National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

NO LONGER FIREPROOF: CANADA'S NATIONAL SECURITY IN THE CYBERWARFARE AGE

Lieutenant-Colonel Christopher L. Jackson

JCSP 45

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

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
2018 – 2020

SOLO FLIGHT

NO LONGER FIREPROOF: CANADA'S NATIONAL SECURITY IN THE CYBERWARFARE AGE

Lieutenant-Colonel Christopher L. Jackson

No Longer Fireproof: Canada's National Security in the Cyberwarfare Age

In 1927, Raoul Dandurand, a Canadian senator, said that Canada was "a fireproof house, far from the sources of conflagration." The long-time politician was noting Canada's distance from Europe and that continent's history of conflict helped protect our nation. The events of 9/11 demonstrated that North America was no longer exempt from the impact of a spillover of violence.[1] While the advent of intercontinental ballistic missiles and long-range bombers started the trend of testing our fireproof nature[2], the arrival of the internet and the subsequent interconnectivity of our nation's critical infrastructure (i.e. banks, electrical and gas networks, telecommunications, etc.) has demonstrated that this threat is now at our respective doorsteps. As such, Canada needs to evolve how it views national defence, and therefore, who is best placed to protect our nation.

Canada's defence vision is to "provide Canada with an agile, multi-purpose combat-ready military, operated by highly trained, well-equipped women and men, secure in the knowledge that they have the full support of their government and their fellow Canadians."[3] Along with this vision of the Canadian Armed Forces (CAF) their mission of defence is defined as:

- **Strong at home**, its sovereignty well-defended by a CAF also ready to assist in times of natural disaster, other emergencies, and search and rescue;
- **Secure in North America**, active in a renewed defence partnership in NORAD and with the United States;

[1] Scott White, Canada Confronts Openness / safety paradox, https://globalpublicsquare.blogs.cnn.com/2014/10/26/canada-confronts-the-opennesssafety-paradox/comment-page-1/ accessed 5 March 2020.
[2] Gwynne Dyer, Canada in the Great Power Game, Random House, 2014, p. 264
[3] Department of National Defence Strong, Secure, Engaged: Canada's Defence Policy https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html?utm_source=dgpaapp&utm_medium=referral&utm_campaign=redirect

- **Engaged in the world**, with the CAF doing its part in Canada's contributions to a more stable, peaceful world, including through peace support operations and peacekeeping.[4]

The CAF has recognized that "Increasingly, threats, such as global terrorism and those in the cyber domain, transcend national borders".[5] Canada will "assume a more assertive posture in the cyber domain by hardening our defences, and conducting active cyber operations against potential adversaries in the context of government-authorized military missions".[6] My question is why should the Department of National Defence (DND) undertake this role when we already have niche areas of responsibility that no other government department can undertake? Secondly, of what use to the Canadian Government is an offensive cyber programme? What stately goals would such a programme accomplish and what is the Government's vision of an offensive cyber campaign? None of these questions are adequately defined, nor discussed in the various open source DND documents.

The Government of Canada believes that a safe and secure cyber space is important for the security, stability and prosperity of the country. Digital technologies and the internet are increasingly important for innovation and economic growth, and good cyber security is critical to Canada's competitiveness, economic stability, and long-term prosperity[7]. However, one can argue that DND should not play a leading role in offensive cyber operations for the fact that it is costly to develop a CAF capability, the return on investment is not sustainable to the defence

[4] Department of National Defence Strong, Secure, Engaged: Canada's Defence Policy https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html?utm_source=dgpaapp&utm_medium=referral&utm_campaign=redirect
[5] Department of National Defence Strong, Secure, Engaged: Canada's Defence Policy https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html?utm_source=dgpaapp&utm_medium=referral&utm_campaign=redirect
[6] Department of National Defence Strong, Secure, Engaged: Canada's Defence Policy https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html?utm_source=dgpaapp&utm_medium=referral&utm_campaign=redirect
[7] Communication Security Establishment, Backgrounder Canadian Centre for Cyber Security, 16 October 2018, https://www.cse-cst.gc.ca/en/backgrounder-fiche-information

budget and the political appetite is not currently present. Certainly, the Canadian military has been discussing the role that it can play in this realm as it is undoubtedly important for Canada's national security. Nevertheless, I would argue that the cost, both financial and personnel, to establish an efficient programme (one that does not merely pay lip service to this role) perhaps should be part of a larger Government of Canada (Canadian Security Intelligence Service (CSIS), Communication Security Establishment (CSE), and the Royal Canadian Mounted Police (RCMP)) mandate in protecting the Nation. Therefore, while DND can participate in active cyber defence and support Canadian cyber operations, it is not the department to which the government should assign these responsibilities.

WHAT IS CYBER WARFARE?

Before we examine what role DND should undertake in cyber warfare, it is important to define what we are discussing. Cyber warfare involves "the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks."[8] Cyber operations are defined as "cyberspace operations (CO) which is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[9] Some of the more known cyber attacks have occurred with the assistance of a nation's security and intelligence services. The first known offensive cyber operation, Stuxnet, "was launched in circa 2009 and came to light in roughly 2010. Stuxnet was a computer worm

[8] RAND Corporation, Cyber Warfare, https://www.rand.org/topics/cyber-warfare.html
[9] Department of Defence, Cyberspace Operations, 8 June 2018, Vii,

aimed at Iran's nuclear facilities and it appeared to have been created by the U.S. National Security Agency, the CIA, and Israeli intelligence."[10]

While this attack damaged thousands of Iranian centrifuges what are the actual consequences of a cyber attack? Some pundits have suggested that cyberwarfare can do little short-term damage. Certain countries, such as Iran, "have a proven history of using cyberattacks against financial systems, oil companies and infrastructure."[11] While there is some evidence that the United States has "refrained from using cyberattacks for fears of starting a larger scale conflict, there is no publicly available evidence that CO have successfully deterred physical attacks."[12]

Given the military parity in Europe between NATO and Russia, the Russians have "increasingly relied on fake news, cyber attacks, and subversion to undermine opponents with threats that are hard to counter."[13] So the question remains, does the Canadian military need to undertake these types of cyber operations or should it focus on the physical defence of our nation while other agencies, working in cooperation, concentrate on the defensive aspects of cyber warfare?

WHAT ARE OUR ADVESARIES DOING?

If we examine what the Chinese People's Liberation Army (PLA) is doing in the cyberwarfare realm it can provide us with insight into the most powerful and integrated enemy

[10] McCaffee, What is STUXNET https://www.mcafee.com/enterprise/en-ca/security-awareness/ransomware/what-is-stuxnet.html
[11] Jackie Schneider, "Iran can use cyberattacks against the U.S. That's not nearly as bad as it sounds" in The Washington Post, 27 February 2020.
[12] Jackie Schneider, "Iran can use cyberattacks against the U.S. That's not nearly as bad as it sounds" in The Washington Post, 27 February 2020
[13] Dominic Nicholls, "Britain should focus more on Russian cyber attacks and fake news than major conflict" in The Telegraph, 9 February 2020

that we face as a nation.[14] The PLA has noted that cyber operations are part of their traditional electronic warfare operations. China has noted that they will conduct cyber operations for five reasons:

- To strengthen political and economic control in China;
- To complement forms of intelligence collection,
- To reconnoitre and gather targeting information in foreign networks for later exploitation,
- To conduct the exploitation using collected information, and
- To develop defence in China's own cyber systems.[15]

To complete the above noted objectives, the PRC has delegated the responsibilities to various departments within the state. The intelligence services (Ministry of State Security (MSS) and Ministry of Public Security (MPS)) have undertaken the roles of strengthening (maintaining) the political and economic control in China. The 3rd Department of the PLA (Signals Intelligence) and the MSS have "cooperated on developing access to the second objective while the remaining three objectives are the primary responsibility of the 3rd Department of the PLA with assistance from the rest of the state apparatus".[16] As we can see from the above, there is an offensive nature given to the various elements of the Chinese security and defence apparatus that is not apparent in Canadian literature. These above cited goals of the Chinese leadership mean that the PRC has viewed the world through a vastly different lens than the West. Since the founding of the PRC in 1949, the PRC's leadership has "been driven to catch up with the West in economic, political and

[14] A cautionary note from the author. While we will review what the PLA does it should be noted that their organization is highly integrated as a controlled state and economy and our democratic institutions may not be able to operate in the same manner.
[15] Larry Wortzel, "Chinese People's Liberation Army and Information Warfare" *Strategic Studies Institute, US Army War College, March 2014* .pg 17

[16] Ibid, pg 25

military terms."[17] In 2015, the Chinese white paper on China's Military Strategy stated that "it is a Chinese dream to make the country strong…without a strong military, a country can neither be safe nor strong.[18]" The PRC has noted that its "five foreign policy objectives are: fostering economic development, reassurances, countering constraints, diversifying access to natural resources and reducing Taiwan's international space."[19] Therefore, the PRC is driven to carve out a larger space for themselves on the international stage. These actions are something that the GoC is not prepared to do via deceptive or aggressive means, including cyber espionage or cyber-attacks to meet our national goals.

While the PRC is attempting to assert their influence on the world stage, the Russians are attempting to maintain their posture as a competitor to the United States and NATO. Academics have noted that since the fall of the Soviet Union in 1991, the Russian Federation has continued to develop their capabilities and reliance upon hybrid warfare. The Russians have understood that by using hybrid warfare they have diminished direct conventional force actions instead use a wide range of hostile actions, such as cyber warfare or the use of propaganda. Recently, Russia's hybrid warfare campaigns "have increasingly relied on cyber warfare as a geopolitical tool to exert influence on other countries."[20] The Russians have been omnipresent in their global activities. Perhaps the most daring was the Russian state's use of the private Internet Research Agency, which interfered in the United States 2016 presidential election. It was noted that the "Russian effort included the weaponization of stolen cyber information, the use of Russia's English-language state media as a strategic messaging platform, and the mobilization of social

[17] Dean Cheng, "The PRC and Intelligence Gathering: Unconventional Targets and Unconventional Methods," Testimony before Committee on Judiciary, U.S. Senate, 12 December 2018.
[18] Defense Intelligence Agency, China. Military Power. 2019, pg. V
[19] Evan S Medeiros, China's Foreign Policy Objectives, RAND Corporation, 2009, pg. 45.
[20] Leo-Paul Jacob, An Exploration into the Growth of Russian Cyber Warfare, NATO Association of Canada, 25 March 2017 http://natoassociation.ca/russias-cyber-warfare/

media bots and trolls to spread disinformation and amplify Russian's messaging."[21] Again, the activities of the Russian state are not congruent with how the Canadian public views how our nation operates on the international stage.

WHO DOES WHAT IN CANADA?

Based on the offensive nature of the state cyber threats to our nation what are the various elements of the Canadian government mandated to accomplish for Canada?

The Communications Security Establishment (CSE) has the following mandate:

- to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;

- to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada;
- to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.[22]

In 2019, the Government passed a new law, with the coming into force of Bill C-59 (*National Security Act, 2017*), which gave CSE the ability to conduct defensive and "active" cyber operations. Active operations are defined as anything that could "degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security."[23]

---

[21] Bill Priestap, Assessing Russian Activities and Intentions in Recent Elections, Statement Before the Senate Select Committee on Intelligence, 21 June 2017, https://www.fbi.gov/news/testimony/assessing-russian-activities-and-intentions-in-recent-elections

[22] Communication Security Establishment - What we do. https://www.cse-cst.gc.ca/en/inside-interieur/what-nos

[23] Howard Solomon, "Canada should think again about having the ability to use offensive cyber weapons: Expert" in ITWORLDCANADA, 12 June 2019, https://www.itworldcanada.com/article/canada-should-think-again-about-having-the-ability-to-use-offensive-cyber-weapons-expert/418912

In 2017, the Canadian Security Intelligence Service (CSIS) was given the ability to conduct Threat Reduction Measures.[24] This means that threats to national security (e.g. promulgated by the PRC's CO) "are fast, complex and dynamic, and threat actors are highly connected and mobile. There is a unique role for CSIS to play in reducing threats, which offers the Government of Canada another important tool to respond to threat activity".[25]

While there are numerous articles on the role that the RCMP can play in the cyber realm they focus solely on the investigation of criminal activities stemming from cyber-attacks. In 2018, the Federal budget provided funding to the RCMP to create the National Cybercrime Coordination Unit which allowed the force to expand its cyber investigations.[26] It does not, however, provide the RCMP with a mandate to conduct offensive cyber operations.

WHAT SHOULD CANADA DO?

When reviewing the national literature on cyber operations most of the publicly available information discusses mainly defensive cyber operations and therefore some of these suggestions may already be in force.

[24] Bill C-59 stresses that threat reduction powers must comply with the Charter, and it provides a closed list of what those powers are: altering or disruption communications and goods, fabricating documents, disrupting financial transactions, impersonating persons, and interfering with persons' movements. This approach allows the government to argue that threat reduction powers are prescribed by law and are a reasonable and justified limit on Charter rights. See Craig Forcese in « L'évaluation du projet de loi antiterroriste C-59 par deux experts de renom : beaucoup de progrès, et quelques améliorations à apporter encore.", in Policy Options, 22 June 2017, https://policyoptions.irpp.org/fr/magazines/juin-2017/a-report-card-on-the-national-security-bill/

[25] Government of Canada, Amendments to the CSIS Act – Threat Reduction Measures, 20 June 2017, https://www.canada.ca/en/security-intelligence-service/news/2017/06/amendments_to_thecsisact-threatreductionmeasures.html. Note that in 2019 the TRM section was further modified to ensure that operations were compliant with the Canadian Charter to Rights.

[26] Thomas Juneau, et al, ed. Canadian Defence Policy in Theory and Practice, Springer Nature, 2020 p, 407

It is evident that Canada cannot ignore the cyber domain to conduct offensive operations. That said, how much should we spend on this activity and is the military the force of choice to conduct them? At this juncture, the state of the Armed Forces is in jeopardy. The Commander of the Canadian Army has, in recent months, indicated that his forces are stretched to the limit with ongoing deployments to Europe and preparations for aide to the civil powers in Canada.[27] This same argument was raised in 2016, when there was debate over the developing role of an offensive cyber capability.[28] Furthermore, DND documents from 2012 also raised questions as to whether the Armed Forces have the necessary funds to properly train and conduct offensive cyber operations. The military will never receive the necessary funds to run offensive cyber operations, so why would we want to divert soldiers away from their above-noted missions to conduct offensive cyber operations? Perhaps, a more cost beneficial solution would be the use of contracts, akin to Private Military Companies (PMC or PMSC), who are operating in the various conflict zones. Contracting out offensive cyber operations is not a new concept; authors have been talking about this for several years. In 2016, Isaac Porche of the Rand Corporation commented that "the masterminds behind many notorious cyberattacks …are America's youth."[29] Porche goes on to comment that "private-sector businesses are inherently able to better react to changes in the market for cyber talent because they can go after the talent they need by paying more and giving better benefits."[30]Therefore, why not establish a contract with Canadian cyber companies to be the offensive cyber capability for the Government? It would allow

[27] Lee Berthiaume," Disaster relief a threat to the Canadian army's fighting edge, commander says" in The National Post, 20 January 2020.
[28] Murray Brewster, "Former CSIS head says Canada should have its own cyber-warriors", CBC, 22 June 2016, https://www.cbc.ca/news/politics/military-cyber-wars-fadden-1.3648214
[29] Isaac Porche, "The Military Should Increase Efforts to Find and Enlist Young Hackers", RAND Corporation, 10 March 2016.
[30] Isaac Porche, "The Military Should Increase Efforts to Find and Enlist Young Hackers", RAND Corporation, 10 March 2016.

Canada to craft its own offensive cyber capabilities while limiting the impact upon the traditional forms of military power.

In the new security environment, "private military and security companies have developed as important actors in the security sector."[31] With the current security environment where phishing and other cyber scams are rampant on the internet, cyber experts have started to help the government protect our national infrastructure. A volunteer recruitment effort led by the SecDev Group is calling "on IT pros to lend a hand by providing preventative measures to thwart attackers. The group is also asking for assistance from volunteers who can offer remedial services that help organizations recover from cyber-attacks."[32] It would not be a difficult stretch to put a request for this type of assistance to corporate Canada to create a group of computer experts to deploy offensive cyber operations for Canada. As NATO pointed out in 2017, "(s)pending on human capital – in terms of recruitment, retention, training and education, appears to be key to getting results. Therefore, targeting of spending is necessary – especially now that the global hunt for talent means that the private sector can easily lure away highly skilled and knowledgeable experts."[33] As such, why should Canada invest in building its own cyber attack specialists within DND when we are risking losing these individuals to the private sector? Why not just hire properly vetted private sector employees to undertake these types of offensive cyber actions if we need them.

---

[31] Warner, Daniel. "Establishing Norms for Private Military and Security Companies." *Denver Journal of International Law & Policy* 40, no. 1-3, p, 109

[32] Sarah Coble, Canadian Volunteers to form civil defence brigade, https://www.infosecurity-magazine.com/news/canadian-volunteers-cyber-defense/ 25 March 2020.

[33] Neil Robinson, "Spending for success on cyber defence", in NATO Review, 6 April 2017, https://www.nato.int/docu/review/articles/2017/04/06/spending-for-success-on-cyber-defence/index.html

As noted in academic publications from the United States, military authors are also pushing private-public partnerships to ensure that they maintain primacy in the cyber world. In an opinion piece for the Modern War Institute, Colonel T Schmidt noted that "our adversaries have foraged through and stolen our intellectual property for decades unhindered…the United States must leverage (an) … unprecedented level of public-private partnership between government and industry"[34]. The major sticking point would be to what end? Why does Canada need to conduct these types of operations? I believe that with our current lack of advanced military hardware and personnel to fulfill our current mandated requirements, any diversion of funds to offensive operations would be a waste of our precious resources.

Much of the national debate over what Canada should do in the cyber realm is focused on how to protect our infrastructure from foreign or criminal assault.[35] As the above passages note, it is expensive and difficult to mount the infrastructure and resources, both in terms of personnel and money, to create an efficient offensive cyber capability. Therefore, the question remains, do the various federal governments want this capability? I would suggest that the public debate, or lack there of, over the issue of an offensive intelligence organization proves that we do not. One clear example is commentary that "we (Canadians) are a shy diffident people who would prefer to be neither shaken nor stirred."[36] The same piece notes that "Canada does not collect foreign intelligence on the capabilities, intentions, and activities of foreign actors (states or individuals) and is used to help Canada understand what is happening on the world stage, what it means to

[34] Colonel T Schmidt, "The Missing Domain of War: Achieving Cognitive Overmatch on Tomorrow's Battlefield", 7 April 2020 in Modern War Institute.
[35] Derek Burney, et al, Braver Canada: Shaping our destiny in a precarious world. McGill-Queen's Press, 2020, preface.
[36] Phil Gurski, "What do you mean Canada does not have a foreign intelligence service?" in The Hill Times, 26 November 2018. https://www.hilltimes.com/2018/11/26/mean-canada-not-foreign-intelligence-service/177178

Canada, and how we can make better decisions and policies based on that intelligence."[37] I would suggest that if Canada has not created a foreign intelligence service to help protect Canada and reinforce our economic place in the world, the idea of conducting offensive cyber operations to thwart the same foreign powers from doing us harm is even less close to realization.

I would also argue that CSE and CSIS, who currently have the legislative mandates to conduct such operations, are perhaps better suited to assist DND with any offensive cyber operational requirements. This is due to their appropriate legislation. It is clearly difficult for the military to obtain authorization for such operations within its current construct without having to table a Bill in Parliament. The various legislations that have come into force for national security (C-51, C-59 etc.) have all mentioned elements of cyber operations but none specifically focused on DND. In our current political landscape, pushing for specific legislation to authorize DND to conduct such operations is likely not feasible.

[37] Ibid,

CONCLUSION

Cyberattacks are not likely to have devastating short-term consequences but they can gradually erode the foundations of social, political and economic stability over time.[38] While there is a requirement for the Canadian government to invest in its capability to defend critical infrastructure from cyber attacks, the necessity for offensive cyber operations, is likely limited in the Canadian context. That said, should there be a need to conduct offensive cyber operations the government can call upon various elements of the national security infrastructure (specifically CSE and CSIS) to conduct these operations on behalf of the government. If there is a need to have a standing capability to conduct cyber operations, then the government should look at working with corporate Canada to contract out this capability and therefore minimize the impact to those agencies already stretched thin. A standing capability means that the GoC has identified a sustained requirement to conduct offensive cyber operations (which is doubtful at this juncture) or simply a stand-by force where contractors could play an important role.

Even before the advent of the financial burden of combating COVID-19, the ability of corporate Canada to undertake these operations (with the proper oversight) is a more cost efficient and punctual need to use sparingly. With the billions of dollars of debt incurred to combat the COVID-19 virus, there will be precious few dollars available to DND to undertake bespoke offensive cyber operations. As such, a political and financially savvy government will need to stay abreast of developments in the private sector in this regard as well as joining forces with like minded allies to pool resources and technologies to fight our common foes. The ability to pool resources and tactics for conducting efficient offensive cyber operations is something that

[38] Jackie Schneider, "Iran can use cyberattacks against the U.S. That's not nearly as bad as it sounds" in The Washington Post, 27 February 2020

the Canadian government will need to explore with its partners, particularly with traditional close allies across the 5 Eyes or the French. In a resource stretched government, collaboration will be key to developing this necessary capability while being good stewards of the public purse.

In conclusion, I believe that the fundamental question that remains unanswered with respect to Canada's role in cyber operations is, do we really need to conduct them? As noted above, there is an absence of discussion in publicly available literature regarding a necessity for Canada to undertake such operations. At present, the focus is solidly on defensive posturing. Therefore, there is little point in arguing for a role for DND to conduct these operations if the government has yet to define how these operations will advance Canada's national interests. It will be interesting to see how this question is answered by the politicians across the political spectrum in the next decade as they work to protect our country.

BIBLIOGRAPHY

United States of America. (September 2018). *National Cyber Strategy of the United States of America.*

Ayers, C. (2018). *Rethinking soverignty in the context of cyberspace.* December 2018: US Army War College.

Berthiaume, L. (2020, January 20). *Disaster relief a threat to the Canadian army's fighting edge*. Retrieved from The National Post.

Brewster, M. (2016, June 22). *Former CSIS head says Canada should have its own cyber-warriors*. Retrieved from CBC: https://www.cbc.ca/news/politics/military-cyber-wars-fadden-1.3648214

Canada, P. S. (2018). *National Cyber Security Strategy.* Ottawa: Her Majesty the Queen in Right of Canada.

Cheng, D. (2018). The PRC and Intelligence Gathering: Unconventional Targets and Unconvential Methods. *US Senate Committe on the Judiciary.* Washington: Library of Congress.

Counter-Terrorism, I. I. (n.d.). *IS-Supporting Hacktivists in Southeast Asia.*

Defence Intelligence Agency. (2019). *China. Military Power.*

Defence, D. o. (2014). *The Future Security Environment 2013-2040.* Winnipeg: Her Majesty the Queen, in right of Canada.

Dyer, G. (2014). *Canada and the Great Power Game.* Toronto: Random House.

Forcese, C. (2017, June 22). *L'evaluation du projet de loi antiterroriste c-59 par deux experts de renom: beaucoup de progres, et quelques ameliorations a apporter encore.* Retrieved from Policy Options: https://policyoptions.irpp.org/fr/magazines/juin-2017/a-report-card-on-the-national-security-bill/

Group, S. I. (2018, November 20). *Ansar Cyber Army claims hacking of CCTV following calls from UCC.* Retrieved from siteintelgroup.com.

Gurski, P. (2018, November 26). *What do you mean Canada does not have a foreign intelligence service.* Retrieved from The Hill Times: https://www.hilltimes.com/2018/11/26/mean-canada-not-foreign-intelligence-service/177178

Keir Giles, K. H. (n.d.). Cyber Defense: An international view. *US Army War College*.

Michael Padgett, J. K. (July 12, 2018). Increasing Economic Power as an Instrument of National Power. *Real Clear Defense*.

Nicholls, D. (2020, February 9). *Britain should focus more on Russian cyber attacks and fake news than major conflict.* Retrieved from The Telegraph.

Office of the Secretary of Defense. (May 16, 2018). *Military and Security Developments Involving the People's Republic of China 2018.* Washington: Secretary of Defense.

Porche, I. (2016, March 10). *The Military Should Increase Efforts to Find and Enlist Young Hackers*. Retrieved from The Rand Corporation.

Pugliese, D. (2020, 01 28). New batch of machine guns for Canadian military to be delivered in December. *Ottawa Citizen*.

Robinson, N. (2017, April 6). *Spending for success on cyber defence*. Retrieved from NATO Review: https://www.nato.int/docu/review/articles/2017/04/06/spending-for-success-on-cyber-defence/index.html

Schneider, J. (2020, February 27). *Iran can use cyberattack against the U.S. That's not nearly as bad as it sounds*. Retrieved from The Washington Post.

Smotherman, J. (August 2016). Justified Physical Response to Cyber Attacks. *Army War College Review*, 43-53.

Staff, J. C. (2018, June 8). *Cyberspace Operations*. Retrieved from Joint Chiefs of Staff, Government of the United States of America: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150

Thomas Juneau, e. a. (2020). *Canadian Defence Policy in Theory and Practice.* Switzerland: Springer Nature.

White, S. (2014, 10 26). Retrieved from Cable News Network: https://globalpublicsquare.blogs.cnn.com/2014/10/26/canada-confronts-the-opennesssafety-paradox/comment-page-1/

Wortzel, L. (March 2014). Chinese People's Liberation Army and Information Warfare. *Strategic Studies Institute, US Army War College*.