National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBERSECURITY: THE NEED FOR A ROBUST ENVIRONMENT AND MORE CAUTIOUS APPROACH TO THE PROCUREMENT AND SUSTAINMENT OF OUR CAPABILITIES

Major Dany Gonthier

JCSP 47

Service Paper

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 47

Étude militaire

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 47 - PCEMI 47
2020 - 2021

SERVICE PAPER – ÉTUDE MILITAIRE

CYBERSECURITY: THE NEED FOR A ROBUST ENVIRONMENT AND MORE CAUTIOUS APPROACH TO THE PROCUREMENT AND SUSTAINMENT OF OUR CAPABILITIES

Major Dany Gonthier

Word Count: 2,235

Nombre de mots : 2.235

CYBERSECURITY: THE NEED FOR A ROBUST ENVIRONMENT AND MORE CAUTIOUS APPROACH TO THE PROCUREMENT AND SUSTAINMENT OF OUR CAPABILITIES

AIM

1. This service paper argues that Canada should review both its procurement practices and policies as well as its industrial base to favour a more robust cybersecurity environment and sustainment of its technological capabilities, which leads to the recommendation that a Whole of Government (WoG) working group be established to ensure that current and future technology components are free of foreign influence or interference.

INTRODUCTION

2. The affordability of technology combined with the accessibility of the internet means that today almost all electronic devices are connected, one way or another, to each other through global networks. Given the fact that electronic devices have vulnerabilities, there is a real and pressing need to ensure that such vulnerabilities are either eliminated or mitigated which will, in turn, safeguard the Government of Canada (GoC), Department of National Defence (DND), and the Canadian Armed Forces (CAF) interests from our potential adversaries. Western military forces have become dependent upon technological superiority over peers and near-peers and our potential adversaries have aggressively advanced their cyber capabilities, which have allowed them to level the field, hence the need to find a solution.

3. The discussion portion of this service paper is divided into five sections. The first section highlights the fact that cyber attacks are on the rise. The second section briefly introduces the notion of cyberwarfare. The third section discusses the potential impacts of cyber attacks and cyberwarfare on western military forces. The fourth section illustrates that organizations are either not aware of or, when confronted with this reality, downplay the risks inherently present in cyberspace. The fifth and last section not only identifies the need to change our procurement practices and policies but also the fact that our industrial base should be reviewed in order to safeguard our technology from foreign influence or interference.

DISCUSSION

Cyber attacks are on the rise

4. The cyberspace has seen an important "increase of the frequency/number, intensity, duration and sophistication of cyber-attacks" at the international level, which is in line with the assessment that was performed on the North Atlantic Treaty Organization (NATO) networks.[1] State actors such as China have frequently attacked the United States

[1] Sorin D. Ducaru, "The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO," *Europolity*, Vol. 10, no. 1, 2016, 8.

(U.S.) and by breaching its cyber protections and firewalls, have caused damages that is catastrophic to the American national security.[2] Canada is no exception and the Canadian Security Intelligence Service (CSIS) has acknowledged that "cyber-espionage, cyber-sabotage, cyber-foreign-influence, and cyber-terrorism pose significant threats to Canada's national security, its interests, as well as its economic stability."[3] The fact that western military forces have become dependent upon technological superiority over peers and near-peers potential adversaries in the last decades is not about to reverse the trend of cyber attacks against our networks.

5. Both state and non-state actors have much to gain from an aggressive cyber posture and the development of cyber capabilities, and for many reasons. First, cyber attacks are an affordable solution to compete against technology prone western military forces, in particular when compared to a full-spectrum conflict that is not only costly, but that can bring military and civilian casualties. Second, cyberspace also offers the luxury of concealment given that the attribution of cyber attacks is difficult to prove and when suspicion goes towards a state, such actions are consistently refuted by the state's diplomatic officials on the world stage. Third, cyber capabilities are effective at deterring potential adversaries, given that one can pre-emptively neutralize vital communications or infrastructure systems, without firing a single shot on the battlefield.[4] Once again, cyber attacks offer the possibility of a strategic victory without the associated potential casualties

Cyberwarfare

6. The advancement of technology is changing the "character of war" and the fact that commercial firms are developing the latest technologies "means that state competitors and non-state actors will also have access to them, a fact that risks eroding the conventional overmatch to which our [U.S.] Nation has grown accustomed."[5] Cyberwarfare, which is the conduct of hostilities in cyberspace, "is less a way to achieve a winning advantage in battle than a means of covertly attacking the enemy's homeland infrastructure without first having to defeat its land, sea, and air forces in conventional military engagements."[6] It is expected that the next major conflict, with a potential adversary such as China, will see the integration of cyberwarfare in which cyber attacks will be a key component of its overall strategy.[7] The fact that today "virtually all digital and electronic military systems can be attacked via cyberspace" will continue to favour the use of cyberwarfare by our potential adversaries, which can have disastrous impacts

---

[2] Megan Manzano, "Cyberwarfare," Vol. First edition. New York: Greenhaven Publishing LLC, 2018, 19, last accessed on 17 Jan 2021, http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1681258&site=ehost-live&scope=site.

[3] Canada, Canadian Security Intelligence Service, "2019 Public Report," 2019, 18.

[4] Magnus Hjortdal, "China's Use of Cyber Warfare Espionage Meets Strategic Deterrence," *Journal of Strategic Security*; San Jose Vol. 4, Iss. 2, 2011, 14.

[5] United States, Department of Defense, "Summary of the 2018 National Defense Strategy of the United States of America," 2018, 3.

[6] John Arquilla, "Cyberwar is already upon us, but can it be controlled?," *Foreign Policy*, accessed on 27 Oct 2020, https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/.

[7] Nigel Inkster, "China's Cyber Power," Milton: Taylor & Francis Group, 2017, 148-149.

on western military forces.[8] China is preparing for a "war under informatization" and even though its current capabilities do not currently allow the country to conduct full-spectrum cyberwarfare, there is arguably not need to wait until the People's Liberation Army (PLA) achieves such a milestone.

Potential impacts of cyberwarfare and cyber attacks

7. Government and military forces alike are vulnerable to cyber attacks and the potential impacts could have long-lasting effects. For the government, the "destruction of financial data, records and transactions, forms of travel, communication means, and national power grid [would] create chaos and confusion resulting in psychological shock" of its citizens.[9] For a western military force that is prone to technology, "the more vulnerable it is to a potential cyber Pearl Harbor attack that will render its technological superiority over its adversary impotent."[10] State actors such as China have taken advantage of the opportunities that offer cyberspace to advance their technological progress which is now leveling the battleground, even with the world's most powerful military, the United States.

8. The U.S.-China Economic and Security Review Commission, which monitor, investigate, and submit an annual report to the U.S. Congress, has indicated that China has saved both time and money given its "large-scale, state-sponsored theft of intellectual property and proprietary information (…) to fill knowledge gaps in its domestic defense and commercial R&D."[11] For example, *Reuters* has reported a case where a Chinese businessman pleaded guilty of conspiracy for his role with the PLA Air Force in illegally accessing and stealing sensitive state of the art military information, in particular plans of strategic airlift platforms of the Globemaster III and advanced fighter jets such as F-22 Raptors and F-35 Lightning II.[12] China can now compete with the U.S. and western military forces with its own indigenous fifth-generation fighter jet, the J-31, which even though is a twin-engine aircraft, its "design bears a striking resemblance to the single-jet F-35."[13]

Organizations are not aware of the risks or downplay them

9. The U.S. Government Accountability Office reported that "[i]n operational testing, [Department of Defence] DOD routinely found mission-critical cyber

---

[8] Magnus Hjortdal, "China's Use of Cyber Warfare Espionage Meets Strategic Deterrence," *Journal of Strategic Security*; San Jose Vol. 4, Iss. 2, 2011, 5.

[9] Megan Manzano, "Cyberwarfare," Vol. First edition. New York: Greenhaven Publishing LLC, 2018, 25, last accessed on 17 Jan 2021, http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1681258&site=ehost-live&scope=site.

[10] *Ibid*.

[11] United States, U.S.-China Economic and Security Review Commission, "2014 Annual Report to Congress," 2014, 292.

[12] Dan Whitecomb, "Chinese man to serve U.S. prison term for military hacking, Reuters Aerospace and Defence," last updated on 13 July 2016, https://www.reuters.com/article/idUSKCN0ZT2RQ.

[13] Marcus Weisgerber, "China's Copycat Jet Raises Questions About F-35." *Defenceone*. 2015. https://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859/.

vulnerabilities in systems that were under development" and when program officials were confronted with these conclusions, they still "believed their systems were secure and discounted some test results as unrealistic."[14] Furthermore, the "DOD does not know the full scale of its weapon system vulnerabilities because, for a number of reasons, tests were limited in scope and sophistication."[15]

10. Canada is not immune to the phenomenon and Nortel, a former multinational telecommunications and data networking equipment manufacturer, is of particular importance given that a cybersecurity breach led to its bankruptcy in 2009. The attackers, who were traced back to China through their IP addresses, infiltrated the company as early as the year 2000 or perhaps earlier and "downloaded technical papers, research reports, business plans, employee emails and other documents from computers under their control."[16] The downfall of Nortel is that even though the breach was discovered in 2004, it was "constantly ignored by top executives."[17] The risks are real, the GoC, DND/CAF are targets of our potential adversaries and there is a need to recognize the fact that these entities are not immune to such cyber breaches.

The need to change procurement practices and policies

11. China, which is arguably one of our potential adversaries, already has in place a robust mechanism to avoid foreign influence or interference into its supply chain and the manufacturing of its technology, military, and civilian. The Chief Executive Officer of Samsung, even though based in South Korea, mentioned that a firm "cannot survive in China without becoming a Chinese company. That includes local technology development, product design, procurement, manufacturing and sales."[18] From a military perspective, the "PLA procurement regulations prohibit the acquisition of sensitive equipment from nongovernment companies."[19] One notable exception has been Huawei, which was authorized to "circumvent" such regulations given that it was "able to meet stringent military requirements over secrecy and other regulatory matters because of the former military backgrounds of its management," who were previously high-ranking officers in the PLA.[20] In a country where the government has a firm grip on businesses and where there are many of state-owned enterprises (SOEs) to choose from, China's procurement practices are protected from any foreign influence. No similar regulations exist in Canada and without SOEs to provide both the GoC and DND/CAF with the latest

---

[14] United States, United States Government Accountability Office, "Report to the Committee on Armed Services, U.S. Senate, Weapons Systems Cybersecurity: DOD Just Beginning to Grapple With Scale of Vulnerabilities," 2018, i.

[15] *Ibid*., 21.

[16] Canada, Canadian Security Intelligence Service, "The Security Dimensions of an Influential China: Highlights from the Conference," 2013, 118.

[17] *Ibid*.

[18] B.J. Lee, "Gotta be Chinese: To Profit in China, Companies have to Go Native from Design to Sales, Says a Top CEO Who has done it." *Newsweek*, 28 June 2004, 1, https://search-proquest-com.cfc.idm.oclc.org/magazines/gotta-be-chinese/docview/1832548082/se-2?accountid=9867.

[19] Tai Ming Cheung, "Fortifying China: The Struggle to Build a Modern Defense Economy," Ithaca: Cornell University Press, 2009, 216.

[20] *Ibid*.

technology, there is a pressing need to change our procurement practices and policies and review our industrial base.

12. There is a credible risk that malicious components are and will continue to be introduced into hardware, including in supply chains.[21] As such, "hardware security will increasingly be dependent on the ability to nullify the impact of malicious components, rather than assuming their absence."[22] The U.S. DOD is aware of the issue and has indicated that to maintain its technological advantage over its potential adversaries, it "will require changes to industry culture, investment sources, and protection across the National Security Innovation Base."[23] A solution will not be easily implemented given that the country "does not have a comprehensive policy of the tools to address this massive technology transfer to China" or even a "holistic view of how fast this technology transfer is occurring."[24]

13. The former CAF Chief of Defence Staff, General (retired) Vance is adamant that allowing China, through a SOE such as Huawei, to enter Canada's networks would be a mistake given that the company is a state tool, "which is entirely owned, operated and penetrated by the state."[25] Canada should not allow state involvement in its networks or its technology, given that this would facilitate state-sponsored activities such as cyber-espionage and open the door to cyber attacks. Similar to the situation in the U.S., a shift in culture needs to happen in Canada in order to protect the country against foreign influence and interference. To that effect, there is a need to change our procurement practices and policies and review our industrial base.

How to protect the GoC, DND/CAF?

14. The fear that China has implemented backdoors for espionage, for instance in equipment manufactured by Huawei, is not unfounded and accordingly many countries have now begun to block the company from competing on government contracts given that the People's Republic of China (PRC) could use critical data for military and economic gain.[26] The first steps to safeguard Canada's national interest are: to understand the magnitude of the issue, to ensure that the risks are known and that all the impacts are assessed. Once all these steps are completed, adjustments will be required to our procurement practices and policies. Furthermore, the industrial base has to be thoroughly reviewed and the inclusion of safeguards is key. More specifically, "[s]afeguards should

---

[21] Yossi Oren, "Focus falls on manufacturers to defend against supply chain attacks," *Jane's Intelligence Review*, 12 November 2018.

[22] *Ibid*.

[23] United States, Department of Defense, "Summary of the 2018 National Defense Strategy of the United States of America," 2018, 3.

[24] Gabriel Dominguez, "US lagging behind China in key dual-use technologies, says US DoD official," *Jane's Update*, 31 October 2019.

[25] Robert Fife, "Gen. Vance calls for grand strategy to confront China and Russia," *The Globe and Mail*, 11 January 2021.

[26] Matt Thomas, "The Weaponization of Chinese Telecoms Companies," in *NATO at 70 Years: Selected Topics in World Security*, NATO Association of Canada, 2019, 53-54, http://natoassociation.ca/wp-content/uploads/2019/04/NATO-at-70-Selected-Topics-in-World-Security.pdf.

include measures to deter firms from embedding malware in products, to clarify the source of content in electronics, to support electronics producers in friendly countries, and to prohibit critical sectors from buying electronics with content from China."[27] *Canada's Defence Policy - Strong, Secure, Engaged* calls for the establishment of a "Cyber Mission Assurance Program" that will "protect critical military networks and equipment" in incorporating "cyber security requirements into the procurement process."[28] A protected supply chain is a step in the right direction for DND/CAF but there is a need to develop an over-arching strategy in a WoG approach to protect all departments. Furthermore, the Cyber Mission Assurance Program should be fast-tracked given the potential consequences of foreign influence and interference into our technology on which western military forces, including Canada, have become dependent.

CONCLUSION

15. Cyber attacks are on the rise and the impacts can have disastrous effects on western military forces and governments alike. Cyberwarfare is a concept that has not been ignored by our potential adversaries and future conflicts will see the employment of such tactics, at a level that is still hard to predict. Organizations are either not aware of the risks from cyber attacks or the use of cyberwarfare or, when confronted with the reality, just downplay them, which is beneficial to our potential adversaries. There is consequently a need for the GoC to change its procurement practices and policies and to thoroughly review its industrial base to ensure that there is no foreign influence or interference in all of our technologies, military and civilian. It is the only way to ensure both a more robust cybersecurity environment and the safe sustainment of Canada's technological capabilities, now and for the future.

RECOMMENDATION

16. It is recommended that a WoG working group be established to review both GoC procurement practices and policies as well as a review of its industrial base to ensure that all components of current and future technology can properly be traced back to the source and origin, which will guarantee that our technology is free of foreign influence or interference. More specifically, the working group should be led by the Privy Council Office with senior representatives from the DND/CAF (Assistant Deputy Minister (Materiel) (ADM(Mat) and ADM (Information Management) (ADM(IM), Canadian Forces Intelligence Command (CFINTCOM)), Shared Services Canada (SSC), Public Services and Procurement Canada (PSPC), Communications Security Establishment (CSE), Global Affairs Canada (GAC), and Canadian Security Intelligence Service (CSIS).

---

[27] Ryan Neuhard, "Flawed by Design: Electronics with Pre-Installed Malware," *Georgetown Security Studies Review*, Georgetown University Center for Security Studies, 2018, last accessed on 20 Jan 2021, https://georgetownsecuritystudiesreview.org/2018/05/23/flawed-by-design-electronics-with-pre-installed-malware/.

[28] Canada, Department of National Defence, "Canada's Defence Policy: Strong, Secure, Engaged," 2017, 73.

BIBLIOGRAPHY

Arquilla, John. “Cyberwar is already upon us, but can it be controlled?” *Foreign Policy*. https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/.

Bae, Sebastien J. “Cyber Warfare: Chinese and Russian Lessons for US Cyber Doctrine.” Georgetown University Center for Security Studies. 2015. https://georgetownsecuritystudiesreview.org/2015/05/07/cyber-warfare-chinese-and-russian-lessons-for-us-cyber-doctrine/.

Canada. Canadian Security Intelligence Service. 2019 Public Report. 2019

Canada. Canadian Security Intelligence Service. The Security Dimensions of an Influential China: Highlights from the Conference. 2013.

Canada. Department of National Defence. Canada’s Defence Policy: Strong, Secure, Engaged. 2017.

Canada. Department of National Defence. Pan-Domain Force Employment Concept: Prevailing in an Uncertain World. 2020.

Canada. Department of National Defence. The Future Security Environment 2013-2040. Ottawa: Chief of Force Development. 2014.

Cheung, Tai, Ming. “Fortifying China: The Struggle to Build a Modern Defense Economy.” Ithaca: Cornell University Press. 2009.

Dominguez, Gabriel. “Jane’s Update: US lagging behind China in key dual-use technologies, says US DoD official.” 2019.

Ducaru, Sorin, D. “The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO.” *Europolity*. Vol. 10, no. 1, 2016.

Groll, Elias. “Many U.S. Weapons Systems Are Vulnerable to Cyberattack.” *Foreign Policy.* 2018.

Hjortdal, Magnus. “China's Use of Cyber Warfare Espionage Meets Strategic Deterrence.” *Journal of Strategic Security*; San Jose Vol. 4, Iss. 2, 2011.

Inkster, Nigel. “China's Cyber Power.” Milton: Taylor & Francis Group. 2017.

Lee, B. J. "Gotta be Chinese." *Newsweek,* 28 June 2004. https://search-proquest-com.cfc.idm.oclc.org/magazines/gotta-be-chinese/docview/214272134/se-2?accountid=9867.

Manzano, Megan. “Cyberwarfare.” Vol. First edition. New York: Greenhaven Publishing LLC. 2018. http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1681258&site=ehost-live&scope=site.

Neuhard, Ryan. “Flawed by Design: Electronics with Pre-Installed Malware.” Georgetown Security Studies Review. Georgetown University Center for Security Studies. 2018. https://georgetownsecuritystudiesreview.org/2018/05/23/flawed-by-design-electronics-with-pre-installed-malware/.

Oren, Yossi. “Focus falls on manufacturers to defend against supply chain attacks.” Jane’s Intelligence Review. 2018.

Robertson, Jordan and Michael Riley. "The Big Hack." *Bloomberg Businessweek* no. 4587. 2018. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=132145450&site=ehost-live&scope=site.

Segal, Adam. “When China Rules the Web Technology in Service of the State.” *Foreign Affairs*. Vol. 97 Issue 5. 2018.

Shoebridge, Michael. “How to deal with the increasing risk of doing business with China.” *The Strategist*, Australian Strategic Policy Institute. 2020. https://www.aspistrategist.org.au/how-to-deal-with-the-increasing-risk-of-doing-business-with-china/.

Thomas, Matt. “The Weaponization of Chinese Telecoms Companies.” In NATO at 70 Years: Selected Topics in World Security, NATO Association of Canada. 2019. http://natoassociation.ca/wp-content/uploads/2019/04/NATO-at-70-Selected-Topics-in-World-Security.pdf.

United States. Department of Defense. Summary of the 2018 National Defense Strategy of the United States of America. 2018.

United States. United States Congress. U.S.-China Economic and Security Review Commission, 2014 Annual Report to Congress. 2014.

United States. United States Government Accountability Office. Report to the Committee on Armed Services: Weapons Systems Cybersecurity: DOD Just Beginning to Grapple With Scale of Vulnerabilities. 2018.

Weisgerber, Marcus. “China's Copycat Jet Raises Questions About F-35.” *Defenceone*. 2015. https://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859/.