National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

DUE ONLINE: IS CANADIAN CYBER CULTURE SECURE?

Maj R.J. Lyttle

JCSP 40

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 40

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 40 – PCEMI 40

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

DUE ONLINE: IS CANADIAN CYBER CULTURE SECURE?

Maj R.J. Lyttle

Word Count: 2471

Compte de mots: 2471

DUE ONLINE: IS CANADIAN CYBER CULTURE SECURE?

Canada is well known for Mounties, maple leaves and hockey. However, Canada is much more than a friendly and culturally diverse place to live. We excel in hi-tech fields, such as aviation, mining, communications and higher learning. Much of our technological advantage stems from the degree of adoption and integration of the internet in our daily lives. According to the Canadian Internet Registry Authority, in 2014 Canada ranked second in the G8 for internet penetration right behind the United Kingdom.[1] The internet, and cyberspace in which it operates, is best characterized by continuous change. From toddler to senior, "cyberspace has become an all-immersive domain, and the global communications environment in which all of society, economics, and politics are now embedded."[2] Unfortunately, cyberspace is not a benign environment. There are numerous actors who regularly pursue opportunities to enhance their own position or undermine that of another. In viewing Canada's position in cyberspace, it is necessary to understand the issues and the environment in which cyberspace operations take place, determine their impact on Canada's defence and security, and finally manage or mitigate the associated risks. Canada unveiled its Cyber Security Strategy in 2010. In the introduction of the strategy the Minister of Public Safety acknowledges that,

> Canadians – individuals, industry and governments – are embracing the many advantages that cyberspace offers, and our economy and quality of life are the better for it. But our increasing reliance on cyber technologies

[1] Canadian Internet Registration Authority, "The Canadian Internet," last accessed 30 May 2015, http://cira.ca/factbook/2014/the-canadian-internet.html

[2] The Huffington Post, "Cyber Security Canada is Failing the World," last modified 26 may 2011, http://www.huffingtonpost.ca/2011/05/26/cyber-security-canada-stephen-harper-g8_n_867136.html

> makes us more vulnerable to those who attack our digital infrastructure to undermine our national security, economic prosperity, and way of life.[3]

The Minister goes on to declare that, "Canada's Cyber Security Strategy is a cornerstone of our Government's commitment to keep Canada – including our cyberspace – safe, secure and prosperous."[4] Some would argue that the development of the strategy was late and under resourced in comparison to our allies.[5] This paper will discuss the legal basis for rights and obligations of a nation as they pertain to cyberspace. It will then discuss the implications of inaction through historical example and lastly elaborate on work to be done. The culmination of these steps will be used to show that Canadian cyber culture needs to change to continue to be relevant to the defence and security of our country in cooperation with our allies and international partners.

Cyberspace is defined as, "…the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship."[6] Given the vast international nature of such an environment with global reach, there have been some attempts to analyze the framework for its governance. In 2011, the White House conducted a review of cyber policy and identified that,

> The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace.[7]

---

[3] Public Safety, *Canada's Cyber Security Strategy* (Ottawa: Public Safety Canada, 2010), 1.
[4] *Ibid*.
[5] The Huffington Post, "Cyber Security: Canada is Failing the World."
[6] Public Safety, *Canada's Cyber Security Strategy*, 2.
[7] United States, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (Washington: The White House, 2011), 9.

As such, the common approach has been to use articles defined in the United Nations Charter to set limits and responsibilities on those that participate in the cyberspace domain. The first article relevant to the discussion is Article 2, Paragraph 4 which states that, "All Members [of the United Nations] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations."[8] In other words, it is unlawful for any state sponsored activity to infringe upon the access or use of cyberspace by any other state. This becomes important later on when we look at the issue of cyber warfare.[9] The second article commonly referred to when evaluating the governance of cyberspace within the context of customary international law and the justification of a state's response to the violation of Article 2 comes from Article 51 which states that, "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations…"[10] The concept of armed attack is fairly well understood that when one state drops a bomb on another state. Then, an armed attack has occurred which may justify a response under Article 51. However, in the cyber domain with the complexities of the integration of the network highlighted in the definition present in the Canadian Cyber Security Strategy and the often anonymous nature of would be attackers in cyberspace, attribution to a state can be difficult, if not impossible. It is also important to note that not every cyber operation rises to the level of a use of force. The Tallinn Manual discusses the necessity of a threshold to be met in order for an attack to be

[8] U.N. Charter, art. 2, para. 4.

[9] Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," Harvard International Law Journal (December 2012): 18.

[10] U.N. Charter, art. 51.

considered a use of force. The Tallinn Manual states that, "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[11] The manual further expands upon the idea of effects to say that, "[a]cts that injure or kill persons or damage or destroy objects are unambiguously uses of force."[12] So to answer the question of what constitutes a cyber-attack, Hathaway et al., have defined a cyber-attack in terms of its objectives in their work on The Law of Cyber Attack, "A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose."[13] Upon reflection, there are other cyber operations that could be undertaken where the use of force threshold is not met and therefore not considered a cyber-attack. However, this does not abdicate a state's responsibility to secure their networks from these other forms of attack, such as; cyber-crime, cyber-espionage or cyber-exploitation. Any or all of these could compromise a technological advantage or economic stability nationally, regionally or globally. Canada must be vigilant to avoid the loss of sensitive information that could weaken relationships with our allies, deteriorate economic stability or result in the loss of privacy for our citizens. The actors seeking to exploit our networks are global and not necessarily state-sponsored, which complicates the types of activities and sources to be monitored. Security in cyberspace is a broad discipline that extends beyond the technical realm to procedural. The actions of those that use our networks are as important as the official organizations that seek to protect us from malevolent cyber operations. Unfortunately, the vast majority of Canadians approach their online presence as an open

---

[11] Michael N. Schmitt, "International Law in Cyberspace…" 19.

[12] *Ibid.*

[13] Oona A. Hathaway et al., "The Law of Cyber Attack," California Law Review, Vol. 100 Issue 4 (August 2012): 826.

book for all to see. Social media in particular is in prevalent use with little regard for the potential repercussions. Therefore, it is quite easy for an individual or group to port their habits from personal use to work related use without consciously considering the implications or appropriate security precautions. Thus far, the cyberspace environment has been explored to define its constituent parts; an assembly of relevant statutes, ideas and deductions on cyberspace governance from a customary international law perspective, and lastly an introduction to other cyber threats to be considered when developing, implementing and monitoring the risks related to cyberspace threats. The next section will look at the implications of inaction or inadequate cyberspace security preparations, as they relate to both domestic and international historical examples.

There are four main elements that make cyber-attacks or operations attractive. Generally, the attacks are: inexpensive, easy, effective and low risk.[14] While internationally, there have been numerous reports of hackers attacking various enterprises in the news compromising client databases and intellectual property, it is not only open internet based networks that are vulnerable to attack. Other networks vulnerable to attack are closed or secure networks that contain more sensitive data and enable more complex processes. Notwithstanding an inability to openly attribute the source of attack to a particular state-sponsored organization, the unprecedented attack against the Canadian Government in 2011 was a wake-up call to this country.[15] The effective penetration of Treasury Board and the Department of Finance drove the two government departments to disconnect access from the internet for a prolonged period of time to prevent the compromised network from sending information back to its source. The effective use of

[14] Public Safety Canada. *Canada's Cyber Security Strategy, 4-5.*

[15] Jordan Press, "Canada's military squeezed out of cyber-defence, email warns," *Ottawa Citizen*, 12 March 2014

a spear-fishing attack resulted in the compromise of system passwords that reportedly permitted access to classified financial records, among other data.[16] The Government of Canada has largely remained silent about the contents of the compromised information and took essential steps in response to the breach; however, there was a loss in productivity from the loss of connectivity to organizations that are reliant on international contact with other stakeholders. It can also be assumed that the subsequent network clean-up efforts would impact users, hardware and substantial interaction with system administrators. Clearly the government was not ready for this scope and scale of attack, nor did it have adequate safe-guards in place to protect its networks from penetration or its users from exploitation. A case could likely be made that the 24 hour news cycle on this subject has long since expired and the vulnerability perceived by Canadian citizens resulting from this attack have likewise expired. Routine reminders about security vulnerabilities and mandatory security awareness training often fall on deaf ears of a saturated, disinterested audience. As George Santayana said, "Those who cannot remember the past are condemned to repeat it." A second example of note and greater complexity was Stuxnet, which was able to compromise the Iranian nuclear programme. Stuxnet was a worm designed to attack industrial control processors and inserted into the Iranian systems via USB thumb drive.[17] In 2010, it was successful in suppressing the Iranian Nuclear programme uranium enrichment centrifuges temporarily. Although there is very little official response from the Iranian government on the impacts to their programme, this is unlikely to be a lapse in security that they are likely to repeat. An apparently politically motivated operation to compromise or delay the Iranian Nuclear

[16] Greg Weston, "Foreign hackers attack Canadian government," *CBC News*, 16 February 2011.
[17] David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum,* 26 February 2013.

programme, the creation and release of the Stuxnet worm globally has permitted other would be hackers to reuse the code for other purposes according to Kaspersky Labs, a leading anti-virus company.[18] All too often forgotten, the second and third order effects of this activity are likely to create waves for other countries in the future as the evolution of tools used in cyberspace operations permeates other control systems. In examining the two examples of systems compromised by cyber operations, one domestic and the second international, the key difference to note is the level of impact that it had on the psyche of the nation. Consequently, the steps taken by the affected nations to change their procedures and culture of security will mitigate subsequent events. Now having seen the environment in which cyber operations occur and the potential consequences of security omissions, the next step will be to discuss the actions underway in Canada to improve our cyber security culture.

At first glance, Canada's scale of implementation for security initiatives pales in comparison to some of our allies in terms of financial commitment and personnel resources. However, it is worth noting that the cyber security and the culture to protect our cyber systems has been articulated in the pillars of Canada's Cyber Security Strategy and continual fine-tuning of the associated action plan.[19] Under the guidance of Public Safety, the three pillars of the Cyber Security Strategy consist of: securing government systems, partnering to secure vital cyber systems outside the federal Government and helping Canadians to be secure online. The government has developed a comprehensive action plan with an appropriate governance framework to ensure cyber integrity. The assembly of the relevant government institutions working alongside other levels of

---

[18] *Ibid.*
[19] Public Safety, *Canada's Cyber Security Strategy*, 9.

government in Canada, the private sector and individuals will continue to work together to protect this vital domain in a shared responsibility. However, the initial steps taken by the Government to articulate the strategy and indoctrinate the people needs additional attention to ensure that the need for cyber security is viewed as essential by the Canadian people. In other words, they feel as though they have a personal stake in the outcome rather than believing that it is the Government's problem. There are numerous tools assembled in the online forums under the Canadian Cyber Incident Response Centre publicly available to assist individuals and businesses establish their own cyber security plans.[20] However, in the absence of an attack against Canadian Values, or perhaps an Olympic hockey game with the gold medal on the line, Canadian citizens are unlikely to internalize the importance of cyber security. As such their respective individual lackadaisical attitudes towards cyber security will compound at their place of work and render Canadians unduly exposed in cyberspace. "Achieving the cyber integrity of Government requires that roles and responsibilities are clear, systems are strengthened and Government employees are aware of proper procedure."[21] Unless the security principles outlined in the strategy can be brought into action, our desired future becomes endangered. Cyber security is achievable, but now we must work for it and undergo a change of mindset to inculcate it in our culture.

> With each passing day, Canadians' dependence on cyberspace grows. There is no turning back to a world without an Internet. Just as previous generations took advantage of increasingly complex and helpful methods of communications, we have embraced the Internet.[22]

---

[20] Public Safety Canada, "Canadian Cyber Incident Response Centre," last modified 12 December 2014, http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx

[21] Public Safety, *Canada's Cyber Security Strategy*, 9.

[22] *Ibid*, 14.

Canadians enjoy relatively secure borders and peaceful existence in tumultuous times around the world. Economic prosperity and growth through advancements in a number of industries, social programmes and stable governance make Canada a desirable place to live in a free democratic society. Ensuring that we remain vibrant is contingent on continued advancements in the exchange of knowledge. The cyberspace gateway that allows Canadians one avenue to participate in the international community needs to be preserved, as prescribed for in customary international law and the UN Charter. The risks to business, communications and prosperity through malevolent cyber operations need to be understood and dealt with through legal means and proper user practice. The potential costs to reputation and reliability of a staunch ally when exposing other networks to threats due to complacency will likely have a limited window of tolerance. The loss of vital infrastructure as was perpetrated against the Iranian Nuclear programme could easily cripple a Western democracy, such as Canada. We all need to play a role in mitigating the risk of compromise to cyber operations. An ingrained responsibility of users to be alert and aware of potential risks will protect progress. There is no one particular technological solution that can be instituted to protect our systems from compromise; rather it is a collaborative effort. Success will depend on our ability to work together. Otherwise, we may find ourselves ill-prepared in the face of some other domestic or international crisis.

BIBLIOGRAPHY

Banerjee, Sidhartha. "Activists Using Social Media to Fight Jihadists." May 31, 2015. http://www.ctvnews.ca/canada/activists-using-social-media-to-fight-jihadists-1.2399470.

Bernier, Melanie, and Joanne Treurniet. "Understanding Cyber Operations in a Canadian Strategic Context: More than C4ISR, More than CNO." *Conference of Cyber Conflict Proceedings.* Tallinn: CCD COE Publications, 2010. 227-243.

Canada. Public Safety Canada. *Action Plan 2010-2015 for Canada's Cyber Security Strategy.* Ottawa: Public Safety Canada, 2013.

—. *Canada's Cyber Security Strategy.* Ottawa: Public Safety Canada, 2010.

Canada. Public Safety Canada. *Canadian Cyber Incident Response Centre.* December 12, 2014. http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx (accessed May 31, 2015).

Canadian Internet Registration Authority. *The Canadian Internet.* n.d. http://cira.ca/factbook/2014/the-canadian-internet.html (accessed 05 30, 2015).

Deibert, Don. *Cyber Security: Canada is Failing the World.* May 26, 2011. http://www.huffingtonpost.ca/2011/05/26/cyber-security-canada-stephen-harper-g8_n_867136.html (accessed May 30, 2015).

Hathaway, Oona A., et al. "The Law of Cyber-Attack." *California Law Review*, 2012: 817-885.

Kushner, David. "The Real Story of Stuxnet." *IEEE Spectrum.* February 26, 2013. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/ (accessed May 31, 2015).

Press, Jordan. *Canada's Military Squeezed out of cyber-defence, email warns.* Ottawa, March 12, 2014.

Schmitt, Michael N. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harvard International Law Journal*, 2012: 13-37.

United States. *International Strategy for Cyberspace: Prosperity, Security and Opennes in a Networked World.* Washington: The Whitehouse, 2011.

Weston, Greg. *Foreign Hackers Attack Canadian Government.* Toronto, February 16, 2011.