NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 16, ISSUE 3: MARCH 2015

TOWARDS A CYBERSECURITY POLICY MODEL: ISRAEL NATIONAL CYBER BUREAU CASE STUDY

Daniel Benoliel*

Designing and implementing a cybersecurity legal policy is an ambitious endeavor. This Article offers primary guidelines focusing on the national level, and uses Israel's newly created National Cyber Bureau as a case in point. Additionally, this Article offers a cross-section comparison between the national cybersecurity policies of the United States, the United Kingdom, Canada, Japan, and the Netherlands.

It further introduces additional considerations including the balancing of cybersecurity with civil liberties, cybercrime policy, adherence to international law and international humanitarian law, forms of regulation (technological standards, legislation, courts, markets, and norms), and prevalent forms of cooperation (intra-governmental, regional, public-private platform, and inter-governmental).

Ultimately, this Article could facilitate academic-government cooperation in the design of an archetypical cybersecurity policy model for countries henceforth.

* Associate Professor, The University of Haifa Faculty of Law and member of the Haifa Center of Law and Technology (HCLT). This Article was originally prepared for the Global Network of Interdisciplinary Internet & Society Research Centers—Network of Centers ("NoC") Internet Governance Case Studies Series and has been presented at a conference in the Nexa Center for Internet & Society—Politecnico di Torino, Turin, Italy. I wish to thank Tal Goldstein and Amit Ashkenazi with the Israeli National Cyber Bureau (INCB) for their important contributions. I also wish to thank Wolfgang Schulz, Ryan Budish, Niva Elkin-Koren, Dalit Ken-Dror, Rachel Aridor, Eldar Haber, and the participants of the Nexa conference. All disclaimers apply.

TABLE OF CONTENTS

I. INTRODUCTION

Recent revelations about the United States National Security Agency's ("NSA") clandestine electronic surveillance projects raised a public debate worldwide concerning the legality of government non-compliance with democratic principles.[1] From a national perspective, developing a comprehensive cybersecurity policy is challenging for two reasons. First, cybersecurity is largely shrouded with secrecy and over-classification. Second, the traditional major stakeholders in the field are national defense and intelligence agencies.

This excessive secrecy within the newly established Israeli National Cyber Bureau and elsewhere is already burdensome in current policy initiatives.[2] Not surprisingly, the original attempts to regulate cybersecurity for the private sector started with, and are still predominantly restricted to, technological standard setting and governmental-industry cooperation. To date, four such private sector endeavors are prevalent. These include the highly popular International Organization for Standardization's ("ISO") ISO 27001,[3] and ISO 27002[4]—two cybersecurity standards offering

---

[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 counters court-approved search terms. *See* Barton Gellman & Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, WASH. POST (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[2] LIOR TABANSKY, CYBERDEFENSE POLICY OF ISRAEL: EVOLVING THREATS AND RESPONSES 2 (2013), *available at* http://sectech.tau.ac.il/sites/default/files/publications/article_3_12_-_chaire_cyberdefense.pdf. Mr. Tal Goldstein, from the Israeli National Cyber Bureau, emphasized that, to a large extent, commercial enterprises themselves withhold their cooperation with INCB cyber defense organizations due to commercially-related secrecy concerns. Interview with Tal Goldenstein, Israeli National Cyber Bureau (Sept. 21, 2014).

[3] INT'L ORG. FOR STANDARDIZATION, *An Introduction to ISO 27001* (ISO27001), *available at* http://www.27000.org/iso-27001.htm (labelled as "specification for an information security management system (ISMS)").

[4] INT'L ORG. FOR STANDARDIZATION, *Introduction to ISO 27002* (ISO27002), *available at* http://www.27000.org/iso-27002.htm (offering "guidelines and

International Organization for Standardization and the International Electrotechnical Commission ("IEC") (jointly labeled "ISO/IEC") voluntary certifications for complying businesses. In addition, there are the Information Security Forum's ("ISF") Standard of Good Practice for Information Security ("SoGP"), which covers 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's ("CSA") best practices for cloud computing.[7] In the backdrop of this technical orientation towards cyber security, the focus has gradually been shifting onto other stakeholders interested in Internet governance-related policy. Such stakeholders typically preside within academia, international non-governmental initiatives, and governments regulating cybersecurity.[8]

To begin with, numerous governments have already taken on this initiative while offering the most advanced sets of cybersecurity policies. These are most noticeably the United States,[9] the United

---

general principles for initiating, implementing, maintaining, and improving information security management within an organization.").

[5] *See* Info Sec. Forum's (ISF), THE STANDARD OF GOOD PRACTICE FOR INFORMATION SECURITY (SOGP*), available at* https://www.securityforum.org/tools/sogp/.

[6] 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*, 3, http://www.opensamm.org/downloads/SAMM-1.0.pdf. 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* 35–37 (3rd ed. 2011), 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. *Id*.

[8] *See infra* notes 9–23 and accompanying text.

[9] *See generally*, Barack Obama. Exec. Order—Improving Critical Infrastructure Cybersecurity (February 12, 2013); The White House, *Presidential Policy*

Kingdom,[10] Canada,[11] Japan,[12] Germany,[13] the Netherlands,[14] and most recently, Israel, with its establishment of an Israel National

---

Directive—Critical Infrastructure and Resilience (February 12, 2013) (PDD-21); H.R. REP. NO. 3696, 113th Cong. 1st Session, *National Cybersecurity and Critical Infrastructure Protection Act of 2013;* U.S Dept. of Homeland Sec., NIPP 2013: *Partnering for Critical Infrastructure Security and Resilience*; THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (May 2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter INTERNATIONAL STRATEGY FOR CYBERSPACE]; *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); The 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.

[10] *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), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf (discussing Great Britain's 2009 policy initiative).

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

[12] *See* Information Security Strategy for Protecting the Nation (June 10, 2013), *available at* http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf. Earlier the Japanese Information Security Policy Council released the Information Security Strategy for Protecting the Nation. *See* Information Security Strategy for Protecting the Nation (May 11, 2010), *available at* http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf.

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

[14] *See* NATIONAL CYBER SECURITY, STRATEGY 2: FROM AWARENESS TO CAPABILITY (2013) [hereinafter NCSS 2]; *see also* The Netherlands Ministry of Science and Justice, THE NATIONAL CYBER SECURITY STRATEGY (NCSS) (2011) [hereinafter NCSS].

Cyber Bureau ("INCB") in 2011. These national initiatives have also served to characterize cybersecurity threats as predominantly national instead of merely global or international.[15] This Article focuses on the national level within this natural regulatory flow.

Other stakeholders have also begun initiating equivalent policies. For example, the NETMundial platform offers a fresh, bottom-up, NGO-based alternative.[16] This platform directly states as one of its seven principles for internet governance: "Security, stability[,] and resilience of the internet should be a key objective" and prioritizes "[e]ffectiveness in addressing risks and threats to security and stability of the Internet depends on strong cooperation among different stakeholders."[17] Similarly, the Organization for Security and Cooperation in Europe ("OSCE") has been discussing cybersecurity issues for many years, offering yet another

---

[15] Brigid Grauman, CYBER-SECURITY: THE VEXED QUESTION OF GLOBAL RULES: AN INDEPENDENT REPORT ON CYBER-PREPAREDNESS AROUND THE WORLD, 66–67 edited by Security & Defence Agenda (SDA) & McAfee Inc. Brussels: Security & Defence Agenda (SDA), 2012 [hereinafter the Security & Defence Agenda (SDA)].

[16] 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* NETMUNDIAL: GLOBAL MULTISTAKEHOLDER MEETING ON THE FUTURE OF INTERNET GOVERNANCE, http://netmundial.br/ (last visited Jan. 19, 2015); *see also GIP Exclusive Coverage of NETmundial,* GENEVA INTERNATIONAL PLATFORM, http://giplatform.org/events/netmundial (last visited Jan. 19, 2015).

[17] NETMUNDIAL, NETMUNDIAL MULTISTAKEHOLDER STATEMENT 5 (2014), *available at* http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf (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 April 22–24, 2014. NETmundial, ROADMAP FOR THE FURTHER EVOLUTION OF THE INTERNET GOVERNANCE ECOSYSTEM (2014), *available at* http://content.netmundial.br/contribution/roadmap-for-the-further-evolution-of-the-internet-governance-ecosystem/177 (reiterating international cooperation "on topics such as jurisdiction and law enforcement assistance to promote cyber security and prevent cybercrime"). 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 cybersecurity and prevent cybercrime." *Id.*

multinational discussion platform. To illustrate, at the 2010 OSCE Summit, the Heads of State and Government of the fifty-six participating states of the OSCE emphasized that "greater unity of purpose and action in facing emerging transnational threats" must be achieved, while offering an international "security community."[18] Significantly, the Astana Commemorative Declaration mentions cyber threats as one of these emerging transnational threats bridging the north-south divide between developed and developing countries.[19] Yet in comparison to the NETMundial policy platform, OSCE's Summit has not yielded more concrete cybersecurity recommendations to date.

Lastly, a landmark decision took place at the United Nations ("UN") in 2013. For the first time, a group of governmental experts from fifteen member states agreed to acknowledge the full applicability of international law and state responsibility to state behavior in cyberspace.[20] They did this by extending traditional transparency and confidence-building measures and by recommending international cooperation, making information and communications technology ("ICT") infrastructure more secure against cyber threats worldwide.[21] However, the decision has not yet become customary international law and is still nonbinding within public international law.

Information security has been on the UN's agenda since the Russian Federation first introduced a draft resolution in the First Committee of the UN General Assembly in 1998.[22] Since then, there have been annual reports by the Secretary-General to the General Assembly incorporating the views of UN member states. There have also been three Groups of Governmental Experts

---

[18] ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE,THE ASTANA COMMEMORATIVE DECLARATION: TOWARDS A SECURITY COMMUNITY arts. 9, 11 (2010), *available at* http://www.osce.org/cio/74985?download=true.

[19] *See id.* art 9.

[20] *See* U.N.G.A., GROUP OF GOVERNMENTAL EXPERTS ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY 5 (2013).

[21] *Id.* at 2.

[22] The General Assembly Resolution was adopted without a vote as G.A. Res. 53/70, U.N. Doc. A/RES/53/70 (Jan. 4, 1999).

("GGE") that have reviewed present and future cyber threats and cooperative measures.[23]

In the backdrop of these surfacing initiatives, this Article offers a comparative review of the Israeli National Cyber Bureau, which was established in 2011. The Article seeks to assist in constructing a comprehensive model national cybersecurity policy partially based on Israel's example, as well as those of the United States, the 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 one of the best. An international comparative study of twenty-three developed countries by a Brussels' security and defense think-tank within a Security & Defense Agenda's ("SDA") cybersecurity initiative recently awarded Israel with a top grade on "cyberdefense," alongside Sweden and Finland.[24] This rating is particularly impressive in light of the number of cyber attacks Israel faces—unlike the two relatively untested Scandinavian countries, Israel sees approximately 1000 cyber attacks within a hierarchy of threats every minute.[25] Second, Israel exports more cyber-related products and services than all other nations combined, excluding the United States.[26] Both Israel's technological

[23] The first successful GGE report was issued in 2010. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2009–2010, U.N. Doc. A/65/201 (2010). In 2011, the General Assembly unanimously approved a resolution calling for a follow-up to the last GGE. G.A. Res. 66/24, U.N. Doc. A/RES/66/24 (Dec. 22, 2011); *see* U.N. Office for Disarmament Affairs, *Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security* 2 (June 2013), *available at* http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf.

[24] *See* The Security & Defense Agenda (SDA), *supra* note 15*,* at 66–67.

[25] *Id.* at 66. In fact, different to the experience of most countries with advanced cybersecurity policies, Israel's policy 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 Tal Goldstein, Israeli National Cyber Bureau, *supra* note 2.

[26] *See* Barbara Opall-Rome, *Israel Claims $3B in Cyber Exports; 2nd Only to US*, DEFENSENEWS, (Jun. 20, 2014, 3:19 PM), http://www.defensenews.com/article/20140620/DEFREG04/306200018/Israel-Claims-3B-Cyber-Exports-2nd-

prominence and its being funneled by global market dominance have turned it into a global leader in the field and a precious, evolving, working example.

Part II introduces the Israeli National Cyber Bureau initiative and the Israeli government's underlying recommendations. Part III then maps main cybersecurity themes through the lens of the Israeli initiative. It opens with cybersecurity definitions including the range of cyber threats, types of cybersecurity risks, and types of practices not designated as cybersecurity risks.

Part III reviews models of cooperation over cybersecurity, including inter-governmental, public-private platform ("PPP"), and regional cooperation. Part III then considers specific cybersecurity-related legal topics including cybersecurity aspects in international law, cyber attacks and international humanitarian law, and cyber treaties and international treaty law. Part III further covers national and state responsibility for cyber attacks, cybercrimes and cyber security, international human rights law, and privacy law. Part IV then offers a cross-section policy comparison between five leading national cybersecurity policies of the United States, the United Kingdom, Canada, Japan, and the Netherlands. Lastly, Part V concludes with primary recommendations aimed at facilitating academia-government cooperation in designing a cybersecurity policy model for countries worldwide.

II. MISSION AND FUNCTION OF THE INCB

Israeli cybersecurity policy was established based on two major official milestones. The first was the 2010 National Cyber Initiative, which aimed for Israel to become a top five global cyber superpower by 2015.[27] The second milestone, coming after years of acknowledged departmentalized activities in various branches, was

---

Only-US (stating that last year Israel sales reached $3 billion which make approximately 5 percent of the global market).

[27] *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), translation provided by Daniel Benoliel.

Resolution No. 3611,[28] which adopted recommendations for the National Cyber Initiative.[29] At the core of these two initiatives stood the establishment of the INCB in the Prime Minister's office. The INCB reports directly to the Prime Minister.[30] The INCB's mission has been to serve as an advisory body for the Prime Minister, the government, and its committees presiding over national policy in the cyber field, and to promote its implementation.[31]

---

[28] Advancing National Cyberspace Capabilities, Isr. Res. 3611 (2011), *available at* http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf (unofficial, English version) [hereinafter Resolution No. 3611].

[29] Against this backdrop, the Israeli government sought to establish a national cyber policy as early as 2002. In the same year, Israel drew a list of nineteen major infrastructures incorporating power production, water supply or banking, held as either public or private with the purpose of standardizing core, albeit effectively limited legal and technological protection thereof. Security & Defence Agenda, *supra* note 15, 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* Tabansky, *supra* note 2, at 2. Israel undertook numerous other steps to address cyber threats. In 2002, a government decision established the State Israel Security Agency (Shabak unit) ("ISA"). The ISA is accountable for the specialized guidance of the bodies under its responsibility 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 an 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. See, ISA website—ISA Statute Chronology, at http://www.shabak.gov.il/english/about/pages/theisastatute.aspx.

[30] *See id.*; *see also* Advancing National Cyberspace Capabilities, *supra* note 28; *National Cyber Bureau*, PRIME MINISTER'S OFFICE, http://www.pmo.gov.il/ENGLISH/PRIMEMINISTERSOFFICE/DIVISIONSANDAUTHORITIES/CYBER/Pages/default.aspx (last visited Jan. 18, 2015).

[31] *National Cyber Bureau*, *supra* note 30 ("The Bureau functions as an advising body for the Prime Minister, the government and its committees, which recommends national policy in the cyber field and promotes its implementation, in accordance with the law and government resolutions.").

The INCB's mandate is threefold. First: defend national infrastructures from cyber attack.[32] This aspect has not been restricted to a traditional reactive strategy as it also considers a preventative approach.[33] Second: advance Israel as a world-leading center of information technology based on the country's technological advancement.[34] Third: encourage cooperation between academia, industry, and the private sector, as well as between government agencies and the security community.[35]

These broad policies were further detailed within Resolution No. 3611. The Resolution's first mentioned purpose and its *raison d'être* is officially establishing the INCB in the Prime Minister's Office.[36] The Resolution further calls for regulating responsibility for dealing with the cyber field albeit broadly.[37] Addendum B to

---

[32] *See id.*; *see also* Resolution No. 3611, *supra* note 28, 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[.]").

[33] *See* NATIONAL RESEARCH COUNCIL, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY (Washington, DC: National Academies Press, 2010) (overviewing the immense challenges facing a traditional law enforcement reactive cybersecurity deterrence); MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR (Santa Monica, CA: RAND, 2009). *But see*, Derek E. Bambauer, *Privacy Versus Security*, 103(3) J. OF CRIM. L. & CRIMINOLOGY, 667 (2013) (arguing that cybersecurity policy must focus on mitigating breaches rather than preventing them).

[34] Resolution No. 3611, *supra* note 28 at 1 ("[A]dvancing Israel's status as a center for the development of information technologies[.]"). 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 Prime Minister Benjamin Netanyahu Announces Creation of CyberSpark in Beer-Sheva*, BEN-GURION UNIV. OF THE NEGEV (Jan. 27, 2014), http://in.bgu.ac.il/en/Pages/news/CyberSpark.aspx. Two giant international companies, Lockheed Martin and IBM, have announced they will join Deutsche Telekom and EMC in setting up their research activities in the park. *Id.*

[35] Resolution No. 3611, *supra* note 28, at 1 ("[E]ncouraging cooperation among academia, industry and the private sector, government ministries and special bodies.").

[36] *Id.* at 2.

[37] *Id.*

the Resolution offers a model description of responsibilities, incorporating a Head Bureau position,[38] steering committee,[39] and related administrative working procedures.[40] 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.[41] Numerous concrete policies are then detailed by the Resolution, which could be categorized as educational, policy compliance-related, or strategic recommendations.

First, the INCB's educational-related recommendations proactively to identify and mitigate specific cybersecurity threats. The INCB is consequently said to devise "national education plans,"[42] generally aimed at "increasing public awareness" of cyber threats.[43] Similar to cybersecurity organizations of the North Atlantic Treaty Organization ("NATO"),[44] the United States Pentagon's cyber-command ("USCYBERCOM"),[45] Germany,[46] United Kingdom,[47] and Finland,[48] the Israeli Cyber Bureau is said to respectively coordinate national

[38] *Id.* at 8 (referring to Addendum B entitled: "Regulating Responsibilities for Dealing with the Cyber Field").

[39] *Id.*

[40] *Id.* at 8–9.

[41] *Id.* at 4–5. Two subsidiary decisions follow. The fourth is a budgetary decision has that been made in section 4, 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.* at 2. The fifth decision upheld in section 5, 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*.

[42] *Id.* at 4 (referring to Recommendation 14).

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

[44] The Security & Defense Agenda (SDA), *supra* note 15, at 71.

[45] *Id.* at 83.

[46] *Id.* at 64.

[47] *Id.* at 80.

[48] *Id.* at 61.

and international exercises,[49] as well as facilitate cooperation with parallel bodies abroad.[50]

And second, the Resolution sets numerous recommendations regarding policy compliance. These recommendations essentially proffer a tailored edition of policy checkpoints. The INCB is set to determine a yearly "national threat of reference,"[51] publish comparable ongoing "warnings,"[52] and identify "preventive practices."[53]

A national Computer Emergency Response Team ("CERT") was put in charge of the INCB's early warning apparatus.[54] The team conducts ongoing national assessments among various essential civil, security, and defense organizations while constituting a firsthand national defensive layer for the entire country's administration.[55] The national cyber situation room directly reports to INCB's central command.[56] One telling occasion sets a case in point concerning the CERT's contribution. During Operation Pillar of Defense, launched by Israel on November 14, 2012 against the Hamas-governed Gaza Strip**,** a massive-scale overseas cyber attack was carried out against Israel.[57] The attack targeted distributed denial of services ("DDoS"),[58] the defacement of Israeli websites, and the publication of citizens' data.[59]

---

[49] Resolution No. 3611, *supra* note 28, at 4 (referring to 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.*

[50] *Id.* Substantive international cooperation is still deemed questionable by INCB, as discussed *infra* Part C.II. *See* Interview with Tal Goldstein, *supra* note 2.

[51] Resolution No. 3611, *supra* note 28, at 3 (referring to Recommendation 5).

[52] *Id*. at 4 (referring to Recommendation 13).

[53] *Id.*

[54] *See Israeli National Cyber Bureau will Establish CERT*, HAIM RAVIA ADV., (Dec. 12, 2013) http://www.law.co.il/en/news/israeli_internet_law_update/2013/12/12/National-Cyber-Bureau-to-launch-Israeli-CERT/.

[55] *Id.*

[56] *Id.*

[57] Daniel Cohen & Danielle Levin, *Cyber Infiltration During Operation Protective Edge*, FORBES (Aug. 12, 2014), http://www.forbes.com/sites/realspin/2014/08/12/cyber-infiltration-during-operation-protective-edge/.

[58] *Id. See also* Chris Preimesberger, *DDoS Attack Volume Escalates as New Methods Emerge*, EWEEK (May 28, 2014) http://www.eweek.com/security/

The INCB further advances coordination and cooperation between governmental bodies, the defense community, academia, industrial bodies, business, and other bodies relevant to the cyber field.[60] INCB conveniently categorizes its projects into three general categories: the development of national cybersecurity infrastructure, the organization of human capital concerning that effort, and the maintenance of a cyber defense network, which includes the aforementioned cybersecurity room. INCB has thus far initiated three national security-related projects, all of which pertain to a multi-stakeholders' apparatus.

The first of three was an INCB project between 2012 and 2013 in cooperation with the Israeli Ministry of Defense's Research Authority and Development of Ammunition and Technological Infrastructure ("MAFAT").[61] Together, these organizations have allocated a sum of 10 million New Israeli Shekels (approximately $3.5 million (USD)) in a project labeled MASAD (per the initials of the term "Dual Cyber R&D" in Hebrew).[62] This joint civil-military project thus approaches the cybersecurity challenge from a dual standpoint. It similarly has endowed 32 million New Israeli Shekels (approximately $10 million (USD)) for the years 2012 through 2014 and is specifically aimed at fostering academic research in the field.[63]

INCB initiated a second national cybersecurity infrastructure product in cooperation with Israel's Office of the Chief of Scientist ("OCS") in the Ministry of Economy. In a project called KIDMA the Chief Scientist adopted a preferential policy for INCB's R&D projects. In compliance with INCB's commitment to the promotion of cybersecurity R&D, KIDMA is officially aimed

---

slideshows/ddos-attack-volume-escalates-as-new-methods-emerge.html (defining DDoS as denial-of-service (DoS) or distributed denial-of service (DDoS) attack as an attempt to make a machine or network resource unavailable to its intended users).

[59] Cohen & Levin, *supra* note 57.

[60] Resolution No. 3611, *supra* note 28, at 4 (referring to Recommendation 16).

[61] Press Release, Israel Prime Minister's Office, Israel National Cyber Bureau and Ministry of Defence Directorate for Research & Development Announce Plan to Advance Dual Civilian-Defense R&D Projects, *available at* http://www.pmo.gov.il/English/MediaCenter/Spokesman/Pages/spokemasad311012.aspx.

[62] *Id.*

[63] *Id.*

at promoting entrepreneurship within this field while preserving and increasing Israel's competitive edge in cybersecurity world markets.[64] The Chief Scientist implemented a program that endowed 80 million New Israeli Shekels (approximately $22 million (USD)) for 2013–14.[65]

A third national cybersecurity infrastructure project focuses on developing cybersecurity research centers through a partnership with academia. To date, INCB has collaborated with two Israeli universities in the establishment of two university research centers.[66] These are the Ben-Gurion University of the Negev, which focuses its research on technology and applicative sciences, and Tel-Aviv University, which has a broader interdisciplinary emphasis including political sciences and law.[67]

The underlying dual proposition upheld by INCB continuously has been that not only is academic research lagging behind the industry, but also this lag is in fact cross-disciplinary, including non-technological fields and, particularly, social sciences and law.[68] In response to this problem, in May 2014, the INCB and the Israeli Ministry of Science published a novel grant program as part

---

[64] KIDMA in Hebrew is an acronym "the promotion of cybersecurity research and development ('R&D')." *See generally* Press Release, Israel Prime Minister's Office, Israel National Cyber Bureau Head Announces Launch of KIDMA (Nov. 13, 2013) [hereinafter Launch of KIDMA], *available at* http://www.pmo.gov.il/English/MediaCenter/Spokesman/Pages/spokekidma131112.aspx (announcing the launch of Program KIDMA). *See also* Israel's Office of the Chief Scientist (OCS), NEWSLETTER 02-2012, (2012), http://www.moital.gov.il/NR/rdonlyres/89646959-5455-4A5A-99FD-C4B07D07E8E5/0/syber122012_3.pdf (stating that KIDMA includes upgraded funding for cybersecurity startups operating in technological incubators, a higher finance percentile in related venture capital funds, a fastened application examination process, etc.)

[65] *See* Launch of KIDMA, *supra* note 64.

[66] *See, e.g.*, *Major Cyber Security Center Launched at Tel Aviv University*, TEL AVIV UNIV. (Sept. 16, 2014), http://english.tau.ac.il/blavatnik_cyber_center (describing a new cyber-security program at Tel Aviv University). Two additional university research centers are presently being discussed. *See* Interview with Tal Goldstein, *supra* note 2.

[67] *Cf. Major Cyber Security Center Launched at Tel Aviv*, *supra* note 66; *see also*, Interview with Tal Goldstein, *supra* note 2

[68] *Id.*

of a broad and interdisciplinary approach, which appeals to scientists, engineers, political scientists, and lawyers alike.

The INCB has further developed a detailed program for promoting the development of human capital concerning cyber security. The INCB initiated advanced studies programs for cybersecurity in leading high schools with a strong technological curriculum and post-graduate academic programs. One such endeavor focuses on high schools within the socioeconomically disadvantaged country's periphery.[69] In another project labeled "Magshimim Leumit" ("Nationally Achieving" in Hebrew), the INCB and the Israel Ministry of Education established a three-year program, from 2013–16, focusing on educating and developing professional skills among outstanding high school students.[70] The program was founded under the assumption that through human capital development, the field of cybersecurity can and will improve greatly.[71]

The INCB regularly advises the Prime Minister, the government, and its committees regarding cyberspace.[72] It also consolidates the administrative aspects of cyber regulation,[73] and advances parliamentary legislation and secondary regulation in the cyber field.[74] In 2012, INCB declared that the Bureau would

---

[69] *Opening of National Youth Cyberwarfare Program*, ISRAEL PRIME MINISTER'S OFFICE, (Dec. 31, 2012), http://www.pmo.gov.il/English/MediaCenter/Events/Pages/eventmagshimim311212.aspx.

[70] *Id.*

[71] *Id.*

[72] Resolution No. 3611, *supra* note 28, at 3 (referring to 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 according to Recommendation 2 on behalf of the Bureau by means of the Israeli National Security Council. *Id*. Recommendation 19 authorizes the Bureau "[t]o carry out any other role in the cyber field determined by the Prime Minister." *Id.* at 4.

[73] *Id.* at 3. 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*.

[74] *Id.* at 4. Recommendation 18 adds that the Bureau will serve as a regulating body in fields related to cyber security. *Id*

incorporate four types of activities and accompanying objectives:[75] the promotion of cybersecurity for organizations, the promotion of cybersecurity for the industrial and civil sectors, market regulation, and cybersecurity regulation through technological standard setting.[76] From July to October 2012, INCB established recommendations for the government through a process that incorporated multi-stakeholder consultation.[77] This process focused on, rather confined, cyber law needs.[78]

Lastly and more importantly are three archetypical strategic propositions focused on establishing a measurable regulatory framework. The first strategic proposition solicits recommendations "to the Prime Minister and government regarding national cyber policy."[79] The second and third propositions are more general and thematic: to "promote research and development in cyberspace and supercomputing,"[80] and to devise a "national concept"[81] for coping with "emergency situations in cyberspace."[82] These three policies also underlay this Article's positive framework.

---

[75] *See INCB's Public Consultation with Multi-Stakeholders in Preparing Cyber Security Regulation*, PRIME MINISTER'S OFFICE, http://www.pmo.gov.il/sitecollectiondocuments/pmo/cyber.doc (last visited Sept. 10, 2014).

[76] *Id.*

[77] *Id.*

[78] *Id.* The process included four stages. Initially, 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 recommendations, which were at first open for public commentary, and then the INCB passed the final regulation recommendations to the Israeli government for consideration. *Id.*; *see also* Interview with Amit Ashkenazi, Israeli National Cyber Bureau (Sept. 18, 2014) (adding that it is clear that adapted legislation is needed yet the goal is not to opt for an overarching statute but rather a modular and proportional set of statutory frameworks for separate cyber threats).

[79] Resolution No. 3611, *supra* note 28, at 3 ("To 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.").

[80] *Id.* Such emblematic "research and development" should be promoted by undefined "professional bodies." *Id.*

[81] *Id.*

[82] *Id.* There remains yet a fourth trade policy-related recommendation that, while seminal in the Israeli Cyber Bureau's mandate, is nevertheless limited to advancement of the local economy. Recommendation 7 thus flatly calls upon the

III. THE POSITIVE FRAMEWORK

Several common cybersecurity themes have emerged in national cybersecurity policies worldwide. This section will discuss those themes. Cybersecurity definitions including the range of cyber threats, types of cybersecurity risks, and types of practices not designated as cybersecurity risks. In addition, models of cooperation over cybersecurity are reviewed including inter-governmental, PPP, and regional cooperation. Lastly, this Article considers specific fields of law for examination, including cybersecurity and international law, cyber attacks and international humanitarian law, cyber treaties and international treaty law, national responsibility for cyber attacks and state responsibility, Cybercrimes and cyber security, cyber attacks and international human rights law, and privacy and cyber security.

A. *Cybersecurity Definitions*

A cybersecurity policy model should include three categories of definitions that are repeatedly present in leading national cyber policies. First, a policy model should *define the range of cyber threats*: ranging from deliberate attacks for military or political advantage to the forms of Cybercrime, cyber warfare, and cyber terror against civil and military objects. Second, a policy model should *define the types of cybersecurity risks*: ranging from concealment (Trojan horse), infectious malware, 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). Last, a policy model should *define the types of practices not designated as cybersecurity risks*: including joke software, hoaxes, scams, spam and Internet cookies.

B. *Models of Cooperation Over Cybersecurity*

A cybersecurity policy model ought to map cooperative international arrangements, involving governments and civil society to reduce risks to cyber security. To date, INCB receives

---

Bureau to "work to encourage the cyber industry in Israel." *Id.* This important, yet only loosely relevant, topic will remain outside the scope this Article.

only a limited degree of international cooperation.[83] This is partially because few countries implement cybersecurity policies and even fewer countries have standing traditions of cyber industries funneled by policy-making mechanisms.[84] Additionally, international consensus could be difficult to achieve given a preference for regional and bilateral alternatives.[85] Notwithstanding these regulatory constraints, numerous cooperative avenues offer greater uniformity across countries.

1. *Inter-Governmental Cooperation*

In view of the national orientation of cybersecurity policies worldwide, inter-governmental cooperation could be expected to be a pivotal mode of cooperation. Alas, when countries opt for a cybersecurity policy, they generally maintain a national, or at most regional, framework for cooperation. The European Union and United States offer key illustrations.

a. *The European Union*

The European Union ("EU") Cyber Security Strategy, "An Open, Safe and Secure Cyberspace," and associated draft directives,[86] set the framework in the EU for cyber security.[87] 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 mirrors the 2009 EU Commission's issuance of a communication on Critical Information Infrastructure Protection ("CIIP"), entitled "Protecting Europe from large scale cyber attacks

---

[83] *See* Interview with Tal Goldstein, *supra* note 2.

[84] *Id.*

[85] *Id.*

[86] *See 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,* COM (2013) 48 final (Feb. 7, 2013), *available at* http://eur-lex.europa.eu/procedure/EN/202368.

[87] *See Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN (2013) 1 final (Feb 7, 2013), *available at* http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

and disruptions: enhancing preparedness, security, and resilience."[88] Similar to the Israeli case, the EU Commission has recently noted that the upcoming challenges for Europe are broadly fourfold. First, EU member states have uneven and uncoordinated national approaches.[89] Second, there is a need for a new European governance model for critical information infrastructures.[90] Third, there is limited European early warning and incident response capability.[91] Lastly, there is a prospective need for appropriate international cooperation.[92] Collaboration with non-European national cybersecurity policies such as the Israeli policy could be productive. This is the European Commission's call to engage the global community to develop a set of principles reflecting European core values for the Internet's resilience.[93]

Moreover, a cybersecurity 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.[94] The program requires all EU member states, and members of the European Economic Area ("EEA"), to incorporate components of the Programme into their national statutes.[95] Israel and the EU are continually discussing the EEA's integration based on a direct

---

[88] *See EU Commission, Communication on Critical Information Infrastructure Protection, Protecting Europe from Large Scale Cyber-attacks and Disruptions: Enhancing Preparedness, Security and Resilience,* COM (2009) 149 final (Mar. 30, 2009), *available at* http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf.

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Communication from the Commission: On a European Programme for Critical Infrastructure Protection,* COM (2006) 786 final (Dec. 12, 2006), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf. *See also* David Satola & Henry L. Judy, *Towards A Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations*, 37 Wm. Mitchell L. Rev. 1745, 1789 (2011).

[95] *Id.*

association agreement with Israel so the prospect of a harmonized edition of a cybersecurity 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.[96] ENISA serves as the EU's coordinated response to cybersecurity issues of the EU and offers yet another platform for inter-governmental cooperation over cybersecurity in the EU.[97]

b. *The United States*

A cybersecurity policy model could further borrow from the example of the 2009 Comprehensive National Cybersecurity Initiative ("CNCI") set forth by the United States government followed by the 2011 International Strategy for Cyberspace.[98]

Most elements of the United States' policy focus on the federal government's cybersecurity capability rather than relying on state governments.[99] In balance, however, similar to the Israeli case, the United States has still not firmly decided what the regulatory authority of the federal government should be in protecting critical infrastructure owned and operated by the private sector.[100] Nevertheless, the United States' designated policy priorities include: (1) the economy, (2) protecting its networks, (3) law enforcement, (4) military, (5) Internet governance, (6) international development, and (7) Internet freedom.[101]

---

[96] *See* European Network and Information Security Agency (ENISA), *National Cyber Security Strategies: Practical Guide on Development and Execution*, (December 2012), *available at* http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide.

[97] *Id.*

[98] *The Comprehensive National Cybersecurity Initiative*, THE WHITE HOUSE (May 2011), http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative; *see also* discussion *infra* Part IV.

[99] *See The Comprehensive National Cybersecurity Initiative*, *supra* note 98.

[100] *Id.*

[101] *See infra* Part III.C.

2. *Regional Cooperation*

A regional or inter-regional cybersecurity initiative incorporating future national examples could borrow from the model of Asia-Pacific's regional cooperation over cybersecurity in National Computer Emergency Response Teams ("CERT") by the Asia-Pacific CERT. This initiative already facilitates regional cooperation and coordination amongst CERTs and Computer Security Incident Response Teams ("CSIRTs").[102]

Another regional initiative that could provide an example of regional or inter-regional cooperation is the comparable Organization of American States' ("OAS") portal aimed at augmenting cybersecurity and regional responses to cybercrime.[103] This rather early-stage portal was created primarily to facilitate and streamline cooperation and information exchange among government experts from OAS member states.

3. *Public-Private Platform*

The business sector has taken on technology standardization initiatives since the early days of cyber security. Technology 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").[104] 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.[105]

Another important example of governmental cooperation with commercial enterprises and educational institutions, albeit with a

---

[102] Council for Security Cooperation in the Asia Pacific (CSCAP), *Ensuring A Safer Cyber Security Environment,* Memo. No. 20 (May 2012), *available at* http://www.cscap.org/uploads/docs/Memorandums/CSCAP%20Memorandum%20No%2020%20--%20Ensuring%20a%20Safer%20Cyber%20Security%20Environmenet.pdf.

[103] *See Inter-American Cooperation Portal on Cyber-Crime*, ORG. OF AM. STATES, http://www.oas.org/juridico/english/cyber.htm.

[104] For general information regarding ICANN, see https://www.icann.org/.

[105] *See* ENISA, *Good Practices Guide for Deploying DNSSEC* (Jan. 2010), http://www.enisa.europa.eu/act/res/technologies/tech/gpgdnssec.

technical orientation, are 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.[106] The lessons from CERTs are arguably still rather preliminary and necessitate further technical testing.

4. *Economics of Information Security Considerations*

The evaluation of incentives for multiple stakeholders to align their cybersecurity initiatives should further incorporate adherence to efficiency considerations.[107] Thus, cybersecurity policy may offer not only direct regulation, but also indirect regulation aimed at incentivizing efficient behavior by end-users. These suggestions may 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.

5. *Administrative Responses to Cyber Crises*

Administrative responses to cyber crises offer additional possibilities regarding the creation of a cybersecurity policy model. Such administrative responses include the Israeli Bureau's call for defining *emergency cyber situations* in Recommendation 8 of the INCB's recommendations, or the Bureau's called for definition for *cyber warnings* in Recommendation 13 to the INCB's recommendations.[108]

---

[106] *See Forum of Incident Response and Security Teams*, FIRST, http://www.first.org (last visited Feb. 20, 2015). The European Government CERTs (EGC) Group has twelve member organizations. *European Government CERTs (ECG) Group*, ECG GROUP, http://www.egc-group.org (last visited Feb. 20, 2015).

[107] Tyler Moore, *Introducing the Economics of Cybersecurity: Principles and Policy Options, in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 33, at 3.

[108] *See* discussion *infra* Part III.C.

C. *Cybersecurity and International Law*

Apart from the national character of most cybersecurity policies, there remains a myriad of international law issues that must be addressed by any policy model.

1. *Cyber Attacks and International Humanitarian Law*

This part 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 a cyber-armed conflict alongside its intensity dialectics, and the classification of cyber and unlawful combatants. It further includes 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.[109] These issues arise in a variety of forums and should be incorporated, at least in part, into a cybersecurity policy model. For example, in 2010 NATO issued a report of expert findings—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.[110] Equally important is the application of Article 51 of the

[109] Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defence, and Armed Conflicts*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 33, at 151. *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, 275–295 (2008).

[110] *See* Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO, *NATO 2020: Assured Security; Dynamic Engagement* (May 17, 2010), 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*. *See* INTERNATIONAL GROUP OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt, ed., Cambridge University Press 2013). The manual was written for NATO, although it does not necessarily represent NATO's views. The manual aims at defining cyber warfare under the international law and set rules to

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

2. *Cyber Treaties and International Treaty Law*

Cybersecurity and the challenge of international agreement within international treaty law and the 1969 Vienna Convention's definition warrants further consideration, especially considering that no single cybersecurity binding agreement within international treaty law thus far entered into force.[111]

3. *National Responsibility for Cyber Attacks and State Responsibility*

Within public international law, the State Responsibility doctrine—a 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.[112] One should recall the breakthrough 2013 agreement by the UN that acknowledges the applicability of international law and state responsibility in cyberspace.[113]

4. *Cybercrimes and Cybersecurity*

Cybercrimes and cybersecurity should be conveniently addressed within the scope of the 2001 Convention on Cybercrime

---

govern such conflicts including rules about the responsibility of the state or international humanitarian law. *Id.*

[111] *See* Abraham Sofaer et al., *Cyber Security and International Agreements*, in PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 33.

[112] *See generally* Lech J. Janczewski & Andrew M. Colarik, CYBER WARFARE AND CYBER TERRORISM (Lech J. Janczewski & Andrew M. Colarik eds., 2008).

[113] *See* U.N. Secretary-General, *Report of the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/68/98* (July 30, 2013). Surely, laws of state responsibility incorporate the principles governing the means by which a state is held responsible for a breach of an international obligation by one of its subjects. *See Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, Rep. of the Int'l Law Comm'n, 53d Sess., U.N. Doc A/56/10, GAOR, 56th Sess., Supp No 10, p 43 (2001).

(the "Budapest Convention") initially adopted by the Council of Europe ("COE").[114] The treaty addresses three issues that relate to cyber security. The first is cybercrime that nations should attend to in their criminal codes.[115] The second is the authorities governments should take on with the purpose of accessing communications or stored records for evidentiary needs.[116] The third issue in cybersecurity policy models is transnational cooperation mechanisms within the context of the Convention on Cybercrime.[117]

5. *Cyber Attacks and International Human Rights Law*

There is a paucity of literature from the lens of human rights over national and international cybersecurity.[118] The legal framework herein should remain distinct from national constitutional legal analyses given that international human rights law surely constitutes a separate public international legal analysis.[119]

6. *Privacy and Cybersecurity*

Privacy and security are occasionally conflated.[120] Academics and advocates oftentimes treat the two as exchangeable.[121] Security

---

[114] COUNCIL OF EUROPE, CONVENTION ON CYBERCRIME (2001), http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. This convention is also known as the "Budapest Convention."

[115] *Id.*

[116] *Id.*

[117] *Id.* 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. *See generally The History of Global Harmonization on Cybercrime Legislation—The Road to Geneva*, *available at* http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (providing a history of cyber crime harmonization); *see also infra* Part IV for comparison of cybercrime policies.

[118] *See* J. B. Wolf, *War Games Meets the Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money*, 28 AM. CRIM. L. REV. 95 (2000).

[119] *See infra* Part IV (discussing policies concerning civil liberties).

[120] *See, e.g.*, Derek E. Bambauer, *Privacy Versus Security, Journal of Criminal Law and Criminology*, 103 J. CRIM. L. & CRIMINOLOGY 667, 667 (2013) (illustrating meta argument beginning with the seminal work of Jon Mills).

and privacy should, however, be treated separately, at least in part. Privacy entails normative decisions about competing claims to legitimate access to, use of, and alteration of information.[122] Security on the other hand implements those choices while mediating between information and privacy selections.[123] Cybersecurity may thus require ongoing, preventive, and widespread surveillance along with significant collaboration with online intermediaries. As in the Israeli case, other countries have adopted data protection laws that follow the EU model,[124] the Organization for Economic Co-operation and Development ("OECD") model,[125] or the Asia-Pacific Economic Cooperation ("APEC") model.[126] Under these laws, the data controller, typically

---

[121] *Id.* at 669.

[122] *Id.* at 667.

[123] *Id.*

[124] *See* EUR. PARL. DOC. (EP-PE_TC1-COD(2010)0273)(2013). 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 of the European Union 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 cybersecurity concepts.

[125] *See* OECD, CYBERSECURITY POLICY MAKING AT A TURNING POINT: ANALYSING A NEW GENERATION OF NATIONAL CYBERSECURITY STRATEGIES FOR THE INTERNET ECONOMY (2012). *See 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.

[126] *See* APEC, THE FIFTH APEC MINISTERIAL MEETING ON TELECOMMUNICATIONS AND INFORMATION INDUSTRY (TELMIN5), STATEMENT ON THE SECURITY OF INFORMATION AND COMMUNICATIONS INFRASTRUCTURES (2002). The Asia Pacific Economic Cooperation ("APEC") Telecommunications and Information Working Group ("APEC-TEL") provides a forum for governments, businesses, and private sectors of the twenty-one APEC member states. At TELMIN 5 in Shanghai, China, on May 29–30, 2002, the Ministers 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, facilitate within, and work on the protection of information and communication infrastructures. Lastly, APEC-TEL holds projects in progress aimed at raising awareness regarding cybersecurity and cybercrime. That is, including the development of an APEC

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.

The latest revelations regarding the NSA's surveillance program designed to counter cyber-terror threats initiated a public debate regarding the limits of governmental powers in the United States.[127] 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 cybersecurity U.S. legislation, named as the Cyber Intelligence Sharing and Protection Act ("CISPA").[128] This proposed law alters the balance between security and civil

---

cybersecurity Strategy. *See also* Recommendation by the APEC Telecommunications and Information Working Group ("TEL") to APEC Senior Officials ("SOM") for an APEC Cybersecurity Strategy (2001).

[127] *See* Niraj Chokshi, *NSA Spying Appears to Stem From 550-Word Section of PATRIOT Act*, NATIONAL JOURNAL (June 7, 2013), http://www.nationaljournal.com/nationalsecurity/nsa-spying-appears-to-stem-from-550-word-section-of-patriot-act-20130607. Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 107 Pub. L. No. 107-56, 115 Stat. 272, § 215 (allowing the FBI in the aftermath of 9/11 terrorist attacks to apply the Secret Foreign Intelligence Surveillance Act ("FISA") court for an order to gather information "for an investigation to protect against international terrorism or clandestine intelligence activities").

[128] *See* Carol. M. Hayes and J. P Kesan, *At War Over CISPA: Towards a Reasonable Balance between Privacy and Security*, ILL. PUB. L. RESEARCH PAPER NO. 13-03 at 1 (2012), *available at* http://ssrn.com/abstract=2135618 (arguing 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 that should constitutes cyber security-related surveillance considerations is the 1994 the Communications Assistance for Law Enforcement Act (CALEA). This act overall 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. Communications Assistance for Law Enforcement, Pub. Law 103-414, 108 Stat. 4279 (1994).

liberties, while allowing sharing of Internet traffic information between the government and private companies.[129]

IV. A CROSS-SECTION COMPARISON

To date, over thirty countries have declared an archetypical national cybersecurity strategy.[130] Countries have conducted a very similar 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 cybersecurity policy model should therefore be especially attuned to leading national cybersecurity policies. This Part offers a cross-section comparison between five such countries, the United States, the United Kingdom, Canada, Japan, and the Netherlands.

[129] *Id.*

[130] *See e.g.*, EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA*), National Cyber Security Strategies in the World*, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (last visited July 14, 2014).

Cross-Section Comparison of Cybersecurity Policy

	United States[i]	United Kingdom[ii]	Canada[iii]	Japan[iv]	The Netherlands[v]
Promote Cybersecurity R&D	(1) Promote collaborative science and technology research to enhance cybersecurity tools and capabilities.[vi] (2) It is also essential to cultivating dynamic, international research communities able to take on next-generation challenges to cybersecurity.[vii]	Enable the UK cybersecurity industry to thrive and expand, while supporting it in accessing overseas markets.[viii]	---	Research 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.[ix]	(1) Promote research and education in cyber security.[x] (2) Encourage innovation in cyber security.[xi] (3) Feasibility study on separate vital network.[xii]
Promote Cybersecurity Education	(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[xiii] (2) In recent years, we have helped make this work a priority at	(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 cybersecurity issues throughout their supply chains.[xvii] (2) By March 2012, conduct research on how to improve educational involvement with cyber security significantly at all levels—including higher	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.[xix]	(1) It 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*."[xx] (2) It is necessary to plan awareness raising activities starting from the elementary and middle school education stages, and implement	(1) Promote research and education in cyber security.[xxii] (2) Create taskforce on cybersecurity education.[xxiii] (3) Encourage individual responsibility.[xxiv]

Cross-Section Comparison of Cybersecurity Policy

	United States[i]	United Kingdom[ii]	Canada[iii]	Japan[iv]	The Netherlands[v]
Promote Cyber Security Education (cont.)	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, and draw attention to this critical need.[xiv] (3) Continually develop and regularly share international cybersecurity best practices.[xv] (4) Enhance states' ability to fight cybercrime—including training for law enforcement, forensic specialists, jurists, and legislators.[xvi]	education and postgraduate level.[xviii]		participatory awareness raising projects such as motto and poster contests.[xxi]	
Ensure Ongoing Risk Assessment	(1) Ensure robust incident management, resiliency, and recovery capabilities for information infrastructure[xxv] (2) The United States Government actively participates in watch, warning, and incident	(1) There can be no such thing as absolute security. We will therefore apply a risk-based approach to prioritizing responses.[xxviii] (2) Improve our ability to anticipate the technological, procedural, and societal behavior	(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.[xxxi] (2) The Canadian Cyber	(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	(1) Ensure appropriate and up-to-date threat and risk assessments.[xxxvii] (2) Promote the information security awareness strategy for government administrators and managers. With the

Cross-Section Comparison of Cybersecurity Policy

	United States[i]	United Kingdom[ii]	Canada[iii]	Japan[iv]	The Netherlands[v]
Ensure Ongoing Risk Assessment (cont.)	response through exchanging information with trusted networks of international partners.[xxvi] (3) The United States will also work to engage international participation in cybersecurity exercises to elevate and strengthen established operating procedures with our partners.[xxvii]	developments that affect our use of cyberspace.[xxix] (3) Establish a scheme for certifying the competence of information assurance and cybersecurity professionals by March 2012, and a scheme for certifying specialist training in 2012.[xxx]	Incident Response Centre will direct the national response to any cyber security incident.[xxxii] (3) Public Safety Canada will also lead public awareness and outreach activities.[xxxiii]	external cyber attacks and put into operation in April of 2008.[xxxiv] (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 readiness system by the government together. In addition, in anticipation of large-scale cyber attacks, prepare countermeasures for the occurrence of incidents.[xxxv] (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.[xxxvi]	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.[xxxviii]

Cross-Section Comparison of Cybersecurity Policy

	United States[i]	United Kingdom[ii]	Canada[iii]	Japan[iv]	The Netherlands[v]
Promote Counter Cybercrime Policy	(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.[xxxix] (3) Protect intellectual property, including commercial trade secrets, from theft and industrial espionage.[xl] The persistent theft of intellectual property, whether by criminals, foreign firms, or state actors working on their behalf, can erode competitiveness in the global economy, and businesses' opportunities to innovate.[xli]	(1) Promote greater levels of international cooperation and shared understanding on cybercrime as part of the process begun by the London Conference on Cyberspace, in addition to promoting the Council of Europe's Convention on Cybercrime (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[xlii] (2) Encourage the courts in the UK to use existing powers to impose appropriate online sanctions for online offences[xliii] (3) Encourage the use of "cyber-specials" to bring in those with specialist skills to help the police[xliv]	(1) The Government will strengthen the ability of law enforcement agencies to combat cybercrime.[xlvi] (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[xlvii] (3) The Department of National Defense and the Canadian Forces will strengthen their capacity to defend their own networks will work with other Government departments.[xlviii]	(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 will occur including the advancement of Internet monitoring systems.[xlix] (2) The Japanese National Cyber-Forensics and Training Alliance (NCFTA) will take measures for sharing information through cooperation with the private sector, including the "Council to Prevent Unauthorized Communications" as a cyber intelligence	(1) International approach to cybercrime: updating and strengthening legislation (including the Criminal Code).[lii] (2) Program-based approach to cybercrime (PAC).[liii] (3) Intensify the investigation of cybercrime and prosecution of its perpetrators.[liv] (4) Create a pool of registered experts from the public and private sectors and knowledge institutions.[lv]

Cross-Section Comparison of Cybersecurity Policy

	United States[i]	United Kingdom[ii]	Canada[iii]	Japan[iv]	The Netherlands[v]
Promote Counter Cybercrime Policy (cont.)		(4) Significantly increase the law enforcement agency capability on cybercrime[xlv]		measure.[l] (3) Japan has ratified the Convention on Cybercrime and will work to strengthen rapid and effective mutual investigations and other cooperation between law enforcement agencies.[li]	
Promote Cyber Security in International Law		(1) 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).[lvi] (2) Governments should act proportionately in cyberspace and in accordance with national and international law.[lvii] (3) Maintain ability in terms of skills, technology, confidence,	---	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.[lxiii]	(1) Develop a hub for expertise on international law and cybersecurity ("Cyber diplomacy").[lxiv] (2) More active approach to cyber espionage.[lxv]

Cross-Section Comparison of Cybersecurity Policy

	United States[i]	United Kingdom[ii]	Canada[iii]	Japan[iv]	The Netherlands[v]
Promote Cyber Security in International Law (cont.)		and opportunity–to access cyberspace.[lviii] (4) Foster tolerance and respect for diversity of language, culture, and ideas.[lix] (5) Promote openness to innovation and the free flow of ideas, information and expression[lx] (6) Encourage respect for individual rights of privacy and intellectual property[lxi] (7) Foster a competitive environment to ensure a fair return of investment[lxii]			
Form of Regulation & Institutional Aspects	(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.[lxvi] (2) Developing international, voluntary, consensus-based cybersecurity standards	(1) Create a new national cybercrime capability as part of the new National Crime Agency by 2013.[lxviii] (2) Working with domestic, European, global and commercial standards organizations to stimulate the development of industry-led	Allows continual improvements to be made to meet emerging threats.[lxxii]	(1) For the diverse entities such as the government, public, academic, industrial, and private sectors in Japan, it becomes necessary for each entity to carry out its own information security measures in an independent and proactive fashion as part of its social responsibilities.[lxxiii]	(1) Strengthen the National Cyber Security Centre.[lxxviii] (2) NCSC develops into Security Operations Centre (SOC) in addition to its role as a Computer Emergency Response Team (CERT).[lxxix] (3) Supported standards, "security by design" and

Cross-Section Comparison of Cybersecurity Policy

	United States[i]	United Kingdom[ii]	Canada[iii]	Japan[iv]	The Netherlands[v]
Form of Regulation & Institutional Aspects (cont.)	and deploying products, processes, and services based upon such standards.[lxvii]	standards.[lxix] (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).[lxx] (4) Manage crucial skills and help develop a community of "ethical hackers" in the UK to ensure that its networks are robustly protected.[lxxi]		(2) It is important that the whole of society participated in the "cyberspace hygiene" as a preventative information security measure against unauthorized intrusions, malware infections, and vulnerabilities as factors for these incidents and other risks.[lxxiv] (3) Japan has worked 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.[lxxv] (4) The government must strengthen the basic functions of the nation related to cyberspace.[lxxvi] (5) Cyberspace-related operators will create a market through development of advanced	"privacy by design."[lxxx] (4) Utilize self-regulation if possible, legislation if necessary.[lxxxi]

Cross-Section Comparison of Cybersecurity Policy

	United States[i]	United Kingdom[ii]	Canada[iii]	Japan[iv]	The Netherlands[v]
Form of Regulation & Institutional Aspects (cont.)				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.[lxxvii]	
Balancing Cyber Security with Civil Liberties	(1) Preserve, enhance, and increase access to an open, global Internet is a clear policy priority.[lxxxii] (2) Support civil society actors in achieving reliable, secure, and safe platforms for freedoms of expression and association.[lxxxiii] 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	(1) Support the open internet, through 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.[lxxxvi] (2) Through the CONTEST strategy, increase its disruption of online radicalization and recruitment, and safeguarding against cyber attack.[lxxxvii]	Reflects Canadian values such as the rule of law, accountability and privacy.[xc]	(1) It is important to multilaterally build and strengthen partnerships with other nations and regions that 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 that promotes a balanced approach to constructing a safe and reliable cyberspace.[xci] (2) Cyberspace has provided us with a variety	(1) The Netherlands builds coalitions for freedom, security, and peace in the digital domain.[xciii] (2) Measures must be proportionate to the threat.[xciv]

Cross-Section Comparison of Cybersecurity Policy

	United States[i]	United Kingdom[ii]	Canada[iii]	Japan[iv]	The Netherlands[v]
Balancing Cyber Security with Civil Liberties (cont.)	speech down to companies.[lxxxiv] (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.[lxxxv]	(3) Use multilateral and bilateral channels to discuss how to apply the framework of international human rights law in cyberspace and to new challenges in guaranteeing such rights.[lxxxviii] (4) Actively engage in the UN Group of Government 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).[lxxxix]		of positive benefits including innovation, economic growth, and solutions for social issues, while still ensuring freedom of expression and protection of privacy.[xcii]	
Intra-Governmental Cooperation	(1) Agencies across the United States Government are collaborating, together with the private sector, to protect innovation from industrial espionage, to protect Federal, state, and local government	(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	Partnering to secure vital cyber systems outside the federal Government.[c]	(1) Advance threat analysis capabilities by promoting information sharing and strengthening cooperation with Computer Security Incident Response Team (CSIRT).[ci]	(1) Divided responsibilities between ministries.[civ] (2) Risk analyses, security requirements, and information sharing within critical infrastructure

Cross-Section Comparison of Cybersecurity Policy

	United States[i]	United Kingdom[ii]	Canada[iii]	Japan[iv]	The Netherlands[v]
Intra-Governmental Cooperation (cont.)	networks, to protect military operations from degraded operating environments, and to secure critical infrastructure against intrusions and attacks.[xcv] (2) Build and enhance existing military alliances to confront potential threats in cyberspace.[xcvi] (3) Given the Internet's importance to the world's economy, it is essential that this network of networks and its underlying infrastructure, the DNS, remain stable and secure.[xcvii]	Operations Group (DCOG). An interim DCOG will be in place by April 2012 and will achieve full operational capability by April 2014.[xcviii] (2) Support Olympic cybersecurity by joining up the relevant departments and conducting exercises to ensure preparations for cyber incidents are robust.[xcix]		(2) Government must work to strengthen the functions of the NISC (the "Cybersecurity Center" (tentative)) as a command post and promote collaboration among relevant actors including between ministries.[cii] (3) "Regarding Notation of Information Security Requirements in Procurement" was released to the various ministries, etc. on January 24, 2012 based on the results of the studies of the "Subcommittee for Strengthening Public-Private Collaboration" established in the Information Security Measure Promotion Council ("CISO Council") which is in turn established in the Information Security Policy Meetings.[ciii]	sectors.[cv] (3) Enhancing civil-military cooperation.
Regional Cooperation	Support the expansion of cyber security to geographic regions currently underrepresented in the	(1) Work with allies to implement NATO's cyber defense policy (agreed in June 2011).[cvi]	Canada will also build on its existing engagement in cyber security discussions at key international fora,	The country will actively participate in multi-country discussions and meetings including regional	The Dutch NCSS2 is in line with the fundamental principles of the EU Cyber Security

Cross-Section Comparison of Cybersecurity Policy

	United States[i]	United Kingdom[ii]	Canada[iii]	Japan[iv]	The Netherlands[v]
Regional Cooperation (cont.)	dialogue—most notably Africa and the Middle East—to further its interest in building worldwide capacity.[cvi]	(2) Work closely with the European Commission and the External Action Service to encourage greater coherence within the EU on cyber issues.[cviii] (3) Encourage international and regional organizations to support capacity building. Work with the Commonwealth (model legislation on cybercrime), the ITU (support training on technical standards), the Council of Europe and with the Organization for Security and Co-operation in Europe OSCE) to promote freedom of expression online.[cix]	such as the United Nations, NATO and the Group of Eight.[cx]	frameworks such as the ASEAN Regional Forum ("ARF") Asia-Pacific forum and other related committees in the United Nations.[cxi]	Strategy.[cxii]
Public-Private Platform (PPP) Cooperation	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	(1) Require everyone—the private sector, individuals and the government—to work together.[cxiv] (2) The expertise and innovation required to keep pace with the threat will be business-driven.[cxv] (3) Work with the	Emphasizes partnerships with Canadians, provinces, territories, Business, NGOs and academia.[cxviii]	(1) The multi-stakeholders in cyberspace need to fulfill each of the responsibilities corresponding to their respective roles in the society while mutually cooperating and assisting with each other including international cooperation	(1) Public-private partnerships.[cxxi] (2) Military and civil, public and private, national and international actors have become more intertwined.[cxxii]

Cross-Section Comparison of Cybersecurity Policy

	United States[i]	United Kingdom[ii]	Canada[iii]	Japan[iv]	The Netherlands[v]
PPP Cooperation (cont.)	international trade and commerce.[cxiii]	companies that own and manage its Critical National Infrastructure ("CNI") to ensure key data and systems continue to be safe and resilient.[cxvi] (4) Seek agreement with ISPs on the support they might offer to internet users to help them identify, address, and protect themselves from malicious activity on their systems.[cxvii]		and cooperation between the public and private sectors.[cxix] (2) It is expected that private companies, educational institutions, and research institutions will work together in industry-government-academia collaboration.[cxx]	
Inter-Governmental Cooperation	Insert cyberspace issues on the agenda at the OAS, the Association of Southeast Asian Nations ("ASEAN") Regional Forum ("ARF"), the APEC, the OSCE, the African Union, the OECD, the Group of Eight ("G-8"), the EU, the United Nations, and the Council of Europe.[cxxiii]	(1) Threats are cross-border, and a strategy requires partnership without countries that share the UK's views.[cxxiv] (2) Implement bilateral commitments set out in high-level communiqués (agreed to in 2010 and 2011) with the US, Australia, and France.[cxxv] (3) Develop new bilateral relationships on cyber with those emerging powers that are active in cyberspace.[cxxvi]	(1) Builds upon our close working relationships with its allies with special emphasis on Canada's closest security and intelligence partners, the United States, the United Kingdom, and Australia.[cxxvii] (2) To the extent possible, Canada will support efforts to build the cybersecurity capacity of less developed states and foreign partners.[cxxviii]	Cooperation with the United States, in which Japan is in an alliance based on the Japan-U.S. Security Arrangements, is vital.[cxxix]	(1) Active international cooperation.[cxxx] Note—The International Security Strategy is aimed at actions taken by the Netherlands abroad and in cooperation with other countries to secure its interests.[cxxxi]

V. CONCLUSION (AND BEST PRACTICES)

Israel's inauguration of the INCB cyber command and its upward national cyber policy has five facets. These are: (1) implementing a medium-run five-year plan to scale up the country as a world industry leader in cyber security; (2) investing in R&D based on interdisciplinary university research centers backed by extensive government funding; (3) encouraging industry to develop new technologies; (4) setting up a supercomputer center; and (5) boosting academic studies in cybernetics.[131]

The effectiveness of Israel's cyber policy is nevertheless still unfolding as many caveats apply. First, cybersecurity is still an evolving cross discipline, whereas future cyber risks and threats are remarkably untried. Any cybersecurity policy model should thus reflect this platitude and adhere to regulatory modularity funneled by administrative flexibility. Furthermore, national cybersecurity policies are often of a reactive nature, typically emerging only after equivalent cyber threats evolve. Israel's experience is no different. As a result, taken from the organizational angle, cybersecurity policies, in due course, hardly replace running administrative organs as they wind up conscientiously coordinating them. The INCB serves yet again as a proof positive. INCB's rather modest thirty-employee core hardly has the means to battle cyber threats directly.[132] That is, as INCB solely coordinates cyber policies by a myriad of local defense and civil agencies and corporations.

Another caveat applies, calling for certain restraint towards the Israeli example. Accordingly, as opposed to most cyber-literate countries worldwide, the INCB materialized in reaction to momentous national security threats unfamiliar, or at least moderately undemanding, in comparison to most of its counterparts. The fact that the cyber attacks that Israel faced were national security threats as opposed to less dangerous cybercrimes which many other nations face, led to a different kind of regulatory regime.

---

[131] *See* discussion *supra* Part II.
[132] *See* Interview with Tal Goldstein, *supra* note 2.

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

A. *Promote Cybersecurity R&D*

Following the experiences of the United States, Israel, and the United Kingdom, national commitment to research and development in cybersecurity is essential for two main reasons. Firstly, it cultivates dynamic international research communities able to take on next-generation challenges to cyber security. Secondly, this commitment enables national cybersecurity industries to expand and access overseas markets. Clearly, such practice should be adapted to the scientific educational frameworks and underlying national preferences.

B. *Promote Cybersecurity Education*

There are three significant types of educational policies within the cybersecurity context. To begin with, educational programs help nations gain the resources and skills to build core capacities in technology and cybersecurity. The promotion of cybersecurity education is meant to raise awareness among businesses of the threat and protective actions they may take. In recent years, the United States most noticeably helped make cybersecurity education a priority at multilateral forums such as the OAS, APEC, and the UN. Cyber security-related education and training is also promoted to help target cybercrime. In this context, cybersecurity education and training programs are aimed at law enforcement officials, forensic specialists, jurists, and legislators. The last educational policy is to improve educational involvement at higher education and postgraduate levels in order to construct a vibrant research community and related cybersecurity industries.

C. *Ensuring Ongoing Risk Assessment*

All national cybersecurity policies reviewed have developed a detailed watch, warning, and incident response to cyber threats through exchanging information with trusted networks. Similarly, nations systematically test their policies in national and international cybersecurity exercises to elevate and strengthen established security procedures. Lastly, national policies have established similar schemes for certifying the competence of information assurance and cyber security.

D. *Promote Counter Cybercrime Policy*

Cybercrime policy has developed both multilaterally like with the Budapest convention and bilaterally occasionally between nations. Given cybercrime's international character, it is likewise the policy of the United States to encourage other countries to become parties to the Budapest convention and help current non-parties use the Convention as a basis for their own laws.[133] Within the European context, cybercrime policy further builds upon the new EU Directive on attacks on information systems. Equally, all reviewed countries have committed to increase the capabilities of their law enforcement agencies to combat cybercrime. On balance however, a cybersecurity 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.[134] Yet the Canadian Security Intelligence Service, similarly, is mandated to analyze and investigate domestic and international threats to the security of Canada.[135]

E. *Promote Cybersecurity in International Law*

All countries reviewed share a unified commitment to the rule of law in cyberspace and to international law. Noticeably, the

---

[133] THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 9, at 20.

[134] *See Canada's Cyber Security Strategy*, *supra* note 11, at 10.

[135] *Id.*

United Kingdom has explicitly adopted an additional international norm-based policy of tolerance and respect for diversity of language, culture, and ideas.[136] The Netherlands added on its behalf a commitment to peace which cybersecurity should uphold.[137] Among the individual rights mentioned, across the countries reviewed, are those of privacy, freedom of speech, and intellectual property.[138] National policies reviewed have not mentioned 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 binding treaties and customary public international law (and even mere state practice) are still noticeably missing.

F. *Forms of Regulation & Institutional Aspects*

The United States, unlike the other reviewed countries, has gone into much detail in 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.[139] The U.S. government further reiterates its understanding that such standard setting activity is not only commercially beneficial to the U.S. economy, but also industry-led by design.[140] 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 Internet's security as they opt for either self-regulation such as the

---

[136] *See* UK CYBER SECURITY STRATEGY, *infra* note ii at 22.

[137] *See* NCSS (2011), *supra* note 14, at 9.

[138] *See, e.g.*, INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 9, at 21; UK CABINET OFFICE, THE UK CYBER SECURITY STRATEGY, PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD 22 (Nov. 2011), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf; Government of Canada, *supra* note 11, at 8; JAPANESE INFORMATION SECURITY POLICY COUNCIL, INFORMATION SECURITY STRATEGY FOR PROTECTING THE NATION 49 (2013), *available at* http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf.

[139] *See International Strategy for Cyberspace, supra* note 9, at 18.

[140] *Id.* at 23.

Netherlands or state regulation backed by judicial review as implied by the United Kingdom and Canada.

G. *Balancing Cybersecurity with Civil Liberties*

National cybersecurity policies equally share a commitment to enhance access to a secure, private, reliable, and safe Internet. The United States further offers to protect Internet service providers ("ISPs") and other providers of connectivity, 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 cybersecurity with civil liberties is further promoted by international and regional partnerships with countries that share comparable fundamental values. Such values were commonly associated with freedom of speech and association, privacy, respect for basic human rights, and the rule of law at large.

H. *Type of Cooperation*

Cybersecurity policies seem 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, and the Council of Europe and the Organization for Security and Co-operation in Europe. Governments similarly collaborate with the private sector in PPP initiatives in order to protect federal, state, and local government as cyber threats are said to be business-driven in part. The Netherlands' cybersecurity policy further calls upon enhancing civil-military cooperation.[141]

On the international level of cooperation, national cybersecurity policies reveal cyber allies to be strongly associated with countries that share similar socio-political values and interests. The countries reviewed were Western democratic countries or otherwise close security and intelligence partners. Leading examples were Canada's closest intelligence partners namely the United States, the United Kingdom, and Australia, and Japan's strategic alliance with the United States.

[141] *See* NCSS 2 (2013), *supra* note 14, at 9.

[i] INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 9.

[ii] UK CABINET OFFICE, THE UK CYBER SECURITY STRATEGY, PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD (Nov. 2011), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [hereinafter THE UK CYBER SECURITY STRATEGY]. Earlier, Great Britain published its 2009 policy initiative to promote growth via the Internet. *See* UK CABINET OFFICE, *supra* note 10.

[iii] *See* Government of Canada, *supra* note 11.

[iv] *See* JAPANESE INFORMATION SECURITY POLICY COUNCIL, INFORMATION SECURITY STRATEGY FOR PROTECTING THE NATION (2013), *available at* http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf.

[v] *See* NCSS 2 (2013), *supra* note 14; *see also* NCSS (2011), *supra* note 14.

[vi] INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 9, at 23.

[vii] *Id.* at 15.

[viii] *See* THE UK CYBER SECURITY STRATEGY, *supra* note ii, at 38.

[ix] JAPANESE INFORMATION SECURITY POLICY COUNCIL, *supra* note iv, at 45.

[x] NCSS 2 (2013), *supra* note 14, at 8.

[xi] *Id.* at 10 ("[C]oordination 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.").

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

[xiii] INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 9, at 22.

[xiv] *Id.*

[xv] *Id.*

[xvi] *Id.*

[xvii] THE UK CYBER SECURITY STRATEGY, *supra* note ii, at 38.

[xviii] *Id.* at 42.

[xix] Government of Canada, *supra* note 11, at 13.

[xx] JAPANESE INFORMATION SECURITY POLICY COUNCIL, *supra* note iv, at 27.

[xxi] *Id.* at 48.

[xxii] NCSS 2 (2013), *supra* note 14, at 9.

[xxiii] *Id.* at 10 ("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).").

[xxiv] NCSS (2011), *supra* note 14, at 6 ("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.").

[xxv] *See* INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 9, at 19.

[xxvi] *Id.*

[xxvii] *Id.*

[xxviii] THE UK CYBER SECURITY STRATEGY, *supra* note ii, at 22.

[xxix] *Id.* at 42.

[xxx] *Id.*

[xxxi] Government of Canada, *supra* note 11, at 10.

[xxxii] *Id.*

[xxxiii] *Id.*

[xxxiv] JAPANESE INFORMATION SECURITY POLICY COUNCIL, *supra* note iv, at 32.

[xxxv] *Id.* 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, causation investigation, and recurrence prevention in the event of cyber-attacks.

[xxxvi] *Id.* at 34.

[xxxvii] NCSS (2011), *supra* note 14, at 6.

[xxxviii] NCSS 2 (2013), *supra* note 14, 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 realised."),

[xxxix] THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 9, at 20.

[xl] *Id.* at 17.

[xli] *Id.* at 18.

[xlii] THE UK CYBER SECURITY STRATEGY, *supra* note ii, at 36.

[xliii] *Id.*

[xliv] *Id.*

[xlv] *Id.*

[xlvi] Government of Canada, *supra* note 11, at 9.

[xlvii] *Id.* at 10 ("The Canadian Security Intelligence Service will analyze and investigate domestic and international threats to the security of Canada.").

[xlviii] *Id.* at 10.

[xlix] JAPANESE INFORMATION SECURITY POLICY COUNCIL, *supra* note iv, at 40.

[l] *Id.* at 40 (stating that 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").

[li] *Id.* at 52. The Convention on Cybercrime has been ratified in the Japanese Diet in April 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.*

[lii] NCSS 2 (2013), supra note 14, at 10 ("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."); *see also* CAN. MINISTRY OF PUB. SAFETY, CANADA'S CYBER SECURITY STRATEGY: FOR A STRONGER AND MORE PROSPEROUS CANADA 13 (2010), *available at* https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf ("The Royal Canadian Mounted Police will be given the resources required to establish a centralized Integrated Cyber Crime Fusion Centre.").

[liii] NCSS (2011), *supra* note 14, at 14 ("In the next few years, the existing programme-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.").

[liv] *Id.* at 5 (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").

[lv] *Id.* at 13.

[lvi] THE UK CYBER SECURITY STRATEGY, *supra* note ii, at 22.

[lvii] *Id.*

[lviii] *Id.*

[lix] *Id.*

[lx] *Id.*

[lxi] *Id.*

[lxii] *Id.*

[lxiii] JAPANESE INFORMATION SECURITY POLICY COUNCIL, *supra* note iv, at 49–50.

[lxiv] NCSS 2 (2013), *supra* note 14, at 14 ("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.").

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

[lxvi] *See* INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 9, at 17.

[lxvii] Government of Canada, *supra* note 11, at 8.

[lxviii] THE UK CYBER SECURITY STRATEGY, *supra* note ii, at 36.

[lxix] *Id.* at 37.

[lxx] *Id.* at 38.

[lxxi] *Id.* at 42.

[lxxii] *Id.* at 8.

[lxxiii] JAPANESE INFORMATION SECURITY POLICY COUNCIL, *supra* note iv, at 22.

[lxxiv] *Id.*

[lxxv] *Id.* at 20.

[lxxvi] *Id.* at 23.

[lxxvii] *Id.* at 28.

[lxxviii] NCSS 2 (2013), *supra* note 14, at 10 ("[T]he NCSC assumes the role of expert authority, providing advice to private and public parties involved, both when asked and at its own initiative.").

[lxxix] *Id.* at 10 ("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).").

[lxxx] *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.").

[lxxxi] NCSS (2011), *supra* note 14, at 6 ("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.").

[lxxxii] INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 9, at 21.

[lxxxiii] *Id.* at 23.

[lxxxiv] *Id.* at 24.

[lxxxv] *Id.*

[lxxxvi] THE UK CYBER SECURITY STRATEGY, *supra* note ii, at 39.

[lxxxvii] *Id.*

[lxxxviii] *Id.* at 40.

[lxxxix] *Id.* at 41.

[xc] Government of Canada, *supra* note 11, at 8.

[xci] JAPANESE INFORMATION SECURITY POLICY COUNCIL, *supra* note iv, at 49.

[xcii] *Id.* at 20.

[xciii] NCSS 2 (2013), *supra* note 14, at 9.

[xciv] NCSS (2011), *supra* note 14, at 6 ("[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.").

[xcv] *See* INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 9, at 19.

[xcvi] *Id.* at 20.

[xcvii] *Id.* at 22.

[xcviii] THE UK CYBER SECURITY STRATEGY, *supra* note ii, at 39.

[xcix] *Id.*

[c] Government of Canada, *supra* note 11, at 8.

[ci] JAPANESE INFORMATION SECURITY POLICY COUNCIL, *supra* note iv, at 22 (explaining that 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").

[cii] *Id.* at 24.

[ciii] *Id.* at 32.

[civ] NCSS (2011), *supra* note 14, at 6 ("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.").

[cv] *See* NCSS 2 (2013), *supra* note 14, at 9 ("[T]he government, working with vital parties, identifies critical ICT-dependent systems, services and processes.").

[cvi] *See* INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 9, at 18.

[cvii] THE UK CYBER SECURITY STRATEGY, *supra* note ii, at 39, section 4.

[cviii] *Id.* at 41.

[cix] *Id.* at 40.

[cx] Government of Canada, *supra* note 11, at 8 (explaining that Canada is "one of the non-European states that have signed the Council of Europe's Convention on Cybercrime").

[cxi] JAPANESE INFORMATION SECURITY POLICY COUNCIL, *supra* note iv, at 50.

[cxii] NCSS 2 (2013), supra note 14, at 14.

[cxiii] *See* INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 9, at 18.

[cxiv] THE UK CYBER SECURITY STRATEGY, *supra* note ii, at 22.

[cxv] *Id.*

[cxvi] *Id.* at 39.

[cxvii] *Id.* at 41.

[cxviii] Government of Canada, *supra* note 11, at 9 ("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.").

[cxix] JAPANESE INFORMATION SECURITY POLICY COUNCIL, *supra* note iv, at 22.

[cxx] *Id.* at 26.

[cxxi] NCSS 2 (2013), supra note 14, at 5 ("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.").

[cxxii] *See id.*

[cxxiii] INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 9, at 18.

[cxxiv] THE UK CYBER SECURITY STRATEGY, *supra* note ii, at 22.

[cxxv] *Id.* at 39.

[cxxvi] *Id.*

[cxxvii] Government of Canada, *supra* note 11, at 8 ("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.").

[cxxviii] *Id.* at 9.

[cxxix] JAPANESE INFORMATION SECURITY POLICY COUNCIL, *supra* note iv, at 50.

[cxxx] NCSS 2 (2013), *supra* note 14, at 6 ("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.").

[cxxxi] *Id.*