National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

RUSSIAN MENACE : IS THE CANADIAN GOVERNMENT CAPABLE OF COUNTERING RUSSIAN DISINFORMATION?

Major Timothy Caines

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*

RUSSIAN MENACE: IS THE CANADIAN GOVERNMENT CAPABLE OF COUNTERING RUSSIAN DISINFORMATION?

By Major Timothy Caines

RUSSIAN MENACE: IS THE CANADIAN GOVERNMENT CAPABLE OF COUNTERING RUSSIAN DISINFORMATION?

A 2019 report by the Communications Security Establishment (CSE), *2019 Update: Cyber threats to Canada's Democratic Process,* describes the likelihood that foreign adversaries will undertake actions to undermine the Canadian democratic processes, particularly during the upcoming October 2019 Federal Election.[1] Although the report does not indicate the likelihood of election interference, the CSE report highlights that Canadians are susceptible to foreign influence due to their large amount of internet usage with at least 74% of Canadians averaging 3 to 4 hours online per day.[2] Canadian allies such as the United Kingdom (UK) and United States (US) have been subject to actions by foreign adversaries to undermine democratic processes. Russian interference in the United States 2016 Presidential Election resulted in the indictment of 13 Russian nationals and three Russian companies for creating disinformation to influence the election outcome.[3] During the 2016 Brexit referendum on the UK's membership in the European Union (EU), an analysis of tweets by the "Vote to Leave" side showed strategically placed Twitter accounts that generated hyper-partisan information that was quickly shared and polarized support to leave the EU.[4] Canada is a crucial contributor to several international organizations such as the G7, the G20, United Nations, and the North Atlantic Treaty Organization (NATO), which allows Canada to influence

---

[1]Canada, Communications Security Establishment, *2019 Update: Cyber threats to Canada's Democratic Process,* (Ottawa: Communications Security Establishment, 2019), 9.
[2]*Ibid.,* 10.
[3]Brennan Weiss, "A Russian Troll Factory had a $1.25 million monthly budget to interfere in the 2016 US election," *Business Insider*, Accessed April 3rd, 2019, https://www.businessinsider.com/russian-troll-farm-spent-millions-on-election-interference-2018-2
[4]Canada, Canadian Security Intelligence Service, "Who Said What? The Security Challenges of Modern Disinformation," (Ottawa: Canadian Security Intelligence Service, February 2018), 53-58.

international trade, aid, diplomatic engagements, and military decisions. Given that Canada is a well-positioned global influencer, with a population well connected to the internet, Canada provides an opportunity for foreign adversaries to target Canadian democratic processes. Russia, based on involvement in Brexit and US elections, may use information operations during the October 2019 Canadian Federal Election to undermine and change Canada's reputations and relations domestically and internationally.[5]

Canadian military doctrine defines information operations as "actions taken in support of national objectives which influence decision makers by affect other's information while exploiting and protecting one's own information."[6] By comparison, the Russian Ministry of Defence defines information operations as the ability to "undermine political, economic, and social systems, carry out mass psychological campaigns against the population of a state in order to destabilize society and governments."[7] While Canada's objective is to influence decisions makers, Russia's objective is to destabilize governments and states by influencing populations.

Russian information operations use disinformation to disseminate "carefully constructed and false messages into the communication system of a target group to deceive decision making elites or public opinion."[8] Disinformation techniques to spread false news stories to create doubt in order to influence Canadian political and military interest have already begun. Early in the Canadian deployment to Latvia as part of Op REASSURANCE in 2017, Russian websites published photos of disgraced former

---

[5]Canada, Communications Security Establishment, *2019 Update: Cyber threats to Canada's Democratic Process,* (Ottawa: Communications Security Establishment, 2019), 9.
[6]Canada, Department of National Defence, B-GG-005-004/AF-010, *CF Information Operations,* (Ottawa: Canadian Warfare Center, 1998), 1-6.
[7]T. S. Allen and A. J. Moore, "Victory without Casualties: Russia's Information Operations," *US War College Quarterly* 48*,* no.1 (Spring 2018), 60.
[8]Martin Kragh and Sebastian Asberg, "Russia's Strategy for influence through public diplomacy and active measures: the Swedish case," *Journal of Strategic Studies* 40, No. 6 (2017), 778.

Canadian Colonel Russell Williams suggesting the "Canadian military is full of homosexuals and shouldn't be counted on by Latvians."[9] Disinformation targeted prominent Canadian politicians such as Foreign Affairs Minister Chrystia Freeland. In 2017, Russian websites attacked Freeland indicating her grandfather was Nazi collaborator. In response to an article alleging Russian responsibility published in *The Globe and Mail,* the Russian Embassy in Ottawa denied any involvement but pointedly stated that Freeland did not directly deny allegations about her grandfather.[10] In response, Freeland acknowledged efforts by Russia to de-stabilize Western states such as Germany and the United States. Minister Freeland stated, "I think that Canadians and indeed other western countries should be prepared for similar efforts to be directed at them."[11] Both examples demonstrate the type of information operations undertaken by Russia directed at undermining the credibility of the Canadian government, through the use of disinformation. While Freeland's comments warn Canadians to remain on guard, the Canadian government's approach to countering Russian disinformation has been less than clear. This paper will analyze the Canadian government's approach to countering Russian information operations against Canadian national and international interests and assess whether or not the Canadian government response to Russian disinformation requires changes to reduce real and potential impacts to Canadian domestic and international interests.

---

[9]Chris Brown, "Anti- Canada Propaganda greets troops in Latvia," Accessed April 3rd, 2019, https://www.cbc.ca/news/world/latvia-propaganda-1.4162612

[10]Robert Fife, "Freeland warns Canadians to be aware of Russian disinformation," *The Globe and Mail*, Accessed April 3rd, 2019, https://www.theglobeandmail.com/news/politics/freeland-warns-canadians-to-beware-of-russian-disinformation/article34227707/

[11]*Ibid.,*

Soviet, and later Russian, espionage and influence activities, both directed by and via Western communist parties, has long been a concern of the Canadian government. During the Cold War, the 1945 defection of Russian cipher clerk Igor Gouzenko revealed the complexity of Soviet espionage networks in Canada and the United States. The Canadian government appointed a Royal Commission to review the Gouzenko disclosures under Conservative justices of the Supreme Court, Roy Kellock and Robert Taschereau. The Commission's report became an 'overnight sensation' that triggered spy hunts in the US and UK.[12] In Canada, Gouzenko wrote about his exposure stating it was "odds and ends of a big and threatening pattern designed to bring this Canada, this United States, this democracy under Soviet domination."[13] Canada's focus on Soviet influence continued when in1969, the Canadian Report of the Royal Commission on Security identified Russian subversion and espionage as a threat to Canada. According to Canadian political scientist, Reg Whitaker, the report highlighted that "communism was a subversive ideology in the services of limitless Soviet expansionism."[14] Although the report received unfavorable scrutiny in the media and Canadian Parliament which reduced its overall impact politically, the continued references to subversion and espionage activities by the Soviet Union in Canada continued to highlight the concern of Soviet communist influence within Canada throughout the Cold War.[15]

With the Cold War ending in the early 1990s, there was a prevalent view that Russia's role in the world as a military power was over.[16] This view precipitates the

---

[12]Laurence Hannat, "Igor Gouzenko and Canada's Cold War." *The Beaver* 75, no. 5 (10, 1995): 20.
[13]*Ibid.,* 20.
[14]Reg Whitaker, "The Politics of Security Intelligence Policy-making in Canada: I 1970-84," *Intelligence and National Security* 6, no. 4 (October 1991): 653.
[15]*Ibid.,* 654.
[16]Bettina Renz, "Russia's Military Revival," (Cambridge: Polity Press, 2018), 4.

notion that Russian interest in Western states such as Canada would decrease. However, this has not been the case as demonstrated by Russian influence activities in the American 2016 elections and the Brexit vote in the UK. In addition, there has been an increase in Russian power projection worldwide since 2014 with the annexation of Crimea and more recently Russian support of the Syrian regime. Russia's involvement in Syria and Ukraine are an effort to increase Russia's geopolitical leverage with the West.[17] Successes in both regions have surprised the West despite ample notice over twenty years that Russia re-emergence due to Western provocation was likely. [18]

In March 2019 speech General Valery Gerasimov, the Chief of the General Staff for the Russian military attributed recent success in Syria by Russian forces to the use of information operations and a small expeditionary force, which he felt should be expanded

---

[17]Emil Aslan Souleimanov and Valery Dzutsati, "Russia's Syria War: A Strategic Trap?," *Middle East Policy* 25, no. 2 (June 2018): 44.

[18]Russia's re-emergence as a military power should not surprise the West. In some aspects, Russia never left as a military power and worked with the West despite several irritants. Since the 1990s, actions by the West have been viewed by Russia as a challenge to Russia's historical power base. NATO countries such as Germany raised concerns (Baun, 2005) as early as 1993 that NATO expansion would antagonize Russia. Bettina Renz (Russia's Military Revival) discusses the impact of Operational ALLIED FORCE, the NATO action in Kosovo in 1999 where Russia felt that the US expected Russia to fall in line with the new international hierarchy post-Cold War even though it was against one of Russia's traditional Allies. A 2012 speech, (Putin, 2012) summarizes Russia's concerns with the West during a meeting with Russian ambassadors and international organizations that Western powers are undertaking unilateral actions not bound by international law. In the speech, Russian President Putin explains how Russia will help restore the balance of power with the West. In 2013 (Putin, 2013), during a meeting with former Ukraine President Yanukovych, Putin highlights close historical ties with Ukraine including language and trade while Ukraine was deciding on further integration with the EU. The reasons for the 2014 invasion of Ukraine (Bukkvoll, 2016) are the idea Ukraine/Russians are the same people, the Euromaidan uprisings represented West strategies to use economic, political, and social means to create uprisings against regimes it did not like. Further, Russia's strategy of using information operations as part of overt public diplomacy (Kragh and Asberg, 2017) within Western countries such as Sweden increased after 2014. Russia's goal was to create the perception that the Ukraine invasion was justified and Western actions toward Russia were unjust. As a result, Russia was compelled to act after 20 years of Western deception. Finally, (Adamsky, 2018) argues current Russian deterrence strategy has synchronize effects of nuclear, information, non-nuclear as part of Russian cultural identity as a form of coercion without full-scale war under next-generation warfare as seen in Ukraine.

to advance national interests.[19] Russia's ability to utilize social media such as Facebook, with 2.32 billion active users, provides a large international audience to demonstrate military strength, power and success, which is projected to ordinary citizens.[20] Russia's utilization of social media transcends national borders providing real-time influence throughout the world.

In some regards, Russia has adopted the strategies of Western states who have strived to integrate information operations with traditional military activities.[21] NATO indicates that information operations "aim is to influence adversary decision-making processes, thereby preventing them from taking the initiative."[22] Within Syria, for instance, Russian interests centre on protecting Syrian President Bashar al-Assad while resisting Western pressure for a Syrian regime change, allowing Russia to demonstrate power at home and abroad.[23] Russia's successful integration of information operations with military forces in Syria influenced attitudes and perceptions of Western States enabling freedom of movement in the operational information environment.[24] Russia is using information operations to gain geopolitical advantage.

---

[19]Andrew E. Kramer, "Russian General Pitches 'Information' Operations as a Form of War," *The New York Times*, Accessed April 3rd, 2019, https://www.nytimes.com/2019/03/02/world/europe/russia-hybrid-war-gerasimov.html

[20]"Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2018," *Statista,* Accessed April 10th, 2019,https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[21]Mike Eckel, "Russia's Shock And Awe: Moscow Ups Its Information Warfare In Syria Operation," *Radio Free Europe Documents and Publications*, Washington, 07 October 2015, 1.

[22]Paul A.L. Ducheine, "Non-kinetic capabilities: Complementing the Kinetic Prevalence to Targeting," in *Targeting: The Challenges of Modern Warfare*, edited by Paul A.L. Ducheine, Michael N. Schmitt, and Frans P. B. Osinga, (The Hague: Springer, 2016), 213.

[23]Jason Ralph and Jess Gifkins, "The purpose of United Nations Security Council practice: Contesting competence claims in the normative context created by the Responsibility to Protect," *European Journal of International Relations* 23, no. 3 (2017): 644.

[24]Paul A.L. Ducheine, "Non-kinetic capabilities: Complementing the Kinetic Prevalence to Targeting," in *Targeting: The Challenges of Modern Warfare*, edited by Paul A.L. Ducheine, Michael N. Schmitt, and Frans P. B. Osinga, (The Hague: Springer, 2016), 213.

NATO was caught off guard by Russia's change of strategy during Russia's 2014 invasion of Crimea. Using unidentified Russian troops and information operations, Russia quickly annexed the Ukrainian territory. A few months after the operations, NATO's supreme commander, General Philip Breedlove, called the annexation the "the most amazing information-warfare blitzkrieg we have seen in the history of information warfare."[25] NATO refers to this Russian strategy as hybrid warfare. NATO defines hybrid warfare as "the use of propaganda, deception, sabotage and other non-military tactics to destabilize adversaries ….by exploiting technological change and global interconnectivity."[26] Information operations are a component of hybrid warfare. Within hybrid warfare, information operations exploit digital media that is cheap, simple to produce and distribute, manipulate, allows the aggressor to control the message.[27] Russia's ability to synchronize information operations with military force and cheap technology furthers concerns of renewed Russian ambitions.

One major challenge that the Canadian government faces with Russian information operations is Canada's requirement for secrecy. Although Minister Freeland alluded to the need for Canadians to be ready for disinformation activities, the Canadian government will need to balance secrecy against security. For Western democracies such as Canada, "secrecy fits awkwardly into the accountability of open democracies; and intelligence has now become more secret again." Also, the requirement of secrecy limits the use of open source material to understand all steps being taken by the Canadian

---

[25]Mike Eckel, "Russia's Shock And Awe: Moscow Ups Its Information Warfare In Syria Operation," *Radio Free Europe Documents and Publications*, Washington, 07 October 2015, 2.
[26]North Atlantic Treaty Organization, "NATO's Response to Hybrid Threats," Accessed April 3rd, 2019, https://www.nato.int/cps/en/natohq/topics_156338.htm.
[27]Frans P. B. Osinga and Mark P. Roorda, "From Douhet to Drones, Air Warfare, and the Evolution of Targeting," in *Targeting: The Challenges of Modern Warfare*, edited by Paul A.L. Ducheine, Michael N. Schmitt, and Frans P. B. Osinga, (The Hague: Springer, 2016), 67.

government to counter Russian disinformation. If the Canadian government provides too much information to maintain transparency on Canadian actions to limit Russian disinformation, the Canadian government risks undermining intelligence sources and Canada's ability to respond to threats against the country covertly. Given the requirements for Western democratic societies to be accountable to its citizenry and institutions, Russia can easily use disinformation to exploit the requirement for transparency against the need for secrecy and security in many western countries, including Canada.

Russia is mastering the ability to use the idea of lawfare to exploit the rule of law. Lawfare, defined as the "strategy of using or misusing law as a substitute for traditional military means to achieve an operational objective."[28] Russia's approach with lawfare is to undermine Western states propensity for following the rule of law by using the strength of democracy against it. One goal of lawfare is "to destroy an opponent's will to fight by undermining public support."[29] Russia successfully used lawfare during the annexation of Crimea even though the 1994 Budapest Memorandum between Russia, Ukraine, the US, and the UK agreed to Ukraine's independence and international borders. During the annexation, Russia argued that "the loss of Ukraine's territorial integrity has resulted from complicated internal processes, which Russia and its obligations under the Budapest Memorandum have nothing to do with."[30] Russia's statement creates

---

[28]Paul A.L. Ducheine, "Non-kinetic capabilities: Complementing the Kinetic Prevalence to Targeting," in *Targeting: The Challenges of Modern Warfare*, edited by Paul A.L. Ducheine, Michael N. Schmitt, and Frans P. B. Osinga, (The Hague: Springer, 2016), 216.
[29]*Ibid.,* 217.
[30]Sacha Dov Bachmann and Andres B Munoz Mosquera, "Lawfare and hybrid warfare – how Russia is using the law as a weapon," Accessed April 20th, 2019, https://www.researchgate.net/publication/320027113_Lawfare_and_hybrid_warfare_-_how_Russia_is_using_the_law_as_a_weapon

uncertainty and implies that Russia was within its rights to annex Crimea during internal struggles within Ukraine.

Russia's use of lawfare to exploit and influence Canadian public support and undermine Canadian democracy is a challenging problem for the Canadian government. A fundamental principle of Canadian Armed Forces (CAF) Public Affairs doctrine is "openness, accountability, and transparency" which appears to be the approach of the Canadian government for Russian disinformation.[31] The effectiveness of an open and transparent approach is challenging for governments such as Canada who must balance secrecy against security. Despite this balance, Canada has taken steps to reduce Russia's disinformation and influence on Canadian society. Evaluation of three steps taken by the Canadian government will occur in the next section.

Since January 2019, the Canadian government has raised concerns that potential Russian interference in the October 2019 Federal Election is growing. The 2019 report by CSE identifies Russia's internet research agency as a prominent organization creating malicious websites and spreading disinformation across multiple social media platforms.[32] Wesley Wark, a Canadian security expert, states that "Canadian governments are known not to spread political fears especially in the national security realm."[33] During March 2019 House of Commons testimony by the outgoing Privy Council Clerk, Michael Wernick, raises concerns about the likelihood and impact of election interference in the

---

[31]Canada, Department of National Defence, Joint Doctrine Manual, *Joint Public Affairs 2017-05,* (Ottawa: Strategic Joint Staff Public Affairs, 2017), 1-4.
[32]Canada, Communications Security Establishment, "2019 Update: Cyber threats to Canada's Democratic Process," (Ottawa: Communications Security Establishment, 2019), 22.
[33]Wesley Wark, "Michael Wernick's Alarmist Words are the Politics of Fear," *The Globe and Mail*, Accessed April 15th, 2019, https://www.theglobeandmail.com/opinion/article-michael-wernicks-alarmist-words-are-the-politics-of-fear/

October 2019 election.[34] Wernick's concerns and the CSE report, indicate the seriousness of the Russian threat on election interference. In response, the Canadian government has created Security and Intelligence Threats to Elections (SITE) Task Force from multiple security agencies. The role of the SITE Task Force is to assist the government to respond to and assess foreign threats against all political parties and elections administrators.[35]

While the success of this Task Force is unknown at this time, its creation is indicative of the severity of the threat to Russian interference poses to the election. Even though created as a warning system, the Task Force's ability to deter Russian interference based upon conventional deterrence theory is difficult. Within cyberspace, deterrence is difficult since it is challenging to "address global reach, anonymity, distributed and interconnected nature of this domain."[36] Canada's approach with the SITE Task Force as warning systems focuses the response as deterrence by defence vice offensive actions. Deterrence by defence means Canada will overtly dissuade Russian disinformation, identify Russian organizations that are undertaking disinformation, and inform Canadians on the threats posed by Russia to the election process.[37] While the success of the Task Force in defending against election interference will not be known until after the election, weaknesses do remain with its approach.

Primarily, despite establishing a Task Force comprised of multi-security agencies, the Canadian government also created a Critical Election Incident Public Protocol, which is led by a group of government appointees. This group includes the Clerk of the Privy

---

[34]*Ibid.* ,
[35]Canada, Communications Security Establishment, "2019 Update: Cyber threats to Canada's Democratic Process," (Ottawa: Communications Security Establishment, 2019), 23.
[36]Maria Rosario Taddeo, "How to deter in Cyberspace," (Helsinki: Hybrid Center of Excellence, June-July 2018), 2.
[37]Elizabeth Baron-Bodine, Todd C. Helmus, Andrew Radin, and Elina Treyger, "Countering Russian Social Media Influence," (Santa Monica: RAND Corporation, 2018), 21-22.

Council, National Security Advisor, and Deputy Ministers from Global Affairs, Justice, and Public Safety.[38] Although the cross-organizational dynamic demonstrates a whole-of-government approach that should improve inter-department cooperation and information sharing, organizationally there is no one person or organization responsible for monitoring election interference or accountable to elected officials. Neither the SITE Task Force nor Critical Election Incident Public Protocol Group addresses any further facets of Russian disinformation outside of the 2019 election. In reality, the Canadian government's response focuses on Russia's ability to influence democratic institutions during elections and not the overall intent of the Russian campaign, which is "to match multiple instruments of power of against the specific weaknesses of the society targeted."[39] By not creating a permanent organization or body to counter Russian disinformation outside of elections, the Canadian government fails to demonstrate a complete understanding of the Russian threat and influence.

A second area that the Canadian government has focused on in response to Russian disinformation is through the amendment of Canadian legal frameworks to increase security agencies' strength to respond to and prevent cyber threats. The cyber realm exploitation generally occurs through "espionage, attack, or data manipulation."[40] The Canadian government introduced Bill C-59 in 2017 to grant new powers to CSE to counter cyber threats, which is awaiting royal assent. New powers under the bill include "explicit authority to launch cyber-attacks — including the ability to disrupt or influence .

---

[38]Amanda Connolly, "No Worries About Wernick's Role on Election Alert Panel, Despite Calls for him to Resign: Gould," *National Online Journalist (Politics) Global News*, Accessed April 15th, 2019, https://globalnews.ca/news/5035336/karina-gould-michael-wernick-snc-lavalin-affair/

[39]Patrick Cullen, "Hybrid Threats as the New 'Wicked Problem' for Early Warning." (Helsinki: Hybrid Center of Excellence, May 2018), 4.

[40]Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue. "Addressing Hybrid Threats." (Stockholm: Swedish Defence University, 2018), 54.

. . intentions or activities of a foreign individual, state, organization or terrorist group."[41] According to the Minister of National Defence Harjit Sajjan, the new mandate within this framework enables Canada to evolve "to the various threats. And I think Canadians expect us to use every tool necessary, but we do it in the right legal framework."[42] Updating legislation to increase the power of CSE provides the opportunity to deter and limit Russian information operations.

Critics of the new legislation believe Bill C-59 could "normalize state sponsoring hacking and information operations."[43] The idea of deterrence by retaliation may increase the risk of escalation. For example, the use of Stutnex in 2010, a software bug meant to disrupt centrifuges on Iranian nuclear reactors, led to escalation when it 'escaped' and attacked internet systems of several countries throughout the world.[44] Stutnex highlights the challenges of operating in cyberspace where directed software bugs or attacks may have unintended consequences for several different countries. Also, despite Sajjan's intention to use legal means, deterrence by defence in cyberspace is difficult. Systems vulnerabilities with information technology and the time to identify and prevent threats within cyberspace are exploitable by adversaries such as Russia. The complexity of the cyber realm provides the most significant advantage to the attacker vice the defender.[45]

Opponents of Bill C-59 argue that Canadians' privacy will be at risk due to the transnational nature of information and technology. Canadian's information may be

---

[41]Alex Boutilier, "Sajjan Defends Proposed New Spy Powers to Conduct 'Information' Warfare," *The Toronto Star*, Accessed April 8th, 2019, https://www.thestar.com/news/canada/2018/01/11/sajjan-defends-proposed-new-spy-powers-to-conduct-information-warfare.html
[42]*Ibid.,*
[43]*Ibid.,*
[44]Maria Rosario Taddeo, "How to deter in Cyberspace," (Helsinki: Hybrid Center of Excellence, June-July 2018), 3-4.
[45]*Ibid.,* 3.

collected even if Canadian law stipulates foreign entities are the targets.[46] These are legitimate concerns that the Canadian government is proactively attempting to regulate national security agencies to reduce these concerns. For example, in 2017 Bill C-22 created the National Security and Intelligence Committee consisting of a group of non-partisan Parliamentarians to oversee national security and intelligence operations across the Canadian government.[47] However, organizations such as the International Civil Liberties Monitoring Group (ICLMG) raise concerns about the reach of security organizations.[48] While critics such as the ICLMG provide alternative views and criticizes steps taken Canada to address Russian disinformation, ICLMG criticisms may also provide an opening for Russia's disinformation. Within Sweden for instance, evidence indicates that Russia routinely exploits organizations on the far left and far right of the Swedish government to influence Swedish public perception on an issue.[49]

Despite these criticisms, the Canadian government's introduction of Bill C59 should set the conditions for the evolving theory of cyber deterrence that includes "target identification, retaliation, and demonstration."[50] CSE may not deter the initial attack, however, identification of the source of attack could allow for retaliation and deter any future attacks.[51] CSE's role with Bill C-59 will shift significantly. CSE will no longer only be responsible for defending Canadian information infrastructure. The provision of

---

[46] Monique Scotti, "Here's what you need to know about Canada's 'extraordinarily permissive' new spying laws," *National Online Journalist (Politics) Global News*, Accessed April 15th, 2019, https://globalnews.ca/news/3999947/cse-c59-new-spy-powers-canada/

[47]"Bill C-22 passes in House of Commons," *The Canadian Press,* Accessed April 15th, 2019, https://www.huffingtonpost.ca/2017/04/04/bill-c-22-passes-in-house_n_15813744.html

[48]Tim McSorley, "Bill C-22: Liberals Undermining Goal of Strong National Security Oversight," Accessed on April 15th, 2019, https://www.huffingtonpost.ca/tim-mcsorley/liberals-bill-c-22_b_15695114.html

[49]Martin Kragh and Sebastian Asberg, "Russia's Strategy for influence through public diplomacy and active measures: the Swedish case," *Journal of Strategic Studies* 40, No. 6 (2017), 801-802.

[50]Maria Rosario Taddeo, "How to deter in Cyberspace," (Helsinki: Hybrid Center of Excellence, June-July 2018), 5.

[51]*Ibid.,* 5-6.

offensive cyber capabilities increases the power of CSE provides an initial deterrence to Russian disinformation.

A third area in which Canada has proactively attempted to dissuade Russian disinformation operations is through the use of economic sanctions.
Annually, since March 2014, successive Canadian governments have used the *Special Economic Measures Act* to enforce sanctions against Russia for continued aggression in Ukraine. The sanctions include freezing assets of individuals or organizations and preventing any Canadian domestically or internationally from dealing with any Russian organization or individual sanctioned.[52] As a whole, these sanctions are "politically motivated denial or normal economic relations with the intent of changing behaviours."[53] There are two competing arguments on whether sanctions are successful in coercing change. Supporters believe that sanctions damage the wealth of those targeted and will lead to a change in behaviour. While opponents believe that sanctions are ineffective and hard to implement as a tool of foreign policy.[54] The challenge with understanding the impact of sanctions is difficult and requires some historical analysis to determine the full impact.

While the real impact of Canada's sanctions on Russia will not be known for some time, Russia has shown concerns with the passage of Canadian legislation in May 2017. The *Magnitsky Act* expands Canada's "international sanctions law to target gross human

---

[52]Canada, Global Affairs Canada, "Canadian Sanctions Related to Russia," Accessed April 15th, 2019, https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/Russia-Russie.aspx?lang=eng
[53]Gary M. Shiffman, "Economic Security," Chap. 15 in *Contemporary Security Studies*, 3rd, edited by Alan Collins, (New York: Oxford University Press, 2013), 213.
[54]Geigeun Shin, Seung-Whan Choi, and Shali Luo, "Do Economic Sanctions Impair Target Economies?," *International Political Science Review* 34, no. 4(2016), 485-486.

rights violators."[55] The legislation named after a Russian lawyer and auditor Sergei Magnitsky, who uncovered significant tax fraud with individuals with close ties to the Kremlin, and then after being arrested died under mysterious circumstances.[56] After Russia's invasion of Ukraine, the law also provided a template for President Barack Obama's administration not to target the entire Russian economy, but on individuals "known to be closely connected to Putin or directly responsible for his policy in Ukraine."[57] By targeting organizations and individuals, Canada is attempting to limit the overall impact on the Russian people. However, studies indicate that economic sanctions on Russia are having a minimal impact on Russia's overall gross domestic product (GDP) as 90% of the decline in GDP is attributable to fluctuating oil prices, while 10% is due to economic sanctions.[58]

The overall impact of economic sanctions may do little to dissuade Russian disinformation activities directly, however, the response to the Canadian Governments *Magnitsky Act*, indicates otherwise. The Russian Congress of Canada lobbied against the legislation stating "everybody realizes that some organizations are being used as a proxy

---

[55]Mike Blanchfield, "Canada Backs Recommendation for Magnitsky Act Targeting Human Rights Violators," *The Toronto Star*, Accessed April 15th, 2019, https://www.thestar.com/news/canada/2017/05/17/canada-backs-recommendation-for-magnitsky-act-targeting-human-rights-violators.html

[56]Alex Horton, "The Magnitsky Act, Explained," *The Washington Post*, Accessed April 15th, 2019, https://www.washingtonpost.com/news/the-fix/wp/2017/07/14/the-magnitsky-act-explained/?utm_term=.aef24170580f

[57]Anne Applebaum, "Russia is furious. That means the sanctions are working," *The Washington Post*, Accessed April 15th, 2019, https://www.washingtonpost.com/opinions/global-opinions/russia-is-furious-that-means-the-sanctions-are-working/2017/10/27/2b8f63dc-bb33-11e7-a908-a3470754bbb9_story.html?utm_term=.e51c9c66b275

[58]Iikka Korhonen, Heli Simola and Laura Solanko, "Sanctions, counter-sanctions and Russia − Effects on economy, trade and finance," (Helsinki: Bank of Finland- Institute for Economies in Transition, 2018), 10.

for Putin."[59] The President of the Russian Congress in Canada denies working on behalf of the Kremlin, and insists that the group represents Russian speaking Canadians "tired of the increase in anti-Russian campaigns."[60] The use of proxy groups to promote agendas in an attempt to influence political within another country is nothing new. Despite denials, groups such as the Russian Congress of Canada share views similar to the Russian government making them favourable tools of disinformation since their views align politically.[61] Given that all Canadian federal parties support the Magnitsky Act, the group had very little political influence. The most substantial influence of the Russian Congress of Canada was furthering Russia's agenda that the West, including Canada, is anti-Russia and that Russia is not the aggressor in the disinformation domain.

Politicians from Canada's major political parties acknowledge the increasing propensity of Russian disinformation targeting Canada. The creation of bi-partisan SITE Task Forces of national security agencies and civil servants is a positive step in addressing Russian election interference. With the approval of Bill C-59, national security organizations, such as CSE, will increase focus on cyber deterrence including target identification, retaliation, and responsiveness vice losing the initiative to Russia by remaining on the defensive by protecting infrastructure while waiting for a cyber-incident to occur. Finally, economic sanctions imposed because of Russian activities within Ukraine have not severely hampered the Russian economy. However, the passage of the *Magnitsky Act* increases the legal tools available to reprimand individuals and

---

[59]Dan Levin and Jo Becker, "Canadian Lawmakers say Pro-Russia Group Tried to Derail Sanctions Law," *The New York Times*, Accessed April 8th, 2019, https://www.nytimes.com/2017/10/04/world/canada/russiamagnitsky.html?partner=bloomberg

[60]*Ibid.,*

[61]Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue. "Addressing Hybrid Threats." (Stockholm: Swedish Defence University, 2018), 58.

organizations with close ties to the Kremlin. Despite these positive steps, Canada's approach to Russian disinformation remains fractured along with many competing activities within a government focused on the 2019 Federal Election. Additional steps by the Canadian government are required to address Russian disinformation in the long term. The following section includes four recommendations to improve the Canadian government's response to Russian disinformation.

The first recommendation is for Canada to institutionalize the SITE Task Force and create a whole-of-government approach to dealing with Russian disinformation. In the current configuration, the SITE appears to only focus on the October 2019 Canadian Federal Election. Marcus Kolga, a Senior Fellow at the Macdonald-Laurier Institute, calls for the creation of a Communications and Democracy Strategy of key ministries meant to "safeguard Canadian democracy against manipulation by disinformation, foreign intelligence active measures, cyber-attacks, and influence campaigns."[62] This organization would be holistic and responsible for tasks such as monitoring and detecting influence while also increasing literacy on Russian disinformation.[63] Kolga does not define the organization's management within a legislative or government framework, however, including it within the Public Safety portfolio to allow for coordination with other national security entities is a consideration. This approach would not be different from other Allies who are dealing with Russian disinformation.

The UK, for instance, already has a whole-of-government approach. Initially, the UK attempted to address national security threats through the use of an emergency council called COBRA (Cabinet Room Briefing Room A). Attendance at COBRA is

---

[62]Marcus Kolga, "Stemming the Virus: Understanding and Responding to the Threat of Russian Disinformation," (Ottawa: Macdonald-Laurier Institute, 2019), 40.
[63]*Ibid.,* 40-42.

threat dependent, however, there is some risk that the right stakeholders from the government are not present during an incident.[64] Canada has a similar structure to COBRA with the Security and Intelligence Assessment Center within the Privy Council Office which is responsible for coordinating national security committee meetings with the National Security Advisor.[65] Due to the risk and complexity of cyber threats, the UK also established a National Cyber Security Centre that unites different sectors of government and engages with industry to counter cyber threats.[66] Canada's solution is currently the SITE Task Force without a long term national strategy to deal with Russian disinformation after October 2019 Federal Election. A centralized organization within Canada should, similar, to the UK, coordinate the government's response and resources to Russian disinformation.

A second recommendation for the Canadian government to improve its response to Russian disinformation is to work with international partners to establish conventional norms for cyber usage. However, this will be difficult. Russia has successfully used lawfare to its strategic advantage. Within the NATO treaty, for instance, Article 5 guarantees collective security only when there is an armed attack. Russian disinformation does not meet the threshold and does not constitute an armed attack capable of garnering a comprehensive response from the Alliance.[67] For Russian disinformation to meet the threshold of an armed attack, Canada and its Allies must find international legal means to

---

[64]Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue. "Addressing Hybrid Threats." (Stockholm: Swedish Defence University, 2018), 80-81.
[65]Canada, Department of National Defence, Canadian Forces Joint Publication, *Intelligence,* (Ottawa: Canadian Forces Joint Warfare Center, 2011), 1-3.
[66]Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue. "Addressing Hybrid Threats." (Stockholm: Swedish Defence University, 2018), 82.
[67]Aurel Sari, "Blurred Lines: Hybrid Threats and the Politics of International Law," (Helsinki: Hybrid Center of Excellence, January 2018), 3.

provide the ability to confront Russian disinformation.[68] In reality, this means there must be a willingness to securitize information so that acts of aggression constitute an attack.

Although it may be difficult for Canada to establish international norms, Russia has previously attempted to establish a non-interference agreement with the US to prevent meddling in each other's domestic politics. Russia also pushed for an International Code of Conduct for Information Security with China to regulate the flow of information from the West across Russian borders. Western countries such as the United States stymied the Russian initiatives viewed as an attempt to limit the promotion of democratic values and reduce freedom of expression.[69] In April 2019, Russia passed legislation that can cut off internet access from foreign servers and limit influence from foreign actors. Essentially Russia is taking proactive steps to counter Western disinformation unilaterally.[70]

If Russia is unwilling to pursue multilateral international agreements on the use of cyberspace and limiting influence activities, Canada must work with Allies within NATO, the European Union (EU), and Five Eyes Partners, to change the international community's response. To do this, organizations such as NATO must re-think how it responds to threats, including cyber aggression, to create a comprehensive strategy to counter Russia's behaviour.[71] Sharing of tools and information amongst like-minded nations is already underway in the EU where a Cyber Diplomacy Toolbox is available to

---

[68]*Ibid.,* 6.
[69]Elizabeth Baron-Bodine, Todd C. Helmus, Andrew Radin, and Elina Treyger, "Countering Russian Social Media Influence," (Santa Monica: RAND Corporation, 2018), 28.
[70]"Russia passes bill to allow internet to be cut off from foreign servers," *The Guardian,* Accessed April 16th, 2019, https://www.theguardian.com/world/2019/apr/11/russia-passes-bill-internet-cut-off-foreign-servers
[71]Heine Sorensen and Dorthe Bach Nyemann, "Going Beyond Resilience: A Revitalized Approach to Countering Hybrid Threats," (Helsinki: Hybrid Center of Excellence, November 2018), 6.

measure aggression in cyberspace and track behaviour and capabilities of adversaries.[72] Also, the EU has implemented a General Data Protection Regulation to improve the privacy of EU citizens and reshape the way organizations protect information.[73] Independently, Canada may lack the political influence to change Russian behavior. However, Canada's October 2018 entrance to the European Centre of Excellence for Countering Hybrid Threats is an important step in the Canadian government's ability to share information and prevent Russian disinformation.[74] Sharing information will strengthen Western states' response to Russian disinformation by increasing their ability to identify targets and retaliate with a coordinated cyber response.

A third approach that Canada should undertake to reduce the impact of Russian disinformation is to work with social media providers to limit Russia's ability to use their platforms to communicate the Russian disinformation. Initially companies such as Google, Facebook, and Twitter "denied that their services could have been manipulated by disinformation."[75] Only recently have the companies admitted that their services were utilized to support disinformation, and have subsequently taken steps to remove false news stories, limit advertisement purchases, and introduce software fixes to close technological loopholes exploited by Russian disinformation.[76] Despite these steps, companies such as Facebook continue to have challenges with transparency. For

---

[72]Liisa Past, "Cyberspace- Just Another Domain of Election Interference?," (Helsinki: Hybrid Center of Excellence, August 2018), 5.

[73]"The EU General Data Protection Regulation (GPDR) is the most important change in data regulation in 20 years," Accessed April 17th, 2019, https://eugdpr.org/

[74]"Canada joins Hybrid COE", Accessed April 16th, 2019, https://www.hybridcoe.fi/news/canada-joins-hybrid-coe/ Between 25-27 October 2017, I represented Canada at the NATO annual hybrid conference in Warsaw, Poland to review Russian activities in Europe. One recommendation, Canada was already leaning that way, was to join the COE.

[75]Keir Giles, "Countering Russian Information Operations in the Age of Social Media, "Accessed April 8th, 2019, https://www.cfr.org/report/countering-russian-information-operations-age-social-media.

[76]*Ibid.,*

example, Canada's Privacy Commissioner Daniel Therrien opened an investigation into *Cambridge Analytica* to determine whether Canadians were subject to a privacy breach with personal information provided in support of President Trump's 2016 election campaign.[77] *Cambridge Analytica* interests in information highlight weaknesses with social media platforms that are transnational and driven by profits. In this context, expecting social media companies to change is increasingly difficult.

Canada could undertake similar steps taken by Allies to address the use of social media platforms. For example, in France, there have been proposals requiring web services providers to disclose advertisement sponsors and even to go as far as removing content or block websites.[78] Blocking content may not align with current Canadian law, however, disclosure of advertising sponsors during election campaigns is common practice in Canada. Canadian elections laws, amended in 2014, limit and force foreign entities to register if they spent more than $500 on election advertisements.[79] Legal changes should also limit the ability of organizations that support Russian disinformation from spending large amounts of money with social media platforms. Finally, Canada's security agencies should work closely with social media organizations to identify troll and bot accounts responsible for "amplifying narratives to a broader global audience."[80] The Canadian government recognizes this requirement as noted in a January 2019 speech by Minister of Democratic Institutions, Karina Gould, where she stated one area of action

---

[77]Kevin Neilson, "Canadian Government to investigate whether Facebook violated *Privacy Act*," *Global News*, Accessed April 15th, 2019, https://globalnews.ca/news/4095409/canadian-government-investigation-facebook-privacy-act/

[78]Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue. "Addressing Hybrid Threats." (Stockholm: Swedish Defence University, 2018), 84.

[79]Canada, Elections Canada, "Information on Third Parties and Election Advertising," Accessed April 15th, 2019, https://www.elections.ca/content.aspx?section=pol&document=info&dir=thi&lang=e

[80]Marcus Kolga, "Stemming the Virus: Understanding and Responding to the Threat of Russian Disinformation," (Ottawa: Macdonald-Laurier Institute, 2019), 15.

was to encourage "expected social media platforms to act."[81] The Canadian government should continue to pressure social media organizations to remain act transparent and open with regards to Russian disinformation. While it is difficult for Canada to be an individual entity working with social media organizations, norms established by the EU such as the General Data Protection Regulation could provide the necessary framework to influence social media organization behavioral change.

The fourth step that the Canadian government should undertake is further educating Canadians on Russian disinformation. CSE believes exploitation Canadian voters will continue due to their use of social media.[82]Canadians, with nearly 90% using the internet, require a better understanding of internet usage and influence.[83] This education should increase personal and corporate understanding of their information technology vulnerabilities regarding Russian disinformation. The Canadian government should undertake steps, whether through the use of educational tools, public service announcements, or regular briefings on disinformation, to ensure Canadians understand basic tools of disinformation such as malware or phishing. Canadians also require education on "personal security measures, such as strengthening passwords and not providing information over email or the phone in response to unsolicited requests, are basic measures that can be communicated."[84] Finally, the Canadian government should

---

[81]Canada, Democratic Institutions, "The Government of Canada's Plan to Safe Guard Canada's 2019 election," Speech by Minister's Gould, Sajjan, Goodale on January 30th, 2019, Accessed April 15th, 2019, https://www.canada.ca/en/democratic-institutions/news/2019/03/speech-thegovernment-of-canadas-plan-to-safeguard-canadas-2019-election.html

[82]Canada, Communications Security Establishment, "2019 Update: Cyber threats to Canada's Democratic Process," (Ottawa: Communications Security Establishment, 2019), 18.

[83] "Canada's Internet Factbook 2018: Canada's source for current internet data," *Canadian Internet Registration Authority,* Accessed April 15th, 2019, https://cira.ca/factbook/canada%E2%80%99s-internet-factbook-2018

[84]Marcus Kolga, "Stemming the Virus: Understanding and Responding to the Threat of Russian Disinformation," (Ottawa: Macdonald-Laurier Institute, 2019), 42.

create and advertise a mechanism that will allow Canadians to report or identify any attempts of disinformation. Establishing a reporting framework may be a complicated endeavor to implement, however, simple security steps as well as having access to a reporting mechanism can improve individual and corporate confidence in the Canadian government's ability to address the serious threat posed by Russian disinformation.

Pursuing a centralized whole-of-government approach that includes members of academia and the private sector may also improve the Canadian government's ability to respond to Russian disinformation activities. In the 1980s, the US established the Active Measures Working Group which was tasked to monitor and expose Soviet disinformation campaigns.[85] A similar response in Canada could work towards limiting Russian disinformation while coordinating "policy and platform solutions with major technology companies, review and propose legislative solutions, and educate the press and public."[86] Industry and academia may want to retain some independence and not want to work within a government task force, however, the strength of a multi-discipline forum should encourage a sharing of ideas, best practices, and observations that should improve the Canadian government's ability to respond to Russian disinformation.[87]

Canada is a democratic nation that is part of NATO, the G7, and actively pursues diplomatic and economic policies that counter Russian ambitions. Russia's combination of military force with information operations along with the transnational nature of social media has increased Russia's position of strength. Successes in Syria and Ukraine, plus Canada's response by implementing targeted sanctions created an environment of overt

---

[85]Elizabeth Baron-Bodine, Todd C. Helmus, Andrew Radin, and Elina Treyger, "Countering Russian Social Media Influence," (Santa Monica: RAND Corporation, 2018), 43.
[86]*Ibid.,* 43.
[87]*Ibid.,* 43.

Russian disinformation in Canada. Initially, Canadian attempts to deter by defence had limited effect and failed to dissuade Russian disinformation actions. Recent admissions by the Canadian government and CSE regarding potential election interference continue to highlight efforts by Russia to undermine Canadian democracy. The effect of the Canadian government response disinformation includes the creation of the SITE Task Force, amendments to cyber legislation intended to enable disruptive offensive operations against adversaries, and targeted sanctions will not be known for several years.

Despite these steps, the Canadian government requires additional steps to address Russian disinformation. Further analysis may be required, however, a whole-of-government approach that unites resources and security agencies outside of election timeframes is required to deal with the persistent Russian threat. Canadians as significant users of the internet require tools to identify, report, and prevent attempts at Russian disinformation. Also, the Canadian government should increase cooperation with academia and private corporations to share best practices and develop policies to pre-empt Russian efforts. Thirdly, Canada needs to explore international regulations to establish norms within cyberspace. Canada should work closely with Allies to share information and respond to threats since Russia continues to demonstrate an unwillingness to cooperate. Finally, perhaps the most challenging, Canada must continue to pressure social media platforms such as Facebook and Twitter to limit the use of their platforms for Russian disinformation. With the transnational nature of technology and funds garnered by advertisement, social media platforms genuinely lack the will to address the threat adequately. Until this occurs, Canada must utilize all tools of power to create a culture of deterrence to identify Russian disinformation targets, retaliate to any

infringements, and disseminate, when secrecy permits, how Canada addressed Russian disinformation.

Bibliography.

Acros, Ruben. “Post-event Analysis of the Hybrid Security Environment: Assessment of Influence Communication Operations.” Helsinki: Hybrid Center of Excellence, October 2018.

Adamsky Dmitry (Dima). “From Moscow with coercion: Russian deterrence theory and strategic culture.” *Journal of Strategic Studies* 41. no 1-2 (2018), 33-60.

Allen T. S. and A. J. Moore. “Victory without Casualties: Russia’s Information Operations.” *US War College Quarterly* 48, no.1 (Spring 2018): 59-71.

Applebaum, Anne. “Russia is furious. That means the sanctions are working.” *The Washington Post*. Accessed April 15th, 2019. https://www.washingtonpost.com/opinions/global-opinions/russia-is-furious-that-means-the-sanctions-are-working/2017/10/27/2b8f63dc-bb33-11e7-a908-a3470754bbb9_story.html?utm_term=.e51c9c66b275.

Bachmann Sacha Dov and Andres B Munoz Mosquera. “Lawfare and hybrid warfare – how Russia is using the law as a weapon.” Accessed April 20th, 2019. https://www.researchgate.net/publication/320027113_Lawfare_and_hybrid_warfare_-_how_Russia_is_using_the_law_as_a_weapon.

Baron-Bodine, Elizabeth, Todd C. Helmus, Andrew Radin, and Elina Treyger. “Countering Russian Social Media Influence.” Santa Monica: RAND Corporation, 2018.

Baun, Michael. "Germany and Central Europe: Hegemony Re-Examined." *German Politics*14, no. 3(2005): 371-389.

“Bill C-22 passes in House of Commons.” *The Canadian Press.* Accessed April 15th, 2019. https://www.huffingtonpost.ca/2017/04/04/bill-c-22-passes-in-house_n_15813744.html.

Blanchfield, Mike. “Canada Backs Recommendation for Magnitsky Act Targeting Human Rights Violators.” *The Toronto Star*. Accessed April 15th, 2019. https://www.thestar.com/news/canada/2017/05/17/canada-backs-recommendation-for-magnitsky-act-targeting-human-rights-violators.html.

Bramham, Daphne. “Daphne Bramham: Voters should brace for foreign interference in Canada’s federal election,” *The Vancouver Sun*, Accessed April 14th, 2019, https://vancouversun.com/opinion/columnists/daphne-bramham-voters-should-brace-for-foreign-interference-in-canadas-federal-election.

Brown, Chris. “Anti- Canada Propaganda greets troops in Latvia.” Accessed April 3rd, 2019. https://www.cbc.ca/news/world/latvia-propaganda-1.4162612

Boutilier, Alex. “Sajjan Defends Proposed New Spy Powers to Conduct ‘Information’ Warfare.” *The Toronto Star*. Accessed April 8th, 2019. https://www.thestar.com/news/canada/2018/01/11/sajjan-defends-proposed-new-spy-powers-to-conduct-information-warfare.html.

Bukkvoll, Tor. “Why Putin went to war: ideology, interests and decision-making in the Russian use of force in Crimea and Donbas.” *Contemporary Politics* 22. No. 3(2016), 267-282

Canada. Communications Security Establishment. “2019 Update: Cyber threats to Canada’s Democratic Process.” Ottawa: Communications Security Establishment, 2019.

Canada. Democratic Institutions. “The Government of Canada’s Plan to Safe Guard Canada’s 2019 election.” Speech by Minister’s Gould, Sajjan, Goodale on January 30th, 2019. Accessed April 15th, 2019. https://www.canada.ca/en/democratic-institutions/news/2019/03/speech-thegovernment-of-canadas-plan-to-safeguard-canadas-2019-election.html.

Canada. Elections Canada. “Information on Third Parties and Election Advertising.” Accessed April 15th, 2019. https://www.elections.ca/content.aspx?section=pol&document=info&dir=thi&lang=e.

Canada. Global Affairs Canada. “Canadian Sanctions Related to Russia.” Accessed April 15th, 2019. https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/Russia-Russie.aspx?lang=eng.

Canada. Canadian Security Intelligence Service. “Who Said What? The Security Challenges of Modern Disinformation.” Ottawa: Canadian Security Intelligence Service, February 2018.

Canada. Department of National Defence. Joint Doctrine Manual. *Joint Public Affairs 2017-05.* Ottawa: Strategic Joint Staff Public Affairs, 2017.

Canada. Department of National Defence. Joint Doctrine Note 2017-02. *Cyber Operations - Draft.* Ottawa: Canadian Warfare Center, 2017.

Canada. "Russia and the West: The Consequences of Renewed Rivalry." Ottawa: Canadian Security Intelligence Service, June 2015.

Canada. Department of National Defence. Canadian Forces Joint Publication. *Intelligence.* Ottawa: Canadian Forces Joint Warfare Center, 2011.

Canada. "Matching Ambitions and Realities: What Future for Russia?" Ottawa: Canadian Security Intelligence Service, May 2010.

Canada. Department of National Defence. B-GG-005-004/AF-010. *CF Information Operations.* Ottawa: Canadian Warfare Center, 1998.

"Canada joins Hybrid COE", Accessed April 16th, 2019, https://www.hybridcoe.fi/news/canada-joins-hybrid-coe/

"Canada's Internet Factbook 2018: Canada's source for current internet data." *Canadian Internet Registration Authority*. Accessed April 15th, 2019. https://cira.ca/factbook/canada%E2%80%99s-internet-factbook-2018.

Chyczij, Alexandra. "Canada is a Target of Russian Disinformation. Let's be Ready." *The Hill Times*. Accessed April 8th, 2019. https://www.hilltimes.com/2019/01/30/canada-target-russias-disinformation-letsready/185567.

Connolly, Amanda. "No Worries About Wernick's Role on Election Alert Panel, Despite Calls for him to Resign: Gould." *National Online Journalist (Politics) Global News*. Accessed April 15th, 2019. https://globalnews.ca/news/5035336/karina-gould-michael-wernick-snc-lavalin-affair/.

Cullen, Patrick. "Hybrid Threats as the New 'Wicked Problem' for Early Warning." Helsinki: Hybrid Center of Excellence, May 2018.

Ducheine, Paul. "Non-kinetic capabilities: Complementing the Kinetic Prevalence to Targeting," in *Targeting: The Challenges of Modern Warfare*, edited by Paul A.L. Ducheine, Michael N. Schmitt, and Frans P. B. Osinga, (The Hague: Springer, 2016), 201-230.

Eckel, Mike. "Russia's Shock And Awe: Moscow Ups Its Information Warfare In Syria Operation." *Radio Free Europe Documents and Publications*. Washington, 07 October 2015, 1-3.

Fife, Robert. “Freeland warns Canadians to be aware of Russian disinformation.” *The Globe and Mail*. Accessed April 3rd, 2019. https://www.theglobeandmail.com/news/politics/freeland-warns-canadians-to-beware-of-russian-disinformation/article34227707/.

Giles, Keir. “Countering Russian Information Operations in the Age of Social Media.” Accessed April 8th, 2019. https://www.cfr.org/report/countering-russian-information-operations-age-social-media.

Hannant, Laurence. “Igor Gouzenko and Canada's Cold War.” *The Beaver* 75, no. 5 (10, 1995): 19-23.

Herman, Michael. “Ethics and Intelligence after September 2001.” *Intelligence and National Security* 19, no. 2 (2004): 342-358.

Horton, Alex. “The Magnitsky Act, Explained.” *The Washington Post*. Accessed April 15th, 2019. https://www.washingtonpost.com/news/the-fix/wp/2017/07/14/the-magnitsky-act-explained/?utm_term=.aef24170580f.

Jackson, Nicole J. “NATO’s and Canada’s Responses to Russia since the Crimea Annexation of 2014: A Critical Literature Review.” *Simons Papers in Security and Development* 61. Vancouver: School for International Studies - Simon Fraser University, December 2017.

Levin, Dan and Jo Becker. “Canadian Lawmakers say Pro-Russia Group Tried to Derail Sanctions Law.” *The New York Times*. Accessed April 8th, 2019. https://www.nytimes.com/2017/10/04/world/canada/russiamagnitsky.html?partner=bloomberg.

Kolga, Marcus. “Stemming the Virus: Understanding and Responding to the Threat of Russian Disinformation.” Ottawa: Macdonald-Laurier Institute, 2019.

Korhonen, Iikka Heli Simola and Laura Solanko. “Sanctions, counter-sanctions and Russia − Effects on economy, trade and finance.” Helsinki: Bank of Finland- Institute for Economies in Transition, 2018, 1-22.

Kragh, Martin and Sebastian Asberg. “Russia’s Strategy for influence through public diplomacy and active measures: the Swedish case.” *Journal of Strategic Studies* 40. No. 6 (2017), 773-816.

Kramer, Andrew E. “Russian General Pitches ‘Information’ Operations as a Form of War.” *The New York Times*. Accessed April 3rd, 2019. https://www.nytimes.com/2019/03/02/world/europe/russia-hybrid-war-gerasimov.html.

Kudors, Andis. "Fortress Russia: Political, Economic, and Security Development in Russia following the Annexation of Crimea and its Consequences for the Baltic States." Riga: The Center for East Europe Policy Studies University of Latvia Free Press, 2016.

McSorley, Tim. "Bill C-22: Liberals Undermining Goal of Strong National Security Oversight." Accessed on April 15th, 2019. https://www.huffingtonpost.ca/tim-mcsorley/liberals-bill-c-22_b_15695114.html.

Neilson, Kevin. "Canadian Government to investigate whether Facebook violated *Privacy Act*." *Global News*. Accessed April 15th, 2019. https://globalnews.ca/news/4095409/canadian-government-investigation-facebook-privacy-act/.

North Atlantic Treaty Organization. "NATO's Response to Hybrid Threats." Accessed April 3rd, 2019. https://www.nato.int/cps/en/natohq/topics_156338.htm.

"Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2018." *Statista.* Accessed April 10th, 2019. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

Osinga, Frans P. B. and Mark P. Roorda. "From Douhet to Drones, Air Warfare, and the Evolution of Targeting." in *Targeting: The Challenges of Modern Warfare*. Edited by Paul A.L. Ducheine, Michael N. Schmitt, and Frans P. B. Osinga. The Hague: Springer, 2016, 27-76.

Past, Liisa. "Cyberspace- Just Another Domain of Election Interference?." Helsinki: Hybrid Center of Excellence, August 2018.

Putin, Vladimir. "Meeting with Russian Ambassadors and Permanent Representatives in International Organizations." Speech from 2012. Accessed April 25th, 2019, http://en.kremlin.ru/events/president/news/15902

Putin, Vladimir. "Meeting with President of Ukraine Viktor Yanukovych." Transcript from the meeting. Accessed April 25th, 2019. http://en.kremlin.ru/events/president/news/19849

Ralph, Jason, and Jess Gifkins. "The purpose of United Nations Security Council practice: Contesting competence claims in the normative context created by the Responsibility to Protect." *European Journal of International Relations* 23, no. 3(2017): 630-653.

Renz, Bettina. "Russia's Military Revival." Cambridge: Polity Press, 2018.

"Russia passes bill to allow internet to be cut off from foreign servers." *The Guardian.* Accessed April 16th, 2019. https://www.theguardian.com/world/2019/apr/11/russia-passes-bill-internet-cut-off-foreign-servers.

Sari, Aurel. "Blurred Lines: Hybrid Threats and the Politics of International Law." Helsinki: Hybrid Center of Excellence, January 2018.

Scotti, Monique. "Here's what you need to know about Canada's 'extraordinarily permissive' new spying laws." *National Online Journalist (Politics) Global News*. Accessed April 15th, 2019. https://globalnews.ca/news/3999947/cse-c59-new-spy-powers-canada/

Shiffman, Gary M. "Economic Security." Chap. 15 in *Contemporary Security Studies*. 3rd ed. Edited by Alan Collins. New York: Oxford University Press, 2016, 208-222.

Shin, Geigeun, Seung-Whan Choi, and Shali Luo. "Do Economic Sanctions Impair Target Economies?." *International Political Science Review* 34, no. 4(2016), 485-499.

Sorensen, Heine and Dorthe Bach Nyemann. "Going Beyond Resilience: A Revitalized Approach to Countering Hybrid Threats." Helsinki: Hybrid Center of Excellence, November 2018.

Souleimanov Emil Aslan and Valery Dzutsati. "Russia's Syria War: A Strategic Trap?." *Middle East Policy* 25, no. 2 (June 2018): 42-50.

Taddeo, Maria Rosario. "How to deter in Cyberspace." Helsinki: Hybrid Center of Excellence, June-July 2018.

"The EU General Data Protection Regulation (GPDR) is the most important change in data regulation in 20 years," Accessed April 17th, 2019, https://eugdpr.org/

Treverton Gregory F., Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue. "Addressing Hybrid Threats." Stockholm: Swedish Defence University, 2018.

Valaskivi, Katja. "Beyond Fake News: Content Confusion and Understanding the Dynamics of the Contemporary Media Environment." Helsinki: Hybrid Center of Excellence, February 2018.

Wark, Wesley. "Michael Wernick's Alarmist Words are the Politics of Fear." *The Globe and Mail*. Accessed April 15th, 2019. https://www.theglobeandmail.com/opinion/article-michael-wernicks-alarmist-words-are-the-politics-of-fear/.

Weiss, Brennan. “A Russian Troll Factory had a $1.25 million monthly budget to interfere in the 2016 US election.” *Business Insider*. Accessed April 3rd, 2019. https://www.businessinsider.com/russian-troll-farm-spent-millions-on-election-interference-2018-2.

Whitaker, Reg. “The Politics of Security Intelligence Policy-making in Canada: I 1970-84.” *Intelligence and National Security* 6, no. 4 (October 1991): 649-668.