliminary recommendations offering prospective changes in the *NATO Strategic Concept* to specify the characteristics of a cyber-attack that would trigger the obligation of collective response under Section 5 of the NATO treaty.[81] Equally importantly, the application of Article

[79] Daniel Jacob Hemel, Regulatory Consolidation and Cross-Border Coordination: Challenging the Conventional Wisdom, Yale Journal on Regulation, Vol. 28(1) (2011) (offering a regulatory paradox whereby in areas where a single regulatory agency enjoys consolidated control over a particular policy matter at the domestic level, that agency is less willing to restrict its policy-making discretion through an international agreement and vise-versa).

[80] Michael N. Schmitt, Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defence, and Armed Conflicts 151 In Proceedings of a Workshop on Deterring Cyber attacks: Informing Strategies and Developing Options for U.S. Policy (2010) [hereinafter, Proceedings of a Workshop on Deterring Cyber attacks]. See, also, Jon P. Jurich, Cyberwar and customary international law: the potential of a "bottom-up" approach to an international law of information operations, 9 Chi. J. Int'l L. 275-295 (2008).

[81] See, NATO 2020: Analysis and recommendations of the group of experts on a new strategic concept for NATO, at: http://www.nato.int/strategic-concept/expertsreport.pdf.

In addition in 2013 a second document concerning one aspect of cyber attacks was published, namely the *Tallinn Manual on the International Law Applicable to Cyber Warfare*. The manual was written for NATO, although it does not necessarily represent NATO's views. The manual aims at

51 of the UN Charter on individual or collective self-defense if an cyber armed attack occurred against a UN member remains unresolved.

b. *Cyber treaties and international treaty law*: Cyber security and the challenge of international agreement within international treaty law and the 1969 Vienna Conventions' *treaty* definition further necessitates consideration. That is, given that no single cyber security binding agreement within international treaty law thus far entered into force.[82]

c. *National responsibility for cyber attacks and State Responsibility*. Within public international law the State Responsibility doctrine governing when and how a state is held responsible for a breach of an international obligation offers additional challenges. Topics such as state responsibility attribution, online national sovereignty and effective governance of information commons are all central to countering cyber attacks while bestowing national responsibility thereof.[83] One should recall the breakthrough 2013 agreement by the United Nations to acknowledge the applicability of international law and state responsibility on state behavior in cyberspace.[84]

d. *Cyber crimes and cyber security* should be conveniently addressed within the scope of the 2001 Convention on Cybercrime (the "Budapest Convention") initially adopted by the Council of Europe (COE).[85] The treaty addresses three issues which relate to cyber security. The first is cybercrime that nations should attend to in their criminal codes. The second is the authorities governments should take on with the purpose of access communications or stored records for evidentiary needs. The third issue which is to be addressed in a cyber security policy model is transnational cooperation mechanisms within the context of the Convention on Cybercrime.[86] Part C comparatively addresses cyber crime policies.

e. *Cyber attacks and international human rights law* uphold a paucity of literature from the lens of human rights over national and international cyber security.[87] The legal framework herein should remain distinct from national constitutional legal analyses given that international human rights law surely

---

defining cyber warfare under the international law and set rules to govern such conflicts including rules about the responsibility of the state or international humanitarian law.

[82] Abraham Sofaer et al, Cyber security and international agreements 179 In Proceedings of a Workshop on Deterring Cyber attacks *Id*.

[83] L. Janczewski & Colarik, A. M., Cyber Warfare and Cyber Terrorism, Cambridge: CUP (2008).

[84] *See*, UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, June 24, 2013.

[85] The Council of Europe (COE), Convention on Cybercrime, 2001. See http://www.conventions.coe.int/cybercrime (the "*Budapest Convention*").

[86] At the pentennial United Nations Crime Congress held in April 2010 in Salvador, Brazil, negotiations of a global cybercrime treaty failed. Disagreements emerged over national sovereignty issues and concerns for human rights mostly. On the history of cyber crime harmonization, see The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva (December 2008), at: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf.

[87] J. B. Wolf, War Games Meets the Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money, American Criminal Law Review, 28 (2000).

constitutes a separate public international legal analysis. Policies concerning civil liberties are detailed in Part C.

4. Privacy and cyber security

Legal scholarship often tends to conflate privacy and security.[88] Remarkably, most academics and advocates treat the two concerns as interchangeable or as inextricably intertwined. However, security and privacy can and should be treated as distinct concerns at least in part. Privacy discourse involves difficult normative decisions about competing claims to legitimate access to, use of, and alteration of information. Security implements those choices as it mediates between information and privacy selections.[89] Cyber security may thus require ongoing preventive massive surveillance and a wide-ranging collaboration with online intermediaries. That is, instead of limited wiretapping as part of an otherwise a reactive approach to law enforcement.

As in the Israeli case, other countries have adopted data protection laws that follow the European Union model,[90] the Organization for Economic Co-operation and Development (OECD) model,[91] or the Asia-Pacific Economic Cooperation (APEC) model.[92] Under these laws, the data controller, typically the entity that has the primary relationship with an individual, remains responsible for the collection and processing of personal data, even when third parties process the data. The data controller is required to ensure that any third party processing personal data on his or her behalf takes adequate technical and organizational security measures to safeguard the data.

---

[88] See, e.g., Derek E. Bambauer, Privacy Versus Security, Journal of Criminal Law and Criminology, Vol. 103(3) (2013). Bambauer illustrates this meta argument beginning with the seminal work of Jon Mills. See, Jon Mills, Privacy: The Lost Rights 301–02 (2008).

[89] *Id*.

[90] The European Parliament recently presented the European Parliament legislative resolution of 4 July 2013 on the proposal for a directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA. In this proposal the European Parliament offers solutions to cyber attacks on information systems. It has done so without clear adherence to the conceptual relations between privacy and cyber security concepts.

[91] See, OECD, Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy and Non-governmental Perspectives on a new Generation of National Cybersecurity Strategies: Contribution from BIAC, CSISAC and ITAC, OECD Report (2012). See, also generally, OECD Guidelines for the Security of Information Systems and Networks -- Towards a Culture of Security – 2002. http://www.oecd.org/dataoecd/16/22/15582260.pdf.

[92] The Asia Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group (APEC-TEL) gathers the governments, business and private sectors of the 21 APEC member states. At the Fifth meeting of Ministers for the Telecommunications and Information Industries (TELMIN 5) in Shanghai, China, on May 29-30, 2002, the Ministers adopted a *Statement of the Security of Information and Communications Infrastructure* that called for domestic implementation of the ten measures included in the United Nations General Assembly Resolution 55/63, titled *Combating the Criminal Misuse of Information Technologies*, of 4 Dec. 2000.

The TELMIN 5 further called on APEC-TEL to give particular precedence to, and facilitate within, and work on the protection of information and communication infrastructures. Lastly, APEC-TEL hold projects in progress aimed at raising awareness regarding cyber security and cybercrime. That is, including the development of an APEC Cybersecurity Strategy. See, also, APEC, Recommendation by the APEC Telecommunications and Information Working Group (TEL) to APEC Senior Officials (SOM) for an APEC Cybersecurity Strategy, 2001.

The latest revelations regarding the National Security Agency (NSA) surveillance program designed to counter cyber-terror threats initiated a public debate regarding the limits of governmental powers also in the United States.[93] These led to several congressional and parliamentary hearings and will soon possibly encounter judicial review. Moreover, pressure by the intelligence community led to the proposal of an archetypical cyber security reactive US legislation, named as the *Cyber Intelligence Sharing and Protection Act (CISPA).* This proposed law challenges the proper balance between security and civil liberties, whilst allowing sharing of Internet traffic information between the government and private companies.[94]

5. *Cyber security and telecommunications law;* The hostile use of telecommunications with the declared or hidden intent of undermining the sovereignty of a foreign state is a violation of the principles and purposes enshrined in the Charter of the United Nations concerning guaranteeing peace and security for all member states. These seminal considerations should be further incorporated into a cyber security policy model.

   These are also a violation of the fundamental principles of the International Telecommunication Union (ITU), expressed in the preamble to its Constitution with the object of facilitating peaceful relations, international cooperation among peoples and economic and social development by means of efficient telecommunication services. Equally, a novel cyber security policy model initiative should consider Provisions CS 197 and CS 198 of the Constitution of the International Telecommunication Union stating that all stations must be effectively established and operated in such a manner as not to cause harmful interference to the radio services or communications of other member States.

   Moreover, a cyber security model should mull over the Agreement at the ninth plenary meeting of the World Radiocommunication Conference (WRC) held in November 2007, stating the seminal paragraph 6.1 (g) "*that a broadcasting station operating on board an aircraft and transmitting solely to the territory of another administration without its agreement cannot be considered in conformity with the Radio Regulations*". In addition, it should consider ITU Radio Regulation 8.3

[93] Since the aftermath of 9/11 terrorist attacks, it is assumed that Section 215 of the USA PATRIOT Act of 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) allows the FBI to apply the Secret Foreign Intelligence Surveillance Act (FISA) court for an order to gather information "*for an authorized investigation...to protect against international terrorism or clandestine intelligence activities*." Later on, it has been equally believed that the NSA's PRISM project designed to address terrorist threats was based on the same section to the PATRIOT act. See, Niraj Chokshi, NSA Spying Appears to Stem From 550-Word Section of PATRIOT Act, The National Journal (June 7, 2013).

[94] See, e.g., Carol. M. Hayes and Kesan, J. P., At War Over CISPA: Towards a Reasonable Balance between Privacy and Security. Illinois Public Law Research Paper No. 13-03 & Illinois Program in Law, Behavior and Social Science Paper No. LBSS13-04 (2012), available at: http://ssrn.com/abstract=2135618 (arguing that the proposed legislation can be useful to achieve the proper balance between security and privacy if it is to be amended appropriately).

An additional law which should constitutes cyber security-related surveillance considerations is the 1994 the Communications Assistance for Law Enforcement Act (CALEA). This act on the whole guarantees that intelligence agencies can monitor all telephone, broadband internet, and VoIP traffic in real-time through back-doors created for them by telecommunications carriers and manufacturers of telecommunications.

establishing that internationally recognized frequency assignments recorded must be taken into account by other administrations when making their own assignments, in order to avoid harmful interference. Lastly, such cyber security policy model should consider ITU Radio Regulation 42.4 prohibiting the operation of a broadcasting service by an aircraft station at sea and over the sea.

6. *Cyber security and contractual obligations* - Even when a particular hazardous activity is not banned in regulation, private entities may have a contractual obligation to secure the personal information of their clients, contactors or employees. So much so, in order to ensure that the data is not misused by second and third parties. Terms and Conditions and Privacy Statements typically opt for such contractual obligations in private websites. Companies may otherwise enter into contracts such as service agreements with its customers, in which it has made specific commitments to protect personal data or company data, or otherwise limit their use or encrypt it to ensure their security. Such obligations make integral part of any cyber security apparatus and may thus require meticulous consideration.

C. A Cross-Section Comparison

Over thirty countries declared to date an archetypical national cyber security strategy.[95] In much resemblance, countries have conducted active debate on codes of conduct for cyberspace, application of international laws, internet governance and other aspects of functions, roles and circumstances of cyberspace. National policies thus deal with the risks surrounding cyberspace from such viewpoints as national security and economic growth. Such national state practice has ultimately turned the functions, roles and circumstances of cyberspace into a common international issue. Designing a cyber security policy model should therefore be especially attuned to leading national cyber security policies. This part offers a cross-section comparison between five such countries, namely the United States, United Kingdom, Canada, Japan and the Netherlands.

[95] See, e.g., European Union Agency for Network and Information Security (ENISA), National Cyber Security Strategies in the World, at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (last retrieved 14 July 2014).

TOWARDS A CYBER SECURITY POLICY MODEL

Country	Promote cyber security R&D	Promote cyber security education	Ensure ongoing risk assessment	Promote counter cyber crime policy	Promote cyber security in international law	Form of regulation (legislation, courts, markets, norms, etc) & institutional aspects	Balancing cyber security with civil liberties	Type of cooperation			
								Intra-governmental cooperation	Regional cooperation	Public-Private platform (PPP)	Inter-governmental cooperation
United States[i]	1) [p]romote collaborative science and technology research to enhance cybersecurity tools and capabilities.[ii] 2) It is also essential to cultivating dynamic, international research communities able to take on next-generation challenges to cybersecurity.[iii]	1) Provide the necessary knowledge, training, and other resources to countries seeking to build technical and cybersecurity capacity. For over a decade the United States has supported a variety of programs to help other nations gain the resources and skills to build core capacities in technology and cybersecurity[iv] 2) In recent years, we have helped make this work a priority at multilateral fora such as the OAS, APEC, and the U.N. The United States will expand these collaborations, work in-country to support private-sector investment in capacity, draw attention to this critical need.[v] 3) Continually develop and regularly share international cybersecurity best practices.[vi] 4) Enhance	1) Ensure robust incident management, resiliency, and recovery capabilities for information infrastructure[vii] 2) The United States Government actively participates in watch, warning, and incident response through exchanging information with trusted networks of international partners.[viii] 3) The United States will also work to engage international participation in cybersecurity exercises, to elevate and strengthen established operating procedures with our partners.[ix]	1) Participate fully in international cybercrime policy developed bilaterally and multilaterally like the Budapest Convention. 2) The United States will continue to encourage other countries to become parties to the Convention and will help current non-parties use the Convention as a basis for their own laws.[x] 3) Protect intellectual property, including commercial trade secrets, from theft and industrial espionage.[xi] The persistent theft of intellectual property, whether by criminals, foreign firms, or state actors working on their behalf, can erode competitive-ness in the global economy, and businesses' opportunities to innovate.[xii]		1) Sustaining a free-trade environment while promoting international standards and innovative open markets to ensure that cyberspace continues to serve the needs of our economies.[xiii] 2) Developing international, voluntary, consensus-based cybersecurity standards and deploying products, processes, and services based upon such standards.[xiv]	1) Preserve, enhance, and increase access to an open, global Internet is a clear policy priority.[xv] 2) Support civil society actors in achieving reliable, secure, and safe platforms for freedoms of expression and association.[xvi] The same protections must apply to Internet Service Providers and other providers of connectivity, who too often fall victim to legal regimes of intermediary liability that pass the role of censoring legitimate speech down to companies.[xvii] 3) Encourage international cooperation for effective commercial data privacy protections. . . .The United States has a robust record of enforcement of its privacy laws, as well as encouraging multi-stakeholder policy development.[xviii]	1) Agencies across the United States Governme nt are collaborati ng, together with the private sector, to protect innovation from industrial espionage, to protect Federal, state, and local gov't networks, to protect military operations from degraded operating environme nts, and to secure critical infrastruc-ture against intrusions and attacks[xix] 2) Build and enhance existing military alliances to confront potential threats in cyberspace[xx] 3)Given the Internet's importance to the world's economy, it is essential that this network of networks and its underlying	Support the expansion of cyber security to geographic regions currently underrepresented in the dialogue—most notably Africa and the Middle East—to further our interest in building worldwide capacity.[xxi]	The public and private sectors must work together to develop, maintain, and implement standards and support the development of international standards and conformity assessment schemes that prevent barriers to international trade and commerce[xxii]	Insert cyberspace issues on the agenda at the Organization of American States (OAS), the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF), the Asia-Pacific Economic Cooperation Organization (APEC), the Organization for Cooperation and Security in Europe (OSCE), the African Union (AU), the Organization for Economic Cooperation and Development (OECD), the Group of Eight (G-8), the European Union (EU), the United Nations (U.N.), and the Council of Europe.[xxiii]

Country	Promote cyber security R&D	Promote cyber security education	Ensure ongoing risk assessment	Promote counter cyber crime policy	Promote cyber security in international law	Form of regulation (legislation, courts, markets, norms, etc) & institutional aspects	Balancing cyber security with civil liberties	Type of cooperation			
								Intra-governmental cooperation	Regional cooperation	Public-Private platform (PPP)	Inter-governmental cooperation
United States - Cont'		states' ability to fight cybercrime—including training for law enforcement, forensic specialists, jurists, and legislators.[xxiv]						infrastructure, the DNS, remain stable and secure.[xxv]			
United Kingdom (2009)[xxvi]	Enable the UK cyber security industry to thrive and expand, supporting it in accessing overseas markets.[xxvii]	1) Raise awareness amongst businesses of the threat and actions that they can take to protect themselves including working through strategically important sectors to raise cyber security issues throughout their supply chains.[xxviii] 2) By March 2012, conduct research on how to improve educational involvement with cyber security significantly at all levels – including higher education and postgraduate level.[xxix]	1) [t]here can be no such thing as absolute security. We will therefore apply a risk-based approach to prioritizing response.[xxx] 2) Improve our ability to anticipate the technological, procedural and societal behavior developments that affect our use of cyberspace.[xxxi] 3) Establish a scheme for certifying the competence of information assurance and cyber security professionals by March 2012, and a scheme for certifying specialist training in 2012.[xxxii]	1) Promote greater levels of int'l cooperation and shared understanding on cyber crime as part of the process begun by the London Conference on Cyberspace, in addition to promoting the Council of Europe's Convention on Cyber crime (the Budapest Convention) and building on the new EU Directive on attacks on information systems. Contribute to the review of security provisions of the EU Data Protection Directive and the proposed EU Strategy on Information Security[xxxiii] 2) Encourage the courts in the UK to use existing powers to impose appropriate online sanctions for	The UK will continue to pursue the international development of norms of acceptable behavior in cyberspace. according to principles proposed by the Foreign Secretary in February 2011 and reiterated at the London Conference on Cyberspace (November 2011):[xxxiv] 1) Govn's should act proportionately in cyberspace and in accordance with national and int'l.[xxxv] 2) maintain ability in terms of skills, technology, confidence and opportunity – to access cyberspace[xxxvi] 3) [t]olerance and respect for diversity of language, culture and ideas[xxxvii]	1) Create a new national cyber crime capability as part of the new National Crime Agency by 2013[xxxviii] 2) Working with domestic, European, global and commercial standards organizations to stimulate the development of industry-led standards [xxxix] 3) Support GetSafeOnline.org to become the single authoritative point of advice on responding to cyber threats (for example, the recent publication of an internet safety guide) [xl] 4) Manage crucial skills and helping to develop a community of 'ethical hackers' in the UK to ensure that our networks are robustly protected. [xli]	1) Support the open internet, working with the Broadband Stakeholder Group to develop industry-wide principles on traffic management and non-discrimination and reviewing its transparency code of practice in early 2012 [xlii] 2) Through the CONTEST strategy, increase our disruption of online radicalization and recruitment, and safeguarding against cyber attack.[xliii] 3) Use multilateral and bilateral channels to discuss how to apply the framework of international human rights law in cyberspace and new challenges in guaranteeing	1) Create and build a dedicated and integrated civilian and military capability within the MoD. Mainstreaming cyber within the organization and setting up a Defense Cyber Operations Group (DCOG). An interim DCOG will be in place by April 2012 and will achieve full operational capability by April 2014.[xliv] 2) Support Olympic cyber security by joining up the relevant departments and conducting exercises to ensure preparations for cyber incidents are robust.[xlv]	1) Work with allies to ensure implementation of NATO's cyber defense policy (agreed in June 2011)[xlvi] 2) Work closely with the European Commission and the External Action Service to encourage greater coherence within the EU on cyber issues.[xlvii] 3) Encourage international and regional organizations to support capacity building... Work with the Commonwealth (model legislation on cyber crime), the ITU (support training on technical standards), the Council of Europe and with the Organization for Security and Co-operation in Europe	1) require everybody, the private sector, individuals and government to work together[xlviii] 2) The expertise and innovation required to keep pace with the threat will be business-driven.[xlix] 3) Work with the companies that own and manage our Critical National Infrastructure (CNI) to ensure key data and systems continue to be safe and resilient.[l] 4) Seek agreement with ISPs on the support they might offer to internet users to help them identify, address, and protect	1) Threats are cross-border. ..We will seek partnership with other countries that share our views.[li] 2) Implement bilateral commitments set out in high-level communiqués (agreed in 2010 15 and 2011) with the US, Australia and France.[lii] 3) Develop new bilateral relationships on cyber with those emerging powers that are active in cyberspace[liii]

Country	Promote cyber security R&D	Promote cyber security education	Ensure ongoing risk assessment	Promote counter cyber crime policy	Promote cyber security in international law	Form of regulation (legislation, courts, markets, norms, etc) & institutional aspects	Balancing cyber security with civil liberties	Type of cooperation			
								Intra-governmental cooperation	Regional cooperation	Public-Private platform (PPP)	Inter-governmental cooperation
United Kingdom - Cont'				online offences[liv] 3) Encourage the use of 'cyber-specials' to bring in those with specialist skills to help the police[lv] 4) Significantly increase the law enforcement agency capability on cyber crime[lvi]	4) [o]penness to innovation and the free flow of ideas, information and expression[lvii] 5) [r]espect individual rights of privacy and intellectual property[lviii] 6) [c]ompetitive environment which ensures a fair return of investment[lix]		such rights.[lx] 4) Actively engage in the UN Group of Gov't Experts, which will reconvene in 2012, to ensure that a constructive report is made to the Secretary-General in 2014 in line with UN General Assembly Resolution 65/141 (driver of open societies, whilst promoting stability and reliability).[lxi]		(OSCE) to promote freedom of expression online.[lxii]	themselves from with malicious activity on their systems.[lxiii]	
Canada [lxiv]	---	The Government's ultimate goal is to create a culture of cyber safety whereby Canadians are aware of both the threats and the measures they can take to ensure the safe use of cyberspace.[lxv]	1) Within Public Safety Canada, the Canadian Cyber Incident Response Centre will continue to be the focal point for monitoring and providing advice on mitigating cyber threats.[lxvi] 2) The Canadian Cyber Incident Response Centre will direct the national response to any cyber security incident.[lxvii] 3) Public Safety Canada will	1) The Government will strengthen the ability of law enforcement agencies to combat cybercrime.[lxviii] 2) The Royal Canadian Mounted Police will investigate, as per the Royal Canadian Mounted Police Act , suspected domestic and international criminal acts against Canadian networks and critical information infrastructure[lxix] 3) The	---	Allows continual improvements to be made to meet emerging threats.[lxx]	Reflects Canadian values such as the rule of law, accountability and privacy.[lxxi]	1) Partnering to secure vital cyber systems outside the federal Governme nt.[lxxii]	Canada will also build on its existing engagement in cyber security discussions at key international fora, such as the United Nations, NATO and the Group of Eight.[lxxiii]	Emphasizes partnerships with Canadians, provinces, territories, Business, NGOs and academia.[lxxiv]	1) Builds upon our close working relationships with our allies with special emphasis on Canada's closest security and intelligence partners, the United States, the United Kingdom and Australia.[lxxv] 2) To the extent possible, Canada will support efforts to build the cyber security capacity of less developed states and foreign partners.[lxxvi]

Country	Promote cyber security R&D	Promote cyber security education	Ensure ongoing risk assessment	Promote counter cyber crime policy	Promote cyber security in international law	Form of regulation (legislation, courts, markets, norms, etc) & institutional aspects	Balancing cyber security with civil liberties	Type of cooperation			
								Intra-governmental cooperation	Regional cooperation	Public-Private platform (PPP)	Inter-governmental cooperation
Canada - Cont'			also lead public awareness and outreach activities.[lxxvii]	Department of National Defense and the Canadian Forces will strengthen their capacity to defend their own networks, will work with other Government departments.[lxxviii]							
Japan[lxxix]	[r]esearch and development and practical testing of technologies aimed at improving the cyber attack detection and advanced analysis functions at research institutions and relevant organizations shall be accelerated.[lxxx]	1) [i]t is important that in addition to the understanding that small and medium-sized enterprises " *are responsible for protecting themselves*" general users must also make efforts to implement measures based on an awareness of "*not bothering others*."[lxxxi] 2) [i]t is necessary to plan awareness raising activities starting from the elementary and middle school education stages, and implement participatory awareness raising projects such as motto and poster contests.[lxxxii]	1) The Japanese Government Security Operation Coordination team (GSOC) was formed in order to strengthen government institutions capability to deal with emergencies related to information security issues such as external cyber attacks and put into operation in April of 2008.[lxxxiii] 2) The collaboration among the GSOC, the CYMAT84 and the CSIRT of each government institution at the time of incident occurrence shall be strengthened in order for immediate sharing of incident information and a full	1) System preparation will be carried out through expansion of organizations such as the Cyber Attack Analysis Center, the Cyber Attack Special Investigations Unit and the Unauthorized Program Analysis Center, information collection and analysis equipment will be enhanced and strengthened and preparation of equipment including the advancement of internet monitoring systems.[lxxxiv] 2) The Japanese National Cyber-Forensics and Training Alliance (NCFTA) will take measures for sharing	For the application of international laws to acts using cyberspace, it is important that existing international laws continue to be applied to acts using cyberspace in terms of maintaining a degree of order in cyberspace, and the deliberation will continue on how to apply specific international laws such as the Charter of the United Nations and the International Humanitarian Law to conducts in cyberspace.[lxxxv]	1) Diverse entities such as the government, public, academic, industrial and private sectors in Japan . . . it becomes necessary for each entity to carry out their own information security measures in an independent and proactive fashion as part of their social responsibilities[lxxxvi] 2) [i]t is important that the whole of society participated in the "cyberspace hygiene" as a preventative information security measure against unauthorized intrusions, malware infections, vulnerabilities as factors for these incidents and other risks.[lxxxvii] 3) Japan has worked	1) [i]t is important to multilaterally build and strengthen partnerships with other nations and regions which share the same basic values including the basic policy, democracy, respect for basic human rights, and the rule of law. For this reason, it is necessary to carry out diplomacy which promotes a balanced approach to constructing a safe and reliable cyberspace[lxxxviii] 2) [c]yberspace has provided us a variety of positive benefits including innovation, economic growth and solutions for social issues while still ensuring freedom of	1) [a]dvance threat analysis capabilities by promoting information sharing and strengthen cooperation between Computer Security Incident Response Team (CSIRT).[lxxxix] 2) govn't must work to strengthen the functions of the NISC (the "Cybersecu-rity Center" (tentative)) as a command post, promote collaboration among relevant actors including between ministries[xc] 3) "Regarding Notation of Information Security Requireme	[t]he country will actively participate in multi country discussions and meetings including regional frameworks such as the ASEAN Regional Forum (ARF) Asia-Pacific forum and other related committees in the United Nations.[xci]	1) the multi-stakeholders in cyberspace need to fulfill each responsibilities corresponding to their respective roles in the society while mutually cooperating and assisting with each other including international cooperation and cooperation between the public and private sectors[xcii] 2) [i]t is expected that private companies, educational institutions and research institutions will work together in industry-government-academia collaboration[xciii]	cooperation with the United States, in which Japan is in an alliance based on the Japan-U.S. Security Arrangements, is vital.[xciv]

Country	Promote cyber security R&D	Promote cyber security education	Ensure ongoing risk assessment	Promote counter cyber crime policy	Promote cyber security in international law	Form of regulation (legislation, courts, markets, norms, etc) & institutional aspects	Balancing cyber security with civil liberties	Type of cooperation			
								Intra-governmental cooperation	Regional cooperation	Public-Private platform (PPP)	Inter-governmental cooperation
Japan - Cont'			readiness system by the government together. In addition, in anticipation of large-scale cyber attacks85 and these possibilities countermeas ures for the occurrence of incidents.[xcv] 3) The Japanese government established the Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR) system for sharing and analyzing information in the 10 critical infrastructure fields in Japan.[xcvi]	information through cooperation with the private sector, including the "Council to Prevent Unauthorized Communicat-ions as a Cyber Intelligence Measure.[xcvii] 3) Japan has ratified the Convention on Cybercrime and will work to strengthen rapid and effective mutual investigation s and other cooperation between law enforcement agencies.[xcviii]		towards constructing a safe and reliable cyberspace in which free flow of information is ensured by ensuring openness and interoperability of cyberspace without excessively administering or regulating it.[xcix] 4) The government must strengthen the basic functions of the nation related to cyberspace.[c] 5) [i]t is important for cyberspace-related operators to create a market through development of advanced technologies and products, cultivation of human resources with high abilities and the use and application of these resources for information security measures in order to strengthen the international competitiveness of Japan's "cybersecurity industry".[ci]	expression and protection of privacy.[cii]	-nts in Procureme nt" was released to the various ministries, etc. on January 24, 2012 based on the results of the studies of the "Subcomm ittee for Strengtheni ng Public-Private Collaborati on" established in the Informatio n Security Measure Promotion Council (CISO Council) which is in turn established in the Informatio n Security Policy Meetings.[ciii]			
The Netherlands[civ]	1) Promote research and education in cyber security[cv] 2) Encouraging	1) Promote research and education in cyber security[cvi] 2) Taskforce on cyber	1) Ensure appropriate and up-to-date threat and risk assessments[cvii]	1) Int'l approach to cyber crime: updating and strengthening legislation (including the Criminal	1) develop a hub for expertise on international law and cyber security	1) Strengthening the National Cyber Security Centre[cviii] 2) NCSC develops into Security	1) The Netherlands builds coalitions for freedom, security and peace in the digital	1) Division of responsibilities between ministries[cix] 2) Risk analyses,	The Dutch NCSS2 is in line with the fundamental principles of the EU Cyber Security	1) Public-private partnership s[cx] 2) Military and civil, public	1) Active international cooperation[cxi] Note - The International Security Strategy is aimed at

Country	Promote cyber security R&D	Promote cyber security education	Ensure ongoing risk assessment	Promote counter cyber crime policy	Promote cyber security in international law	Form of regulation (legislation, courts, markets, norms, etc) & institutional aspects	Balancing cyber security with civil liberties	Type of cooperation			
								Intra-governmental cooperation	Regional cooperation	Public-Private platform (PPP)	Inter-governmental cooperation
The Netherlands - Cont'	innovation in cyber security[cxii] 3) Feasibility study on separate vital network[cxiii]	security education[cxiv] 3) Individual responsibility[cxv]	2) The information security awareness strategy for government administrators and managers. With the Taskforce on Management, Information Security and Services, the government pursues an active awareness policy to get the government's information security at the desired level.[cxvi]	Code).[cxvii] 2) Program-based approach to cybercrime (PAC)[cxviii] ; 3) Intensify the investigation of cybercrime and prosecution of its perpetrators[cxix] 4) Create a pool of registered experts from the public and private sectors and knowledge institutions[cxx]	('Cyber diplomacy').[cxxi] 2) More active approach to cyber espionage[cxxii]	Operations Centre (SOC) in addition to its role as a Computer Emergency Response Team (CERT)[cxxiii] 3) Supported standards, 'security by design' and 'privacy by design'.[cxxiv] 4) Self-regulation if possible, legislation if necessary[cxxv]	domain.[cxxvi] 2) Measures must be proportionate[cxxvii]	security requirements and information sharing within critical infrastructure sectors[cxxviii] 2) Enhancing civil-military cooperation	Strategy.[cxxix]	and private, national and international actors have become more intertwined[cxxx]	actions taken by the Netherlands abroad and in cooperation with other countries to secure its interests.[cxxxi]

Conclusion (and Best Practices)

Israel's inauguration of the INCB cyber command and its upward national cyber policy has apparently five facets. These are: 1) the implementation of a medium-run five-year plan to scale up the country as a world industry leader in cyber security, 2) the inclusion of investment in R&D based on interdisciplinary university research centers and backed by extensive governmental funding, 3) encouraging industry to develop new technologies, 4) the setting up of a super computer center and 5) boosting academic studies in cybernetics.

The effectiveness of Israel's cyber policy is nevertheless still unfolding as all caveats apply. At a start, cyber security is still an evolving cross discipline whereas future cyber risks and threats are remarkably untried. Any cyber security policy model should thus reflect this platitude and adhere to much regulatory modularity funneled by administrative flexibility. Furthermore, national cyber security policies often carry a reactive nature as they regularly emerge merely after equivalent cyber threats evolve. Israel's experience is no different. As a result, taken from the organizational angle cyber security policies in due course hardly replace running administrative organs as they wind up conscientiously coordinating them. Israel's INCB serves yet again as a proof positive. INCB' rather modest thirty employee core in fact hardly battles or even has the means to battle cyber threats directly. That is as INCB coordinate cyber battles of myriad local defense and civil agencies and corporations

solely. A third caveat calling for certain restraint towards the Israeli example applies. Accordingly, different than with most cyber-literate countries worldwide, Israel's INCB materialized in reaction to momentous national security threats unfamiliar or at least moderately undemanding to most of its counterparts. Fairly judicious cyber crimes alongside other civil liberties infringing forms of cyber attacks against most other countries thus make partly related regulatory modules in comparison to the Israeli one at least to date.

That said, in opting for a cyber security policy model for countries at large, the policy brief reviews the main legal themes to be considered and does so in particular reference to the national cyber security policies of the United States, United Kingdom, Canada, Japan, the Netherlands and of course Israel. The state practice by these countries and declared policies may suggest the following list of conclusive best practices.

Promoting cyber security R&D; following the experience of the United States, Israel or the United kingdom, national commitment to research and development in cyber security is essential for two main reasons. Firstly, is cultivates dynamic international research communities able to take on next-generation challenges to cyber security. Secondly, it enables national cyber security industries to expand while supporting it in accessing overseas markets. Clearly, such practice should be adapted to the scientific educational frameworks and underlying national preferences.

Promote cyber security education; there seem to be three types of educational policies within the cyber security context. At a start, educational programs help nations gain the resources and skills to build core capacities in technology and cyber security. The promotion of cyber security education is meant to raise awareness amongst businesses of the threat and protective actions they may take. In recent years, the United States most noticeably helped make education over cyber security a priority at multilateral fora such as the OAS, APEC, and the UN. Cyber security-related education and training offers another purpose within the related context of cyber crime. In this context cyber security educational and training programs are aimed at law enforcement officials, forensic specialists, jurists, and legislators. The third educational policy is to improve educational involvement at the higher education and postgraduate level aimed at constructing a vibrant research community and related cyber security industries.

Ensuring ongoing risk assessment; All national cyber security policies reviewed have developed a detailed watch, warning, and incident response to cyber threats through exchanging information with trusted networks. Similarly, national policies systematically participate in national and international cybersecurity exercises, to elevate and strengthen established security procedures. Lastly, national policies similarly have established equivalent schemes for certifying the competence of information assurance and cyber security.

Promote counter cyber crime policy; Cyber crime policy has developed both multilaterally like with the Council of Europe’s Convention on Cyber crime (the Budapest Convention) or bilaterally. Given cyber crime's international character it is likewise the policy of the United States to encourage other countries to become parties to the Convention and help current non-parties use the Convention as a basis for their own laws. Within the European context, cyber crime policy further build upon the new EU Directive on attacks on information systems. Equally, all reviewed countries have committed to increase their law enforcement agency capabilities to combat cybercrime. In balance however, a cyber security policy model should

carefully scale institutional preferences related to online law enforcement at large. Canada to name but one example has delegated to the Royal Canadian Mounted Police domestic and international enforcement responsibilities. Yet the Canadian Security Intelligence Service, by the same token, is mandated to analyze and investigate domestic and international threats to the security of Canada.

Promote cyber security in international law; All countries reviewed share a unified commitment to the rule of law in cyberspace and to international law. The United Kingdom noticeably has explicitly adopted an additional international norm-based policy of tolerance and respect for diversity of language, culture and ideas. The Netherlands added on its behalf a commitment to peace which cyber security should uphold. Among the individual rights mentioned are mostly rights of privacy, freedom of speech and intellectual property. National policies reviewed have not mention however international humanitarian law or state responsibility policy preferences. For the application of international laws to cyberspace, it is important that existing international laws be adapted to cyberspace although much binding treaty and customary public international law (but even mere state practice) is still missing.

Form of regulation (legislation, courts, markets, norms, etc) & institutional aspects; The United States unlike other reviewed countries has gone in much detail into elaborating the role of technological standards in regulating cyber security. It has consequently called for industry-government cooperation over an open, voluntary and compatible standardization of the net's security. The US government further reiterates its understanding that such standard setting activity is not only commercially beneficial to the US economy but also industry-led by design. There is thus a conceptual gap between the United States and Canada, the United Kingdom and the Netherlands over this issue. The latter countries implicitly undermine the role of standards in regulating the net's security as they opt for either self regulation such as the Netherlands or state regulation backed by judicial review as implied by the United Kingdom or Canada.

Balancing cyber security with civil liberties; National cyber security policies equally share a commitment to enhance access to an secure, private, reliable and safe Internet. The United States further offers to protect Internet service providers (ISPs) and other providers of connectivity. The US national policy states so, while explaining that ISPs too often fall victim to legal regimes of intermediary liability that pass the role of censoring legitimate speech to such companies. Balancing cyber security with civil liberties is further promoted by international and regional partnerships with countries which share comparable basic values. Such values mentioned were commonly associated with freedom of speech and association, privacy, respect for basic human rights, and the rule of law at large.

Type of cooperation; Cyber security policies seems to be deeply intertwined with cooperation between countries internationally or regionally. Leading regional cooperative frameworks are NATO's cyber defense policy, ASEAN Regional Forum (ARF) Asia-Pacific forum or the Council of Europe and the Organization for Security and Co-operation in Europe. Government similarly collaborate with the private sector in public-private platform (PPP) initiatives in order to protect Federal, state, and local government as cyber threats are said to be business-driven in part. The United States cyber security policy further calls upon enhancing civil-military cooperation.

On the international level of cooperation, national cyber security policies deem cyber threats to be strongly associated with countries which share similar socio-political values and interests. In the countries reviewed these were Western

democratic countries or otherwise closest security and intelligence partners. Leading examples were Canada's closest intelligence partners namely the United States, the United Kingdom and Australia, or Japan's strategic alliance with the United States.

[i] The White House, International Strategy for cyberspace: Prosperity, Security, and Openness in a Networked World (May 2011)
[ii] *Id*., at 23.
[iii] *Id*., at 15.
[iv] *Id*., at 22.
[v] *Id*.
[vi] *Id*.
[vii] *Id*., at 19.
[viii] *Id*.
[ix] *Id*.
[x] *Id*., at 20.
[xi] *Id*., at 17.
[xii] *Id*., at 18.
[xiii] *Id*., at 17.
[xiv] *Id*., at 18.
[xv] *Id*., at 21.
[xvi] *Id*., at 23.
[xvii] *Id*., at 24.
[xviii] *Id*.
[xix] *Id*., at 19.
[xx] *Id*., at 20.
[xxi] *Id*., at 18.
[xxii] *Id*.
[xxiii] *Id*.
[xxiv] *Id*.
[xxv] *Id*., at 22.
[xxvi] The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world (November 2011). Earlier, Great Britain published its 2009 policy initiative to promote growth via the internet. See, UK Cabinet Office, Cyber Security Strategy of the United Kingdom: Safety, security and resilience in cyber space (London: The Cabinet Office, CM 7642, June 2009), at: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf.
[xxvii] The UK Cyber Security Strategy, *Id*., at 38.
[xxviii] *Id*., at 38.
[xxix] *Id*., at 42.
[xxx] *Id*., at 22.
[xxxi] *Id*., at 42.
[xxxii] *Id*.
[xxxiii] *Id*., at 36.
[xxxiv] *Id*., at 22.
[xxxv] *Id*.
[xxxvi] *Id*.
[xxxvii] *Id*.
[xxxviii] *Id*., at 36.
[xxxix] *Id*., at 37.
[xl] *Id*., at 38.
[xli] *Id*., at 42.
[xlii] *Id*., at 39.
[xliii] *Id*.

[xliv] *Id*., at 39.
[xlv] *Id*.
[xlvi] *Id*.
[xlvii] *Id*., at 41.
[xlviii] *Id*., at 22.
[xlix] *Id*.
[l] *Id*., at 39.
[li] *Id*., at 22.
[lii] *Id*., at 39.
[liii] *Id*.
[liv] *Id*.
[lv] *Id*.
[lvi] *Id*.
[lvii] *Id*.
[lviii] *Id*.
[lix] *Id*.
[lx] *Id*., at 40.
[lxi] *Id*., at 41.
[lxii] *Id*., at 40.
[lxiii] *Id*., at 41.
[lxiv] *See* Government of Canada, Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada, (2010), at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.
[lxv] *Id*., at 13.
[lxvi] *Id*., at 10.
[lxvii] *Id*.
[lxviii] *Id*., at 9.
[lxix] *Id*., ("*The Canadian Security Intelligence Service will analyze and investigate domestic and international threats to the security of Canada."*), at 10.
[lxx] *Id*., at 8.
[lxxi] *Id*.
[lxxii] *Id*.
[lxxiii] *Id*. (Canada is "*one of the non-European states that have signed the Council of Europe's Convention on Cybercrime*"), *Id*.
[lxxiv] *Id*. ("*Responsibility for digital security in the Netherlands lies with many parties. There is still insufficient cohesion between policy initiatives, public information, and operational cooperation. The Government therefore considers it essential to foster a collaborative approach between the public sector, the private sector, and knowledge institutions.*"), at 9.
[lxxv] *Id*. ("*Three of our closest security and intelligence partners, the United States, the United Kingdom and Australia, recently released their own plans to secure cyberspace. Many of the guiding principles and operational priorities set out in those reports resemble our own*."), at 8.
[lxxvi] Id., at 9.
[lxxvii] *Id*.
[lxxviii] *Id*., at 10.
[lxxix] *See*, Japanese Information Security Policy Council, Information Security Strategy for protecting the nation (2013). Earlier the Japanese Information Security Policy Council released the Information Security Strategy for Protecting the Nation, (May 11, 2010), at: http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf.
[lxxx] Japanese Information Security Policy Council, Information Security Strategy for protecting the nation (2013), at 45.
[lxxxi] *Id*., at 27.
[lxxxii] *Id*., at 48.
[lxxxiii] *Id*., at 32.
[lxxxiv] *Id*., at 40.
[lxxxv] *Id*., at 49-50.
[lxxxvi] *Id*., at 22.
[lxxxvii] *Id*.
[lxxxviii] *Id*., at 49.

[lxxxix] *Id*. (CSIRT is a "*system at businesses and government organizations for monitoring to check if any security issues exist with information systems and for carrying out investigations including cause analysis and extent of impact in the event an incident occurs.*"), at 22.

[xc] *Id*., at 24.

[xci] *Id*., at 50.

[xcii] *Id*., at 22.

[xciii] *Id*., at 26.

[xciv] *Id*., at 50.

[xcv] Japanese Information Security Policy Council, Information Security Strategy for protecting the nation (2013), at 33. Cyber incident Mobile Assistant Team (Information security emergency support team) (CYMAT) was established in in June of 2012, and provides technical support and advice related to preventing spread of damages, recovery, cause investigation and recurrence prevention in the event of cyber-attacks. *Id.*

ministries or other agencies under the National Information Security Center director who is the government

CISO.

[xcvi] Japanese Information Security Policy Council, Information Security Strategy for protecting the nation (2013), at 34.

[xcvii] *Id*., at 40 (NCFTA is "a non-profit organization established in the United States and made up of members from the FBI, private sector businesses and academic institutions.") *Id*.

[xcviii] *Id*., at 52. The Convention on Cybercrime has been ratified in the Japanese Diet in April of 2004, coming into effect on November 1, 2012 through the enactment of the "*Law for Partial Revision of the Penal Code, etc. to Respond to Increase in International and Organized Crimes and Advancement of Information Processing*". *Id.*

[xcix] *Id*., at 20.

[c] *Id*., at 23.

[ci] *Id*., at 28.

[cii] *Id*., at 20.

[ciii] *Id*., at 32.

[civ] *See* National Cyber Security, Strategy 2: From awareness to capability (2013). Beforehand see also Ministry of Science and Justice, The National Cyber Security Strategy (NCSS), The Ministry of Security and Justice, the Netherlands (2011).

[cv] *Id*., at 8.

[cvi] *Id*., at 8.

[cvii] *See* National Cyber Security, Strategy 2: From awareness to capability (2013), *Id*., at 8.

[cviii] *Id*. ("*the NCSC assumes the role of expert authority, providing advice to private and public parties involved, both when asked and at its own initiative."*), at 10.

[cix] The National Cyber Security Strategy (NCSS), The Ministry of Security and Justice, the Netherlands (2011), *Id.* ("*The Minister of Security and Justice is, in accordance with the National Security Strategy, responsible for coherence and cooperation on cyber security. At the same time, each party in the cyber security system has its own tasks and responsibilities*,"), at 6.

[cx] The National Cyber Security Strategy (NCSS), The Ministry of Security and Justice, the Netherlands (2011), *Id*. ("*Every party concerned must gain value from participation in joint initiatives – an outcome that will be facilitated by an effective cooperation model with clearly defined tasks, responsibilities, powers, and guarantees.*"), at 5.

[cxi] The National Cyber Security Strategy (NCSS), The Ministry of Security and Justice, the Netherlands (2011), *Id*. ("*The Netherlands supports and actively contributes to efforts such as the EU's Digital Agenda for Europe and Internal Security Strategy, NATO's development of cyber defense policy as part of its new strategic vision, the Internet Governance Forum, and other partnerships*."), at 6.

[cxii] *Id*. National Cyber Security, Strategy 2: From awareness to capability (2013) ("*coordination of supply and demand, which can be achieved by linking innovation initiatives to leading sector policy. In addition, the government, the business community and the world of academia will launch a cyber security innovation platform where start-ups, established companies, students and researchers can connect, inspire one another and attune research supply and demand.*"), *Id.*

[cxiii] *Id*. ("*An exploratory study is conducted to determine whether it is possible and useful, from both a technical and organizational perspective, to create a separate ICT network for public and private vital processes*."), at 9.

[cxiv] *Id.* ("*To enlarge the pool of cyber security experts and enhance users' proficiency with cyber security, the business community and the government join forces to improve the quality and breadth of ICT education at all academic levels (primary, secondary and professional education)*"), *Id.*

[cxv] The National Cyber Security Strategy (NCSS), The Ministry of Security and Justice, the Netherlands (2011), *Id.* ("*All users (individuals, businesses, institutions, and public bodies) should take appropriate measures to secure their own ICT systems and networks and to avoid security risks to others*".), at 6.

[cxvi] *Id.*, at 14 ("*This is not only an important precondition for the implementation of the government's plans concerning the concept of the digital government 2017, but also in view of the Government-Wide Implementation Agenda for eGovernment Services until 2015 (i-NUP), in which a basic infrastructure will be realized*."), *Id.*

[cxvii] *Id.* ("*There is a need for effective, swift and efficient investigation of cyber crime in accordance with clear rules. . . The Netherlands assumes a vanguard role in harmonising legislation governing international investigations, for instance in the Council of Europe. The Netherlands will also work to*

strengthen and expand international partnerships like EC3, at Europol."), at 10.In addition, ("*[t]he Royal Canadian Mounted Police will be given the resources required to establish a centralized Integrated Cyber Crime Fusion Centre*."), *Id*., at 13.

[cxviii] *Id.* ("*In the next few years, the existing program-based approach to cybercrime (PAC) will play a central part in creating a police knowledge centre, strengthening the police's organizational system, and shifting emphases within existing capacities*."), at 14.

[cxix] *Id.* Broadly upholding the findings of the 2010 National Report on Trends in Cybercrime and Digital Security and the National Security Think Tank's report on ICT Vulnerability and National Security. *Id.*, at 5.

[cxx] *Id*., at 13.

[cxxi] *Id.* ("*The goal of the hub for expertise is to promote the peaceful use of the digital domain. To this end, the Netherlands combines knowledge from existing centers. The centre brings together international experts and policymakers, diplomats, military personnel and NGOs.*"), *Id.*

[cxxii] *Id*., ("*To this end, the intelligence and security services have combined their cyber capabilities in the Joint Sigint Cyber Unit (JSCU)*"), at 9. Both 2010 (cyber conflict) and 2012 (cyber espionage) cyber security scenarios were included in the NV Strategy. *Id*., at 14.

[cxxiii] *Id.* ("*Finally, based on its own detection capability and its triage role in crises, the NCSC develops into Security Operations Centre (SOC) in addition to its role as a Computer Emergency Response Team (CERT).*"), *Id.*

[cxxiv] *Id*., ("*Together with private sector partners, the government works to develop standards that can be used to protect and improve the security of ICT products and services*."), *Id.*

[cxxv] The National Cyber Security Strategy (NCSS), The Ministry of Security and Justice, the Netherlands (2011), *Id.* ("*The public and private sectors will achieve the ICT security they seek primarily through self-regulation. If self-regulation does not work, the Government will examine the scope for legislation*."), at 6.

[cxxvi] *Id*., at 9.

[cxxvii] The National Cyber Security Strategy (NCSS), The Ministry of Security and Justice, the Netherlands (2011), *Id.* ("[*i]t aims to protect our society's core values, such as privacy, respect for others, and fundamental rights such as freedom of expression and information gathering. We still need a balance between our desire for public and national security and for protection of our fundamental rights.*"), at 6.

[cxxviii] *See* National Cyber Security, Strategy 2: From awareness to capability (2013), *Id.* ("*[t]he government, working with vital parties, identifies critical ICT-dependent systems, services and processes.*"), at 9.

[cxxix] *Id*., at 9.

[cxxx] *See* National Cyber Security, Strategy 2: From awareness to capability (2013), *Id*., at 14.

[cxxxi] *Id*., at 9.

END OF DOCUMENT