National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

MORE THAN JUST ONES AND ZEROS : CANADIAN CYBER DETERRENCE POSTURE

Major Daniel Bégin

JCSP 45

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 45

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 45 – PCEMI 45
MAY 2019 – MAI 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

MORE THAN JUST ONES AND ZEROS: CANADIAN CYBER DETERRENCE POSTURE

By Major Daniel Bégin

"This paper was written by a candidate attending the Canadian Forces College in fulfillment of a one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of an agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

"La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale."

MORE THAN JUST ONES AND ZEROS: CANADIAN CYBER DETERRENCE POSTURE

INTRODUCTION

The threats and impacts of cyber-attacks are well documented today. Government's information systems and critical infrastructures (CI) providers are all interconnected and can consequently become vulnerable to cyber influence if not properly secured and defended. As recently as 2007, cyber threats were not officially recognized within the U.S. Government, but in 2015, cyber threats ranked first in the lists of threats to national security by the director of national intelligence.[1] The Russian hacking of the Democratic National Committee (DNC) servers during the last moments of the 2016 U.S. Presidential campaign[2], the destruction of more than 1,000 Iranian nuclear centrifuges in 2010 from the Stuxnet virus,[3] the 2014 North Korean cyber-attack on Sony Pictures and the subsequent unattributed cyber-attack causing a loss of all North Korean internet access[4] and the 2016 cyber subversion targeting a power grid company in Kiev, Ukraine,[5] are some cases where state actors used cyberspace to achieve national objectives and cause important physical impacts and consequences. Additionally, the Internet of Things (IoT) is expected to have more than 20 billion devices connected in the next five years, thus continuing to widen the spectrum of available cyber targets in the

[1] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," International Security 41, no. 3, (2017;2016;), Page 44-45, https://www.mitpressjournals.org/doi/full/10.1162/ISEC_a_00266.

[2] Alex, Wilner, "Cyber Deterrence and Critical-Infrastructure Protection: Expectation, Application, and Limitation," *Comparative Strategy* 36, no. 4 (2017), Page 314, https://www.tandfonline.com/doi/pdf/10.1080/01495933.2017.1361202?needAccess=true.

[3] Joseph Nye, "Deterrence and Dissuasion . . .," Page 48.

[4] Uri, Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence," *Journal of Strategic Studies* 40, no. 1-2 (2017), Page 110-111, https://www.tandfonline.com/doi/pdf/10.1080/01402390.2015.1115975?needAccess=true.

[5] Jun, Osawa, "The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?" *Asia-Pacific Review* 24, no. 2 (2017), Page 117, https://www.tandfonline.com/doi/pdf/10.1080/13439006.2017.1406703?needAccess=true.

future.[6] As a result of the current threats, of the attacks that have occurred and the ever growing interconnectivity of systems, nations have no other choice than to strengthen their cyber defensive posture in the future and to put in place necessary conditions to avoid such encounters in the first place. For this reason, the need for effective cyber deterrence strategies is required.

According to *Cyber Threats to Canada's Democratic Process* from the Canadian Communication Security Establishment (CSE), Canada is not immune to cyber threats and the likelihood of them "targeting Canada's democratic process during the 2019 federal election has increased."[7] The question to ask is what can Canada do to better protect itself and to influence potential adversaries that the costs of a cyber-attack against Canada will outweigh the benefits? This essay will explore the current trends in the field of cyber deterrence and attempt to understand why classical deterrence models seem to be insufficient in cyberspace. Additionally, this essay will evaluate Canada's current and future cyber deterrence posture. This essay will show that deterrence as a primary model is insufficient in cyberspace, and that Canada's current initiatives, although a step in the right direction, require additional efforts. Canada should focus on strengthening CI, increasing the overall cooperation with industries, and considering a greater leadership role internationally in the establishment of cyber norms and development of a legal cyber framework.

To prove this thesis, this essay will first examine the reasons that make cyber deterrence a unique and difficult challenge to solve. Second, it will lay out the most

[6] Joseph Nye, "Deterrence and Dissuasion . . .," Page 44.

[7] Government of Canada, Canadian Center for Cyber Security, "Update on cyber threats to Canada's Democratic Process," Last modified 5 April 2019, https://cyber.gc.ca/en/guidance/update-cyber-threats-canadas-democratic-process.

important proposed deterrence and compliance models in circulation today, namely the cumulative deterrence model, the mosaic model, the cyber persistence model and the approach proposed by Joseph Nye which includes deterrence by entanglement and norms. Lastly, it will evaluate Canada's current posture, considering the 2018 Canadian Cyber Security Strategy, the proposed Bill C-59 and international initiatives, in order to propose areas of improvement in the future. It should be noted that cyber deterrence in the context of this essay considers the deterrent threats as not limited to offensive and defensive cyber activity, but can include diplomatic, kinetic and economic threats as well. In other words, cyber weapons are not the only available tools to use to deter potential aggressors. Lastly, this essay will build on the idea of the need for an Active Cyber Defense strategy for Canada proposed by Alfred Lai.[8]

SECTION 1 - WHY IS CYBER DETERRENCE A COMPLEX PROBLEM

The Uniqueness of the Cyber domain

The cyber domain allows for a wide range of targets, a very low entry cost for its participants, and the ability to use cyber operations, activities, and actions (OAAs) to reach across interconnected Information Systems (IS), military capabilities, IoT and CI.[9] Unlike nuclear deterrence, where only a small number of state are able to participate, cyber OAAs are available to anyone with access to the internet and a desire to influence. From less sophisticated Script Kiddies such as *Anonymous*, non-state actors such as *Hacktivist*s, criminal organizations, robust and capable Advanced Persistent Threat

[8] Alfred Lai, "Cyber Deterrence: Implication for Canada and its allies," National Security Studies Course Paper, Canadian Forces College, 2018. Page 1-2.

[9] Michael P, Fischerkeller, and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2017), Page 382, https://www.sciencedirect.com/science/article/pii/S0030438717300431.

(APT) state actors; the type and quality of attacks are wildly different.[10][11] These attacks can be grouped into three categories. First, espionage attacks seek to gain access to an IS to extract desired information. A recent espionage example includes the theft of critical information regarding the F-35 Fighter program via cyber means.[12] Second, sabotage activities seek to weaken or destroy economic and military IS, Industrial Control Systems (ICS), and supervisory control and data acquisition systems.[13] In an attempt to retaliate to Stuxnet, Iran conducted several sabotage OAAs, including Distributed Denial of Services (DDoS) attacks on U.S. banks, and attacks on *Saudi Aramco* and Qatar's *Rasgas*, destroying thousands of computer systems.[14][15] The last category is subversion which seeks a “deliberate attempt to undermine the authority, integrity, and constitution of established authority or order.”[16] Examples of recent subversion OAAs include the 2016 Russian hack on the DNC as previously mentioned above, and the 2017 Russian release of nine gigabytes of emails from presidential candidate Emmanuel Macron days before the election.[17] Given that cyberspace also contains effectively three layers, namely the physical network layer, the logical network layer and cyber-personas layer, the previous types of attacks can also occur in each of those layers which exponentially increases the

[10] Ben, Buchanan, "Cyber Deterrence Isn't MAD; it's Mosaic," *Georgetown Journal of International Affairs* 15, no. SI (2014), Page 132 - 135, https://search.proquest.com/docview/1832801294?pq-origsite=summon.

[11] Johan, Sigholm, "Non-State Actors in Cyberspace Operations," *Journal of Military Studies* 4, no. 1 (2013), Page 24-29, https://content.sciendo.com/view/journals/jms/4/1/article-p1.xml.

[12] Michael P, Fischerkeller, and Richard J. Harknett, “Deterrence is Not a Credible Strategy . . .,” Page 384.

[13] *Ibid,.*

[14] Martin, Libicki, "Expectations of Cyber Deterrence," *Strategic Studies Quarterly* 12, no. 4 (2018), Page 48, https://search.proquest.com/docview/2166946651?pq-origsite=summon.

[15] Michael P, Fischerkeller, and Richard J. Harknett, “Deterrence is Not a Credible Strategy . . .,” Page 384.

[16] *Ibid,.*

[17] Wired Magazine, “The NSA Confirms It: Russia Hacked French Election ‘Infrastructure’,” Last modified 05 Septembre 2017, https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/.

types of attacks to deter.[18] Lastly, cyber OAAs can generally be accomplished via three distinct vectors: via network intrusion, via the supply chain procurement systems, and via careless or malicious human insiders.[19] The number of potential adversaries and motives, the means by which attacks can be orchestrated and the availability of targets make cyberspace a unique domain to operate, defend and ultimately deter.

Can Classical Deterrence Models apply to cyber?

Classical deterrence models work by convincing potential adversaries that the cost of their actions will outweigh the benefits of their gains, hence ultimately discouraging them from acting in the first place. Deterrence by punishment or retaliation seeks to avoid contact in the first place by threatening greater retaliation. For example, in the case of nuclear deterrence against Russia, the retaliation threat is the Mutually Assured Destruction (MAD) threat.[20] Deterrence by denial seeks to increase the difficulty of an adversary to achieve an objective, and seeks to lower the benefits of an aggression by making a target harder to get and keep, such as tripwires and air defense systems.[21] In order for these methods to be effective against an adversary, the threat of retaliation must follow the three *Cs* (Credibility, Capability, and Communication), or “the full formulation of one’s intent to protect a nation; [...] the acquisition and deployment of capacities to back up that intent; [...] the communication of intent to a potential aggressor.”[22]

[18] Aaron F, Brantly, "The Cyber Deterrence Problem," NATO CCD COE, 2018, doi:10.23919/CYCON.2018.8405009, Page 40, https://ieeexplore.ieee.org/document/8405009.

[19] Joseph Nye, “Deterrence and Dissuasion . . .,” Page 50.

[20] Alex, Wilner, “Cyber Deterrence and Critical-Infrastructure Protection . . .,” Page 310.

[21] Wess Mitchel, The American Interest, “The Case For Deterrence By Denial” last modified 12 August 2015, https://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial/.

[22] Aaron F, Brantly, "The Cyber Deterrence Problem . . .,” Page 36.

Up until recently, deterrence by denial was the main model used in cyber security, which aimed at passively hardening the security parameters of a system, but there are numerous problems associated with cyber deterrence. The most discussed issue is the difficulty of attribution. The internet and cyberspace was developed, and is still maintained today with an important requirement for anonymity: encryption, virtual private network tunnel, network address translation, proxy servers, and the triviality of spoofing addresses are just a few examples of protocols enforcing anonymity.[23] The possibility of a credible retaliation against an aggressor will likely diminish if the aggressor cannot be properly identified. In addition, "retaliation absent strong evidence is likely to lead to misidentification and unnecessary escalation."[24] However, when attribution is possible, it often requires significant amount of time to investigate and publish the findings, diminishing the credibility and capability of retaliation. In 2016, the U.S. indicted seven Iranians for DDoS OAAs for events that occurred between 2011 and 2013. These indictments are so temporally distant from the time of attack, that they were probably "ineffective at signaling deterrence."[25] Lastly, when attribution is done, the non-disclosure of the methods used to identify aggressors rarely provides prosecutable evidences.[26] Given the problems surrounding attribution, aggressors often resort to plausible deniability when accused of cyber-attacks,[27] which makes attribution the single most critical roadblock to effective cyber deterrence.

Other important factors of cyberspace make deterrence difficult. First, the covert nature of cyber OAAs act as a double edged sword for deterrence. Taking credit for cyber

[23] Hal, Berghel, "On the Problem of (Cyber) Attribution," *Computer* 50, no. 3 (2017): 87, https://ieeexplore.ieee.org/document/7888425.

[24] Aaron F, Brantly, "The Cyber Deterrence Problem . . .," Page 45.

[25] *Ibid*, Page 43.

[26] Hal, Berghel, "On the Problem of (Cyber) . . ," Page 86.

[27] *Ibid,* Page 87.

OAAs by conducting overt cyber activities could inherently communicate threats and retaliation options.[28] However, the effectiveness of cyber weapons is based on not communicating system vulnerabilities and exploit characteristics.[29] By doing so, a state would reveal the tools and methods used and would immediately lose the advantage it had, and therefore, lose any deterrent value. Second, the concept of equivalency and proportionality is also ambiguous within cyber deterrence. As retaliation should be of equivalent force to the act of aggression, it will be difficult to create an equivalency scale between "the initial event and the reprisal if the former takes place in the physical world and the latter takes place in the virtual world."[30] Third, denying access to IS is easier said than done. There appears to be many more opportunities to infiltrate systems in the virtual world than in the physical world.[31] This leads deterrence by denial to be less effective, and could motivate aggressors to resort to cyber rather than other 'better secured' and deterred domains like conventional kinetic and nuclear environments. Fourth, the cyber domain needs to have a deterrence model that will target all actors within it. Actors can range from rational state actors to irrational script kiddies who target infrastructure for fun, and both can produce significant damages.[32] Fifth, the red lines of what constitute an aggression are not clear and often change. The domain is emerging, and "the logic of deterrence has only just begun catching up" and the red lines are blurry.[33] "Moreover, there is currently no internationally agreed upon concept of

[28] Martin, Libicki, "Expectations of Cyber Deterrence . . ," Page 48.

[29] Jyri Raitasalo, The National Interest, "Cyber Deterrence is an Oxymoron for Years to Come," Last November 2018, https://nationalinterest.org/blog/buzz/cyber-deterrence-oxymoron-years-come-36352. Oxymoron article - page 7

[30] Martin, Libicki, "Expectations of Cyber Deterrence . . ," Page 50.

[31] Alex, Wilner, "Cyber Deterrence and Critical-Infrastructure Protection . . .," Page 310.

[32] *Ibid*, Page 313.

[33] *Ibid*, Page 314.

cyberspace sovereignty."[34] Sixth, cyber weapons are rapidly exchanged and easily created covertly. The spread of these weapons and methods will most likely be hard to control and the hope of achieving *cyber non-proliferation* is small.[35] Lastly, actors in cyberspace are interconnected and therefore constantly in a state of *contact* attempting to exert influence. How is it possible to deter aggressors from acting when they are already in contact with their target in a borderless environment?

In summary, while the classical deterrence models of retaliation and denial can bring some actors to operational restraint in cyberspace, they remain insufficient to prevent and control all types of aggressions. The nature of IS in cyberspace, the problem of attribution, and the uniqueness of cyber OAAs require a review of the efficacy of current models, and highlight the need to integrate new and innovative models.

SECTION 2 - PROPOSED MODELS AND ALTERNATIVES TO CYBER DETERRENCE

What does an effective deterrence model look like for cyberspace? Many authors wrote on this subject in an attempt to propose fulsome methods. However, the field of deterrence with respect to cyber has been described as an attempt to recycle conventional and nuclear cold war ideas.[36] This section seeks to illustrate the main ideas diverging from traditional models of absolute deterrence by denial and punishment.

Active Cyber Defence (ACD) Strategy

Networks and systems security have always been, and will continue to be assured by traditional network security operations. These operations are vulnerability focused,

[34] Michael P, Fischerkeller, and Richard J. Harknett, "Deterrence is Not a Credible Strategy . . .," Page 382.

[35] Dorothy, Denning, "Cybersecurity's Next Phase: Cyber-Deterrence," The New York Observer; New York, N.Y. [New York, N.Y]13 Dec 2016, Page 1, https://search.proquest.com/docview/1848526332?accountid=9867.

[36] Jyri Raitasalo, The National Interest, "Cyber Deterrence is an Oxymoron . . .," Page 6.

threat agnostic, industry safeguard compliant, and provide network and information assurance.[37] Traditional network security hardens systems, but fails to impose a cost on adversaries attempting to conduct OAAs against these systems. The ACD option, seeks to build on traditional network security foundations and add "real-time detection, analysis and mitigation [...] combined with aggressive use of legal countermeasures [...]"[38] Using deceptive strategies such as honeypots and sinkholes, ACD activities add a cost to adversaries OAAs by interference, delay, obstruction and trickery.[39] An important attribute of ACD, mentioned by Jasper Scott, is the possibility of ACD to occur on friendly terrain by Internal Defensive Measures (IDM), but also to occur outside the defended network going after threats by Response Actions (RA) activities.[40] ACD operations add to an overall deterrence model by increasing the denial cost of traditional network security with IDM, and by retaliation with RA activities. ACD operations are focused on adversary activities rather than a strict defensive posture, and are founded on intelligence, protection, fires, movements and maneuvers.[41] ACD strategies have been adopted by the U.S. Department of Defense in 2015,[42] and the UK government in 2016,[43] who recently posted positive results.[44]

[37] Department of National Defence, JDN 2017-02, Canadian Armed Forces Joint Doctrine Note - Cyber Operations, (Ottawa: DND Canada, 2017), D Cyber FD, Page 1-3.

[38] Scott, Jasper, "Strategic Cyber Deterrence – The Active Cyber Defence Option," Rowman & Littlefield, Maryland 2017, Page 18.

[39] *Ibid*, page 18.

[40] *Ibid*, page 23.

[41] Department of National Defence, JDN 2017-02, Canadian Armed Forces Joint Doctrine Note . . ., Page 1-3.

[42] National Security Agency, "Active Cyber Defense (ACD)," Last Modified 04 August 2015, https://apps.nsa.gov/iaarchive/programs/iad-initiatives/active-cyber-defense.cfm.

[43] Stuart Russell, Nadiya Kostyuk, Lawfare, "Evaluating the U.K.'s 'Active Cyber Defence' Program," Last Modified 14 February 2018, https://www.lawfareblog.com/evaluating-uks-active-cyber-defence-program.

[44] Ian Levy, National Cyber Security Center, "Active Cyber Defence - One Year On, "Last Modified 05 February 2018, https://www.ncsc.gov.uk/information/active-cyber-defence---one-year-on.

The implementation of ACD strategies poses some problems for states and corporations. They must establish an offensive capability capable of conducting IDMs and RA operations. They must acquire and configure surveillance systems to collect on various sensors and targets, often clashing with privacy laws.[45] Lastly, RA activities require to "hack back" which also poses significant legal dilemmas. ACD strategies are vastly capable and a good addition to traditional security defenses, but must be implemented with an offensive mindset and must be supported by laws.

A Four Pronged Approach: Punishment, Defense, Entanglement and Norms

Joseph Nye proposed a comprehensive approach to cyber deterrence utilizing punishment and defense as the traditional means to deterrence coupled with deterrence by entanglement and by norms. When used together, these four complementary methods can "reduce the likelihood of adverse acts causing harm in the cyber realm. They can complement one another in affecting actors' perception of the costs and benefits of particular actions."[46]

Deterrence by punishment. Nye acknowledges that the problem of attribution remains the biggest challenge for punishments to effectively constitute deterrence. However, when attribution is possible, he argues that states should make use of intra-domain retaliation as much as possible to include diplomatic, economic, cyber, physical force and nuclear force if necessary.[47] While punishment in the cyber domain remains "weak" in contrast to other means, intra-domain options can be more tailored for effective and proportionate retaliations.

[45] Forbes, "Caution: Active Response to Cyber Attacks Has High Risk," Last modified 29 November 2012, https://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/#5bf98e4a6d71.

[46] Joseph Nye, "Deterrence and Dissuasion . . .," Page 62.

[47] *Ibid,* Page 55.

Deterrence by Denial. The author proposed that an effective balance of defensive and offensive means in cyber is necessary to deter potential adversaries. He acknowledged the importance of differentiating between active defense and traditional security operations: "active defense goes beyond firewalls to patrolling inside one's networks."[48] In addition, he underlines that the importance of good cyber hygiene across systems, networks, and allies is fundamental to deter adversaries.[49] Such measures would remove low-hanging fruits from adversaries, and allow for the defending forces to maintain focus on CI rather than less important and trivial attacks, and to focus on APTs.[50]

Deterrence by Entanglement. Entanglement refers to the perception that maintaining the status quo provides more benefit than conducting cyber OAAs. The complex set of interactions between nations and organizations can lead to restraint in the cyber domain. The more interconnected nations are, the more complicated the cost-benefit calculation becomes. An example of cyber deterrence by entanglement could be: "a Chinese cyber-attack on the U.S. power grid imposing great costs on the U.S. economy, the two countries' economic interdependence would mean costly damage to China as well."[51] Entanglement deterrence can lead to cooperative restraint in cyber by capitalizing on small economic and diplomatic gains between nations and organizations.[52]

Deterrence by Norms. Similar to entanglement, cyber norms can impose a cost on an adversary even if retaliation and denial deterrence have not been successful.

[48] *Ibid,* Page 56.
[49] *Ibid,*.
[50] *Ibid,*.
[51] *Ibid,*.
[52] *Ibid,* Page 59.

Normative deterrence seeks to impose reputational costs and threatens to degrade the adversary's soft power.[53] Conducting cyber OAAs against established and internationally recognized norms increases the risk of nation's becoming the target of *naming and shaming* in cyberspace which has recently gained considerable notoriety and effectiveness.[54] There are many examples of work conducted in the establishment of norms in cyberspace internationally: (1) The U.S. proposal to apply the Law Of Armed Conflict (LOAC) in cyberspace with respect to attacks on civilians,[55] (2) The United Nation Group of Governmental Experts (UN GGE) studied the application of international law in cyberspace, and how to mitigate cyber threats with measures such as norms, rules and principles of responsible behavior of states,[56][57] (3) NATO's creation of the Cooperative Cyber Defense Center Of Excellence (CCDCOE) and its cyber defense pledge outlining seven conditions to abide for all participants,[58] (4) The Council of Council recommendations and efforts to reconvene the UN GGE to push for international cooperation for cyber vulnerabilities, to create a cybercrime convention, to accelerate

[53] *Ibid,* Page 60.

[54] Danny Palmer, ZDNet, "Naming and shaming nations that launch cyber attacks does work, say intel chiefs", Last Accessed On 26 April 2019, https://www.zdnet.com/article/naming-and-shaming-nations-that-launch-cyberattacks-does-work-say-intel-chiefs/#ftag=CAD-00-10aag7e.

[55] Joseph Nye, "Deterrence and Dissuasion . . .," Page 61.

[56] The Diplomat, "UN GGE on Cybersecurity: The End of an Era," Last Modified On 31 July 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

[57] NATO Cooperative Cyber Defense Centre Of Excellence (CCDCOE), "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law," Last Accessed On 01 April 2019, https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/. The UN GGE proposed in its final report in 2015 five limiting norms for all state to abide, including 1- Not knowingly allowing their territory to be used for wrongful cyber actions, 2- Not conducting illegal cyber activities with the intent to degrade critical infrastructures, 3- Take steps to strengthen supply chain security and integrity, 4- Not conducting cyber OAAs with the intent of targeting IS for state emergency response teams, 5- Respect UN resolution linked to human rights on the internet and the right to privacy. They also proposed six good practice and positive duties.

[58] North Atlantic Treaty Organization, "Cyber Defence Pledge," Last Modified On 8 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

efforts of cyber attribution, and to codify cyber-attack into international law,[59] (5) The Tallinn Manual study on how international law applies to cyber warfare and the cyber domain,[60] (6) The Microsoft proposal for six essential norms required for a Cyber Geneva Convention,[61] and (7) The Council of Europe Convention on Cybercrime proposal for the adoption of appropriate legislation and the fostering of international cooperation.[62] These activities occur internationally and at many levels of governments, and can foster cooperation between alliances, countries, industries, and security organizations.

In summary, Joseph Nye's approach is complementary and acknowledges that none of the four pillars presented can be a successful deterrent by themselves. Until such a time when the cyber attribution problem can be resolved, a comprehensive approach to deterrence using all available tools of power will be necessary to augment to classical and ACD strategies.

Mosaic Model

The Mosaic model, proposed by Ben Buchanan, seeks to use different deterrence methods based on threats, actors, and activities. Recognizing that threats take various forms in cyberspace, the model applies deterrence with two main attributes (assuming that the adversary has been identified): the first attribute is specific or general deterrence, and the second attribute can be absolute or restrictive.[63] More harmful OAAs, such as

[59] Council on Foreign Relations, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms," Last Modified On 23 Feb 2018, https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

[60] Schmitt, Michael N, and NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. Cambridge;New York, NY; Cambridge University Press, 2017.

[61] Microsoft, "The need for a Digital Geneva Convention," Last Modified On 14 February 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

[62] Council of Europe, "Details of Treaty No. 185 Convention on Cybercrime," Last Accessed 15 April 2019, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[63] Ben, Buchanan, "Cyber Deterrence Isn't MAD; it's Mosaic . . .," Page 135; The Author defines "Deterrence against a specific threat involves crafting a set of punishments designed to respond to a

Chinese and Russian Computer Network Attacks (CNA) against national CI must have a specific and absolute deterrence effect, whereas criminal activities and less sophisticated Computer Network Exploitation (CNE) can have a more general and less restrictive deterrence effect.[64] By acknowledging that absolute deterrence is not suited for all OAAs in cyberspace, this method assumes that contact will occur between adversaries and defenders. General and specific deterrence options offer a framework to prioritize systems, means, and efforts in cyber deterrence.

Strategy of Cyber Persistence

The strategic persistence model seeks to avoid the concept of operational restraint as one of the main tenets of Cyber deterrence, and replace it with the total control and dominance of cyber OAAs by the defender. This strategy seeks to dominate activities on systems and the internet to set the conditions for proper and favorable norms to be eventually established. It is based heavily on the ACD strategy discussed earlier, but contains a unique offensive cyber arm with automated IDM and RA activities to shape the environment. This offensive activity is described as a pairing of action-targets capable of denying, degrading, disrupting and destroying in cyberspace.[65] This strategy, while founded in information technology and cyberspace, also seeks to influence Information Operations (IO) to achieve total counter-subversion effects.[66]

specific action by a specific actor.” “General deterrence is the crafting of a set of punishments that are not targeted to any individual actor, but which could apply to any individual from a large and broadly-defined group of actors.” “Absolute deterrence seeks to prevent any deviant behavior of a particularly damaging sort, such as the launch of nuclear weapons.” “Restrictive deterrence seeks to encourage other actors to moderate their behavior in either quantity or quality in order to reduce the likelihood of consequences.”

[64] Ben, Buchanan, "Cyber Deterrence Isn't MAD; it's Mosaic . . .,” Page 138

[65] Michael P, Fischerkeller, and Richard J. Harknett, “Deterrence is Not a Credible Strategy . . .,” Page 389.

[66] *Ibid,* Page 391.

Israeli’s cumulative deterrence, a form of cyber persistence, is based on constant contact and continuous “burst of violence” to achieve the effect of deterrence in the long term.[67] The strategy assumes an aggressive posture with cyber OAAs in an attempt to introduce restrictive deterrence instead of relying strictly on an absolute deterrence approach and “shape the behavior of rivals in cyberspace rather than prevent all attacks [...].”[68] The ultimate goal is to draw effective ‘red lines’ using a norm based approach rather than an interest based approach. The author, Uri Tor, outlines five essential conditions to acquire cumulative deterrence: (1) effectively communicate ‘red lines’, (2) the ability and willingness to conduct cyber OAAs on aggressors, (3) the ability and willingness to threaten and demonstrate force, (4) to have overwhelming supremacy in cyberspace, and (5) to have and maintain a strong cyber security and deterrence by denial.[69]

One could argue that a strategy of cyber persistence does not essentially constitute deterrence, but rather a concept of compellence. However, some argue it is necessary in order to avoid escalation. This approach seeks to establish a form of cyber ‘peace’ by using strong offensive and defensive postures to ultimately achieve ultimate control of cyberspace. Critics to cyber deterrence argue that a state of compellence marries better to cyberspace than deterrence in general, hence the proposal for the cumulative model. However, the aggressive and controlling nature of this model may not be suited for nations who hold the values of privacy and freedom of speech to a high standard, and would most likely renounce to a surveillance state.

Recurring Themes

[67] Uri, Tor, "‘Cumulative Deterrence’ . . .,” Page 94.
[68] *Ibid,* Page 103.
[69] *Ibid,* Page 103-106.

In summary, proposed models and recent literature seem to agree on the difficulty of applying absolute deterrence to cyberspace and that relying strictly on cyber retaliation and strong cyber defense is not sufficient with today's threats. The adoption of an offensive cyber mindset to active defense takes into account the unique characteristics of cyberspace and acknowledges the constant state of contact. The importance of establishing and ratifying international cyber norms is a recurring characteristic of most models, along with the positive effect that international interconnectedness entanglement can have on deterrence. The importance of communicating 'red lines', of strengthening rules and norms within coalitions and alliances, and of creating clear policies to strengthen governments command and control of cyber deterrence activities all seem to be necessary for reducing the likelihood and impacts of cyber-attacks.[70]

SECTION 3 - CANADA'S POSTURE AND POTENTIAL FOR IMPROVEMENT

Amid the rising cyber threats, Canada must ensure that it is postured to maintain control of its information and CI. Canada is one of the most interconnected countries and Canadians spend more time online than any other country in the world.[71] In 2017, roughly 10 million Canadians, from ordinary citizens to corporations to different levels of government, experienced cybercrime costing $1.5 billions in damages and recovery.[72] Nation state actors, such as Russia and China, are constantly developing and deploying cyber weapons in attempts to gain access to Canada's networks, and communications of

[70] Alex, Wilner, "Cyber Deterrence and Critical-Infrastructure Protection . . .," Page 315-316.

[71] Government of Canada, Public Safety Canada, National Cyber Security Strategy, Page 1-5, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

[72] Symantec, "2017 Norton Cyber Security Insights Report Global Results," Last Accessed 2 May 2019, https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf.

government officials.[73] Are Canada's actions sufficient to prevent and deal with cyber-attacks in today's new threat environment? This section aims at reviewing Canada's current posture on cyber deterrence.

Canada's Cyber Security Strategy - a Way Forward

Released in 2018, Canada's Cyber Security Strategy aims at improving Canada's cyber posture with improvements in cyber security and resilience, cyber research and development and innovation and collaboration between federal, provincial and industry.[74] It creates, and at the same time, consolidates accountabilities, authorities, and coordination and collaboration efforts, within the Canadian Center for Cyber Security under the Canadian Security Establishment (CSE).[75][76] This center will provide a single authority for matters of cyber security, and will provide cyber security services to government departments and industry (namely those responsible to maintain CI), and cyber security advice for both the public and the private sectors. It also creates a National Cybercrime Coordination Unit under the RCMP acting as a hub for domestic and international allies.[77] Lastly, it creates a voluntary certification program for small and medium sized businesses to enhance their cyber security.[78]

The consolidation of authorities under the Center for Cyber Security will allow Canada to command and control all deterrence activities within Canada's infrastructure.

[73] Government of Canada - National Security and Intelligence Committee of Parliamentarians, Annual Report 2018," Page 27, www.nsicop-cpsnr.ca/reports/rp.../2019-04-09_annual_report_2018_public_en.pdf.

[74] Government of Canada, National Cyber Security Strategy . . ., Page 1-5.

[75] *Ibid*, Page III.

[76] Government of Canada, "Canadian Centre for Cyber Security," Last Accessed 2 May 2019, https://cyber.gc.ca/en/.

[77] Government of Canada, National Cyber Security Strategy . . ., Page III.

[78] Newswire, Cision, "Update - New Cyber Security Strategy bolster cyber safety, innovation and prosperity," Last modified July 13 2018, https://www.newswire.ca/news-releases/update---new-cyber-security-strategy-bolsters-cyber-safety-innovation-and-prosperity-688155151.html.

In addition, allowing for more cooperation between provincial governments, federal departments, and industry will allow for information sharing occurring faster. It is also a step in the right direction to achieve what Major Alfred Lai referred as a 'Whole-Of-Country' concept for cyber deterrence, where all private and public departments cooperate towards strong cyber security empowered by ACD strategies and systems.[79]

However, the Cyber Security Strategy is vague in certain areas. First, it does little in the consumers' education on the risks associated with IoT which will increasingly become an important attack vector to protect against.[80] Second, not enough is done to protect consumer information. As such, the Standing Committee on Banking Trade and Commerce (SCBTC) recommends making "necessary legislative changes to the Privacy Act and the Personal Information Protection and Electronic Document Act" to rapidly improve sharing of critical information between the private sector, government, and international partners.[81] Better information sharing of harmful cyber OAAs can lead to faster attribution which in turn increases the overall deterrence effect. For this reason, Canada must continue to improve information sharing between key sectors to ensure systems and CIs are covered. Third, while the strategy offers a voluntary certification program, it does little to motivate private sectors to upgrade their security posture and abide to national standards. As a result, the SCBTC recommends to provide "incentives

[79] Alfred Lai, "Cyber Deterrence: Implication for Canada and its allies," National Security Studies Course Paper, Canadian Forces College, 2018. Page 11.

[80] Senate Canada, the Standing Senate Committee on Banking, Trade and Commerce, "Cyber.Assault, It should keep you up at night," Page 19-20,https://sencanada.ca/en/info-page/parl-42-1/banc-cyber-security/; Often, government and industry information are the focus of all security activities within governments and security efforts. However, consumer's information must also be protected. IoT vulnerabilities will offer state-sponsored cyber activities opportunities to obtain information which can give foreign companies a competitive advantage over Canadian firms. This can have long term negative and economic impacts on Canada. For this reason, the report suggests more education to Canadians on the risks associated with IoT devices. An example of the importance to consider the protection of Canadian information can be seen today with the national debate whether or not Huawei's 5G technology can be authorized in Canada.

[81] *Ibid*, page 23.

to all business, particularly those in CI sectors" to strengthen security and comply with policy.[82] Lastly, the strategy outlines the authorities, but does not clarify leadership roles in emergencies. As a result, the SCBTC recommends furthering consolidating cyber security leadership with the creation of a minister of cyber security, reporting directly to the Prime Minister.[83] This would clarify roles and responsibilities, accelerate response times, and improve the covert/overt challenges of cyber OAAs discussed earlier.

In summary, the Canadian National Cyber Security Strategy adds to the overall deterrence effect against cyber aggression by centralizing authorities and policies, and by putting in place the conditions for better cooperation between different levels of government and the private sectors. However, modification and improvement in legislation, information sharing, leadership, incentives for the private sector, especially surrounding CI industries, and federal cyber structures are needed to improve Canada's overall deterrence posture.

Bill C-59 - Canada's entry in Active Cyber Defence and more

Canada's Bill C-59 is the proposed National Security Act which provides significant changes to intelligence gathering and the conduct of cyber security and operations. It proposes the establishment of the National Security and Intelligence Review Agency (NSIRA) to provide oversight and review any activities taken by

[82] *Ibid*, Page 27.
[83] *Ibid*, Page 30.

Canada's cyber agency, CSE.[84] It also creates the CSE Act, an act from which the CSE will now draw its authorities and mandates. This act outlines key aspects of the CSE's mandate, namely the conduct of defensive cyber operations, active cyber operations, information assurance and cyber security.[85] Whereas the provision of defensive operations will allow CSE to conduct and coordinate ACD-like activities such as IDM and RA operations, active operations (or offensive cyber operations), will create cyber state sponsored-like actors capable to "degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of foreign" actors.[86] Such a shift in cyber outlook in Canada will provide the tools to activate robust ACD strategies at many levels of government, and in support to the private sector. Furthermore, offensive activities would not only enhance deterrence by denial, but could provide the platform required to achieve certain aspects of deterrence by persistence or cumulative deterrence discussed above. Lastly, offensive maneuvers could allow for specific and restrictive deterrence options as proposed in the Mosaic deterrence model.

The main concern of Bill C-59 with respect to cyber deterrence is that it gives CSE, the same organization tasked to provide IT and cyber security for all Canadians, in other words, communicating and fixing dangerous vulnerabilities, the competing task of exploiting these vulnerabilities for strategic gains.[87] For the former, the vulnerability is required to be broadly and publicly communicated, whereas in the later, the vulnerability

[84] Government of Canada, Parliament of Canada, "Bill C-59, An Act respecting national security matter, Third Reading," Last accessed 26 April 2019, Page 2-5, https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/third-reading.

[85] *Ibid*, Page 67; CSE authorities used to be provided under the National Defence Act. Bill C-59 will consolidate the authorities of CSE under the new CSE act, separating them from the NDA.

[86] *Ibid*, Page 68.

[87] Canadian Civil Liberties Associations, "The New Communications Security Establishment Act in Bill C-59," Last Modified 12 Sept 2017, https://ccla.org/new-communications-security-establishment-act/.

must be kept secret until exploitation. In such instances, CSE would need to decide which role to prioritize. It is possible that the SCBTC's recommendation to create a separate minister of cyber security was aimed at that problem. Regardless, such confusing roles and single organization structure creates ambiguity in Canada's position on cyber security, and could have a negative effect on cyber deterrence.

The Canadian Armed Forces (CAF) also significantly shifted their approach with its definition of cyber operations as part of the new National Defence Policy, *Strong*, *Secured*, *Engage*. Particularly, the CAF recognized that solely relying on IT security and passive defensive cyber operations no longer meets the security requirements of today's threats.[88] As a result, SSE creates initiatives to develop active cyber capabilities, and to create a new Cyber Mission Assurance program that will be incorporated into the procurement process to protect supply chain cyber vectors.[89] Since then, the CAF published a detailed and comprehensive Joint Doctrine Note on Cyber Operations outlining "concepts required to operationalize the fundamental principles of cyber operations as a distinct operational domain."[90] The doctrine outlines the various cyber methods, such as defensive cyber operations, aka ACD, and offensive cyber activities within the context of a military operation. Consequently, the CAF is positioning itself to become an important actor in ACD and active cyber operations within the Government of Canada. However, the CAF's cyber capability must be created and operated jointly with CSE "until a certain degree of maturity is achieved."[91] As a result, operational deterrence

[88] Government of Canada, Strong, Secure, Engaged: Canada's Defence Policy, Ottawa: Department of National Defence, 2017, Page 72.

[89] *Ibid*, Page 73; the initiatives listed in the article refers to SSE's initiative number 87-88-89.

[90] Department of National Defence, JDN 2017-02, Canadian Armed Forces Joint Doctrine Note . . ., Page V.

[91] Guillaume Corriveau, "Canada's Foray Into Offensive Cyber: A joint CAF-CSE Endeavour," National Security Studies Course Paper, Canadian Forces College, 2018, Page 14.

to CAF activities abroad and at home will likely benefit from this added active and defensive cyber capability. Lastly, a stronger and more secure cyber CAF will fundamentally have positive effects on the overall Canadian cyber deterrence posture.

Canada's contributions internationally

Internationally, Canada is involved at many different levels influencing laws relating to cyber warfare and the establishment of norms in cyberspace. Canada contributed to the creation of the Tallinn 2.0 Manual which examines international law governing cyber warfare and is arguably the most comprehensive study of laws and norms in cyberspace today.[92] In addition, Canada participated heavily in the UN GGE in 2010, 2013, and 2015, maintaining that international, humanitarian and human rights laws also apply in cyberspace.[93] However, the 2017 UN GGE failed to reach a consensus due to competing Russian and Chinese objections; Canada contributed to a joint declaration in 2018 supporting more GGE efforts in cyberspace.[94] Canada also supported the 2018 Paris Call for trust and security in cyberspace, the UN backed Internet Governance Forum (IGF) which outlined six critical norms to rapidly introduce into laws,[95] ratified the Budapest convention within the Council of Europe, and is involved in developing norms on cyber-crime within the G7, the UN office of Drug and Crime, and the Organization of Americas States.[96]

[92] Schmitt, Michael N, and NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0* . . .

[93] Josh Gold, Canadian International Council, "Toward Norms in Cyberspace, Recent Progress and Challenges," Last accessed 25 April 2019, https://thecic.org/en/toward-norms-in-cyberspace-recent-progress-and-challenges/.

[94] Government of Canada, "Joint statement on Information and Telecommunications in the Context of International Security," Last Modified 7 Nov 2018, https://www.international.gc.ca/world-monde/international_relations-relations_internationales/un-onu/statements-declarations/2018-10-26-info_telecommunications.aspx?lang=eng.

[95] Josh Gold, Canadian International Council, "Toward Norms in Cyberspace . . ."

[96] Government of Canada, Global Affair Canada, "Cybercrimes," Last Modified 30 Jan 2019. https://www.international.gc.ca/crime/cyber_crime-criminalite.aspx?lang=eng.

Critics argue that Canada is not sufficiently leading the development of norms and should use its legacy of strengthening multilateral relations and rules-based order to create and export norms. Josh Gold, a doctorate student on cyber governance at the University of Toronto, proposes that Canada should lead the creation of an international strategy for cyberspace.[97] Overall, Canada is currently established as an important partner to develop, support and implement cyber norms, but more could be done leveraging Canada's long standing international reputation. Canada's current effort to strive for more leadership in multilateral forums should allow for more innovation and leadership in the development of norms.[98] Canada's growing multilateral economy and involvement in multitudes of cyber norm organizations worldwide proposes a strong potential for deterrence by norms and by entanglement. Canada must continue to maintain its current involvement, and should strive to consider more leadership responsibilities.

In summary, Canada seems to be advancing in the right direction to enhance its overall cyber deterrence in the future. The establishment of an updated strategy will allow for more authorities, accountability, and simplicity going forward, where bill C-59 should allow Canada's cyber force to effectively man oeuvre cyberspace to enhance deterrence by denial and by retaliation. However, recommendations are proposed to align various government departments and key private sector industries. Lastly, Canada's involvement internationally on the development of norms is a step in the right direction to provide deterrence by norms, but critics argue that more could be done to lead efforts and to establishing Canada as a cyber-norms pioneer.

[97] Josh Gold, Canadian International Council, "Toward Norms in Cyberspace . . ."

[98] Government of Canada, "Address by Minister Freeland on Canada's foreign policy priorities," https://www.canada.ca/en/global-affairs/news/2017/06/address_by_ministerfreelandoncanadasforeignpolicypriorities.html.

CONCLUSION

This essay has examined the challenges associated with cyber deterrence and the reasons why classical deterrence is insufficient. The uniqueness of cyber threats and OAAs and the characteristics of cyberspace, such as, the attribution problem, the constant state of contact, the impossibility of controlling the proliferation of weapons, creates an environment where a strategy of restraint, mostly encouraged by classical deterrence methods, cannot work by itself in cyberspace. As a result, many deterrence strategies build on current IT security foundations by putting emphasis on embracing contact with aggressors, such as the ACD strategy, cumulative deterrence, deterrence by persistence, and the mosaic model. All of these models provide additional tools to increase the control of the deterrent. In addition, the proposed model by Joseph Nye putting emphasis on deterrence by norms and entanglement makes full use of all available instruments of power to prevent and control acts of aggression in cyberspace. As was discussed, developing multilateral economies and ratifying internationally recognized cyber norms are critical factors of a comprehensive deterrence posture in cyberspace.

This essay has also looked at developments in Canada and how the current Canada Cyber Security Strategy and the incoming Bill C-59 are hopeful promises towards the establishment of ACD strategies. However, Canada must continue to improve the protection of its CI sector and strengthen the command and control of its cyber deterrence operation at the federal level. In addition, Canada's involvement on the international stage is a step in the right direction, but "Canada should steadfastly keep itself at the forefront of any norms processes for the internet and cyberspace."[99]

[99] Josh Gold, Canadian International Council, "Toward Norms in Cyberspace . . ."

As long as the problem of attribution remains a significant roadblock, states have to rely on comprehensive approaches to deterrence in cyberspace. Countries like Canada, will need to use all means of power to influence, compel, and motivate other states to remain peaceful and lawful when it comes to cyberspace. Is it possible that a strategy of international collaborative deterrence, where states are rewarded for restraining themselves in cyberspace and prosecuting aggressors internally, could be a necessary addition to the current deterrence model for cyberspace?

BIBLIOGRAPHY

Berghel, Hal. "On the Problem of (Cyber) Attribution." *Computer* 50, no. 3 (2017): 84-89. https://ieeexplore.ieee.org/document/7888425.

Buchanan, Ben. "Cyber Deterrence Isn't MAD; it's Mosaic." *Georgetown Journal of International Affairs* 15, no. SI (2014): 130-140. https://search.proquest.com/docview/1832801294?pq-origsite=summon.

Brantly, Aaron F. "The Cyber Deterrence Problem."NATO CCD COE, 2018. doi:10.23919/CYCON.2018.8405009. https://ieeexplore.ieee.org/document/8405009.

Canadian Civil Liberties Associations, "The New Communications Security Establishment Act in Bill C-59," Last Modified 12 Sept 2017, https://ccla.org/new-communications-security-establishment-act/.

Council of Europe, "Details of Treaty No. 185 Convention on Cybercrime," Last Accessed 15 April 2019, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Council on Foreign Relations, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms," Last Modified On 23 Feb 2018, https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

Corriveau, Guillaume. "Canada's Foray Into Offensive Cyber: A joint CAF-CSE Endeavour." National Security Studies Course Paper. Canadian Forces College. 2018.

Denning, Dorothy. "Cybersecurity's Next Phase: Cyber-Deterrence." The New York Observer; New York, N.Y. [New York, N.Y] 13 Dec 2016. https://search.proquest.com/docview/1848526332?accountid=9867.

Department of National Defence, JDN 2017-02, Canadian Armed Forces Joint Doctrine Note - Cyber Operations, (Ottawa: DND Canada, 2017), D Cyber FD.

Fischerkeller, Michael P. and Richard J. Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." *Orbis* 61, no. 3 (2017): 381-393. https://www.sciencedirect.com/science/article/pii/S0030438717300431.

Forbes, “Caution: Active Response to Cyber Attacks Has High Risk,” Last modified 29 November 2012, https://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/#5bf98e4a6d71.

Gold, Gold. Canadian International Council, “Toward Norms in Cyberspace, Recent Progress and Challenges,” Last accessed 25 April 2019, https://thecic.org/en/toward-norms-in-cyberspace-recent-progress-and-challenges/.

Government of Canada. Canadian Center for Cyber Security. “Update on cyber threats to Canada’s Democratic Process.” Last modified 5 April 2019. https://cyber.gc.ca/en/guidance/update-cyber-threats-canadas-democratic-process.

Government of Canada. Public Safety Canada. “National Cyber Security Strategy,” https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

Government of Canada. “National Security and Intelligence Committee of Parliamentarians, Annual Report 2018,” www.nsicop-cpsnr.ca/reports/rp.../2019-04-09_annual_report_2018_public_en.pdf.

Government of Canada. “Canadian Centre for Cyber Security.” Last Accessed 2 May 2019. https://cyber.gc.ca/en/.

Government of Canada. Senate Canada. “The Standing Senate Committee on Banking, Trade and Commerce. “Cyber.Assault, It should keep you up at night,”https://sencanada.ca/en/info-page/parl-42-1/banc-cyber-security/

Government of Canada. Parliament of Canada. “Bill C-59, An Act respecting national security matter, Third Reading.” Last accessed 26 April 2019, https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/third-reading.

Government of Canada. Strong, Secure, Engaged: Canada's Defence Policy. Ottawa:
Department of National Defence, 2017.

Government of Canada. “Joint statement on Information and Telecommunications in the Context of International Security.” Last Modified 7 Nov 2018. https://www.international.gc.ca/world-monde/international_relations-relations_internationales/un-onu/statements-declarations/2018-10-26-info_telecommunications.aspx?lang=eng.

Government of Canada. Global Affair Canada. “Cybercrimes,” Last Modified 30 Jan 2019. https://www.international.gc.ca/crime/cyber_crime-criminalite.aspx?lang=eng.

Jasper S. “Strategic Cyber Deterrence – The Active Cyber Defence Option”, Rowman & Littlefield, Maryland 2017.

Jyri Raitasalo, The National Interest, “Cyber Deterrence is an Oxymoron for Years to Come,” Last Modified November 2018, https://nationalinterest.org/blog/buzz/cyber-deterrence-oxymoron-years-come-36352.

Lai, Alfred. “Cyber Deterrence: Implication for Canada and its allies.” National Security Studies Course Paper, Canadian Forces College, 2018.

Levy, Ian. National Cyber Security Center. “Active Cyber Defence - One Year On.” Last Modified 05 February 2018. https://www.ncsc.gov.uk/information/active-cyber-defence---one-year-on.

Libicki, Martin C. "Expectations of Cyber Deterrence." *Strategic Studies Quarterly* 12, no. 4 (2018): 44-57. https://search.proquest.com/docview/2166946651?pq-origsite=summon.

National Security Agency. Active Cyber Defense (ACD). Last Modified 04 August 2015, https://apps.nsa.gov/iaarchive/programs/iad-initiatives/active-cyber-defense.cfm.

Microsoft. “The need for a Digital Geneva Convention.” Last Modified On 14 February 2017. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

NATO Cooperative Cyber Defense Centre Of Excellence (CCDCOE). “2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law.” Last Accessed On 01 April 2019.
https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.

North Atlantic Treaty Organization. “Cyber Defence Pledge.” Last Modified On 8 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

Newswire, Cision. “Update - New Cyber Security Strategy bolster cyber safety, innovation and prosperity.” Last modified July 13 2018. https://www.newswire.ca/news-releases/update---new-cyber-security-strategy-bolsters-cyber-safety-innovation-and-prosperity-688155151.html.

Nye, Joseph S. "Deterrence and Dissuasion in Cyberspace." International Security 41, no. 3 (2017;2016;): 44-71. https://www.mitpressjournals.org/doi/full/10.1162/ISEC_a_00266.

Palmer, Danny, ZDNet. “Naming and shaming nations that launch cyber attacks does work, say intel chiefs.” Last Accessed On 26 April 2019. https://www.zdnet.com/article/naming-and-shaming-nations-that-launch-cyberattacks-does-work-say-intel-chiefs/#ftag=CAD-00-10aag7e.

Sigholm, Johan. "Non-State Actors in Cyberspace Operations." *Journal of Military Studies* 4, no. 1 (2013): 1-37. https://content.sciendo.com/view/journals/jms/jms-overview.xml.

Schmitt, Michael N. and NATO Cooperative Cyber Defence Centre of Excellence. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge;New York, NY;: Cambridge University Press, 2017.

Stuart Russell, Nadiya Kostyuk, Lawfare, “Evaluating the U.K.'s ‘Active Cyber Defence’ Program.” Last Modified 14 February 2018. https://www.lawfareblog.com/evaluating-uks-active-cyber-defence-program.

Symantec, “2017 Norton Cyber Security Insights Report Global Results,” Last Accessed 2 May 2019, https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf.

The Diplomat, “UN GGE on Cybersecurity: The End of an Era,” Last Modified On 31 July 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

Tor, Uri. "‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence." *Journal of Strategic Studies* 40, no. 1-2 (2017): 92-117.https://www.tandfonline.com/doi/pdf/10.1080/01402390.2015.1115975?needAccess=true.

Osawa, Jun. "The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?" *Asia-Pacific Review* 24, no. 2 (2017): 113-131.https://www.tandfonline.com/doi/pdf/10.1080/13439006.2017.1406703?needAccess=true.

Wess Mitchell, The American Interest. “The Case For Deterrence By Denial.” Last modified 12 August 2015. https://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial/.

Wilner, Alex. "Cyber Deterrence and Critical-Infrastructure Protection: Expectation, Application, and Limitation." *Comparative Strategy* 36, no. 4 (2017): 309-318. https://www.tandfonline.com/doi/pdf/10.1080/01495933.2017.1361202?needAccess=true.

Wired Magazine. “The NSA Confirms It: Russia Hacked French Election ‘Infrastructure’.” Last modified 05 Septembre 2017. https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/.