National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Information Is Power: Threats to the CAF in the Information Domain

Major Thomas J. Dinner

JCSP 46 DL

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 46 AD

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 46 DL – PCEMI 46 AD
2019 – 2021

SOLO FLIGHT

INFORMATION IS POWER: THREATS TO THE CAF IN THE INFORMATION DOMAIN

By Major T.J. Dinner

INFORMATION IS POWER:
THREATS TO THE CAF IN THE INFORMATION DOMAIN

The world has fundamentally changed with the improvement of technology and transmission of information. With this shift, information is highly sought after by a vast portion of the global population to remain informed on current events and to aid in developing an opinion or making a decision. As such, methods of warfare are adapting to an information-dominated society with the primacy placed on acquiring information and exploiting it. As recently as 2014, information operations have been conducted by various state and non-state entities which aim to adversely affect their opponents in the information domain. Russia has successfully utilized disinformation to foster internal conflicts and to influence public opinion against their adversaries, specifically NATO partners. As such, the lessons learned from these operations are being applied to current Canadian participation in NATO operations, specifically Operation REASSURANCE in Latvia. Although there are different methods to countering adversarial messaging and disinformation, Canada and NATO must attain and retain the initiative in the information domain to ultimately deter these threats. This paper will argue that it is imperative for the CAF to counter adversaries' manoeuvre in the information domain and regain the initiative in order to deter a growing and significant threat to Canada.

Through the analysis of literature, Canadian and Allied doctrine this paper will examine the importance of information operations in modern warfare, specifically use of media and messaging to influence target audiences. Part one of this paper will analyse recent examples of adversary capabilities, particularly the Russian information operations against Ukraine in the annexation of Crimea in 2014. Part two will examine current information operations against NATO and Canada on Operation REASSURANCE and their effects on credibility. Part three will consider allied information operations doctrine compared to that of Canada, and the

importance of strategic communications to allied partners. Part four will be a discussion on ways Canada can enhance understanding and regaining the initiative in the information domain.

INFORMATION WARFARE – RUSSIAN APPLICATION

Russia strives to achieve the influence and power of its predecessor state, the Union of Soviet Socialist Republic (USSR). When the USSR collapsed, the Baltic region and Ukraine became independent countries and expelled any vestige of the USSR's military might and influence. Other former Soviet states also rejected Russian influence; Latvia took a more pro-NATO and pro-Western stance. Russia saw and continues to see this as a threat to its security, influence and ambitions. While Russia sought to become stronger and more relevant in a post-Soviet world, it managed to grow its military and expand on older techniques like *maskirovka* to gain influence in former USSR territories. *Maskirovka* is aimed to influence adversaries and set a favourable situation for military forces through the use of deception, misinformation and psychological operations.[1] Russian *maskirovka* is a hybrid threat which is non-violent actions under the threshold of conflict that are used to gain strategic leverage.[2] These actions aim to achieve political decisive outcomes without overt use of military force.[3]Methods available to execute information operations cover a broad range of systems including "computers, smartphones, real or invented news media… [and] online trolls"[4] to name but a few. These methods are used to influence or distort the narrative of current events.[5] Ultimately, a narrative

---

1 James Q. Roberts, "Maskirovka 2.0: Hybrid Threat, Hybrid Response," *Joint Special Operations University Centre for Special Operations Studies and Research*, (December 2015), 1.

2 Sean Monaghan, "Countering Hybrid Warfare: So What for the Future Joint Force?" *Prism 8*, no. 2 (4 October 2019), 84-85.

3 Bastian Giegerich, "Hybrid Warfare and the Changing Character of Conflict," *Connections: The Quarterly Journal 15,* no. 2 (Spring 2016), 66-67.

4 Keir Giles and Anthony Seaboyer, *The Russian Information Warfare Construct*, (Toronto, ON: DRDC, March 2019), 5.

5 Scott Ruston, "Narrative & Strategic Communications", in *Russia's Footprint in the Nordic-Baltic Information Environment, Report 2019/2020*, (Riga, Latvia: NATO Strategic Communications Centre of Excellence, November 2020), 16. A narrative is a "system of stories structures in such a way as to make meaning about the world around us."

will be wielded as a weapon to influence the deeper meaning that individuals would infer from a specific event or story.[6] This is congruent with Russian information warfare concepts which act to influence an adversary's perception and behaviour. As well, Russia sees the superiority in the information domain as a key enabler for success in any conflict against its rivals.[7]

CRIMEA – APPLICATION OF INFORMATION OPERATIONS TO ENABLE HYBRID WARFARE

As seen in Crimea in 2014 Russia utilized a series of information and cyber operations to influence ethnic Russians and create a narrative which vilified Ukrainian authority. This emboldened pro-Russian sentiment and enabled the infiltration of armed militias and other Russian forces to seize Crimea whilst discrediting Ukrainian authority and military power. This is an example of hybrid warfare, which is the use of different modes of warfare, specifically conventional capabilities coupled with irregular tactics which incorporate the use of terrorist activities by state and non-state entities[8]to offset the power of stronger nations' conventional forces through the use of cyber, information operations and deniable use of special operations elements to gain an asymmetric advantage.[9]To achieve the goal of seizing Crimea, Russia set favourable conditions to gain the initiative on their target and NATO in general through the use of effective information operations. Information Operations are actions which aim to influence decision makers by affecting the perception of information[10] with the aim to affect the will of adversaries or target audiences by influencing understanding and to change behaviour of the

---

6 Maris Cepuritis and Austeris Keiss, "Hostile Narratives and their Impact: The Case of Latvia," in *Russia's Footprint in the Nordic-Baltic Information Environment, Report 2019/2020*, (Riga, Latvia: NATO Strategic Communications Centre of Excellence, November 2020), 18.

7 Keir Giles and Anthony Seaboyer, *The Russian Information Warfare Construct...,* 6.

8 James K. Wither, "Making Sense of Hybrid Warfare," C*onnections: The Quarterly Journal 15, no. 2* (2016), 75.

9 Sean Monaghan, "Countering Hybrid Warfare: So What for the Future Joint Force?"…, 84-85

10 Canada, Department of National Defence, *B-GG-004-005/AF-010, CF Information Operations* (Ottawa: Joint Doctrine Branch, 1998), 1-2.

target.[11]The Russian perception of Information Operations sees its use as a decisive effect to enable success in operations and achievement of political goals.

Russia's effectiveness in Information Operations aims to shape or own the narrative. Shaping the narrative served to embolden pro-Russian sentiments and developed the requirement to justify any intervention.[12] Through influence operations conducted on social media, news and political messaging Russia helped shape anti-West sentiments which aimed to isolate and to erode trust in government institutions.[13] In 2014 for instance, Russia was able to effectively influence ethnic Russians in Crimea through the use of cyber effects and other state instruments to deceive and shape the narrative, such as "fake news"[14] and playing on historical precedents of Ukrainians being aligned with fascists.[15] This acted to cultivate a culture of fear and hate among ethnic Russians in Ukraine.[16] Once the narrative was shaped and Ukraine's credibility weakened, Russia enabled armed groups to seize Crimea with deniability and deception covering their actions.[17] However, the effective use of *maskirovka* tactics was not necessarily to persuade the world to believe Russia's disinformation, rather it was to exploit the social tensions within the targeted regions.[18] This shaping effort enabled the use of "little green men," an irregular militant organization, to provoke insurrection supported by continued offensive operations within the

---

[11] North Atlantic Treaty Organization. *NATO Bi-SC Information Operations Reference Book*.(SHAPE: North Atlantic Treaty Organization, 5 March 2010), 9-10.

[12] Edwin Armistead and Scott Starsman, "Perception Shaping and Cyber Macht: Russia and Ukraine," *International Conference on Cyber Warfare and Security* (2015), 15.

[13] Todd C. Helmus, Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman, *Russian Social Media Influence — Understanding Russian Propoganda in Eastern Europe*, (Santa Monica, CA: RAND Corporation, 2018) 8-9.

[14] David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, (New York, NY: Broadway Books, 2018), 157.

[15] Dr. Cerwyn Moore, "Russian Disinformation: The Case of Ukraine", *Centre for Research and Evidence on Security Threats*, (March 2019), 6.

[16] Sanda Svetoka, *Social Media as a Tool of Hybrid Warfare*, (Riga, Latvia: NATO StratCom COE, May 2016), 19.

[17] Geir Hågen Karlsen, "Tools of Russian Influence: Information and Propaganda." In *Ukraine and Beyond: Russia's Strategic Security Challenge to Europe*, edited by Janne Haaland Matlary and Tormod Heier, 181-208, (Cham: Palgrave Macmillan, 2016), 192.

[18] Ibid.

information domain aimed at discrediting Ukrainian officials and institutions provided Russia deniability.[19]Through shaping the narrative, coupled with the exploitation of social media to divide the ethnic populations of Ukraine, Russia was able to discredit and disrupt the Ukrainian government and enable pro-Russian factions to seize Crimea. Through the use of a Whole of Government (WoG) approach, Russia's use of strategic *maskirovka* and targeted information operations enabled the seizure of the strategically important port city of Sevastopol and the deterrence of NATO in the region through hybrid warfare.[20]Although one could only infer Russia's true intentions and political objectives, it is apparent that the annexation of a significant portion of an aspiring NATO member can be deemed a success by all observers. Through the use of information operations Russia enabled this annexation of Crimea through mostly non-violent means while demonstrating the weakness of Ukraine and damaging the credibility of NATO, specifically its initial response, on an international stage.

ADVERSE EFFECTS OF RUSSIAN INFORMATION OPERATIONS TO THE CAF

As a member of NATO, Canada has deployed forces and taken a leading role in the enhanced forward presence force in Latvia. Operation REASSURANCE is to act as deterrence against aggression in Eastern Europe, specifically the Baltic region and to reinforce NATO's collective defence.[21] Eager to prevent the hybrid warfare witnessed in Ukraine, significant military forces have been mustered all across NATO's eastern sphere of influence.[22] Despite the presence of significant military forces, Russia remains undeterred in the information domain.

---

19 David E. Sanger, *The Perfect Weapon.…*,,255.

20 Ben Connable, Stephanie Young, et al. "Russia's Hostile Measures: Combating Russian Gray Zone Aggression Against NATO in the Contact, Blunt, and Surge Layers of Competition", RAND Corporation, (Santa Monica, CA: 2020), 42.

21 Canada, Department of National Defence, "Operation REASSURANCE", https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-reassurance.html, last updated 20 May 2021.

22 North Atlantic Treaty Organization, "NATO's Enhanced Forward Presence", https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/2103-factsheet_efp_en.pdf, March 2021.

Having found varying degrees of success in Ukraine in shaping the narrative, Russia continues to utilize instruments of state power and pro-Russia media in target nations to attack the legitimacy and credibility of not only the host nation's governments but the military forces and governments of the NATO members partaking in the enhanced forward presence (eFP) force.

Studies conducted by NATO's Strategic Communications Centre of Excellence (StratCom COE) into Russia's information operations in Ukraine and Crimea have identified a linkage between media outlets, use of developed social media platforms like Twitter and ideological groups.[23] This consists of trolls who push messaging and commentary on websites and social media platforms to disrupt discussion and initiate conflict amongst different groups through deception and disruptive behaviour. Hybrid trolls use this deceptive behaviour to advance a political agenda and have been found to operate under the orders of states or organizations aiming to advance these narratives.[24] Russia has also been using a tactic known as information laundering to advance their narratives while maintaining deniability. Information laundering encompasses the legitimization of false information through intermediaries like pro-Russian media outlets to obscure the originating source.[25] This tactic has potential in the Latgale region of Latvia, which is home to a large Russian-speaking population influenced by Russian media.[26]

Canada and the Latvian population has been subject of many information attacks by Russia or pro-Russian entities. Prior to the arrival of the Canadian Armed Forces contingent to Latvia pro-Russian media and affiliated outlets published false news stories indicating that

---

[23] Sanda Svetoka, *Social Media as a Tool of Hybrid Warfare*, (Riga, Latvia: NATO StratCom COE, May 2016), 24.

[24] Ibid., 27.

[25] Belen Carrasco Rodriguez, *Information Laundering in the Nordic-Baltic Region*, (Riga, Latvia: NATO StratCom COE, November 2020), 11-13.

[26] Mark MacKinnon, "For many in Latvia's Russified east, Canada's 'Operation Reassurance' is anything but," *The Globe and Mail*, (Toronto: 15 April, 2017).

"serial killer and former RCAF Colonel Russell Williams was an example of Canadian military leadership"[27] which was perpetuated by hybrid trolls to demonstrate the moral superiority of Russian leadership and to denigrate that of Canada.[28] Though easily dismissed by Western media, stories like these can become numerous and eventually damaging to Canada's presence in Latvia among if not effectively countered and discredited as false. However, more convincing messaging in Canada has been utilized through reputable state broadcasters like the Canadian Broadcasting Corporation (CBC) by framing ongoing discussions in a fashion that suited Russia's narrative. For instance, Russia seized on a CBC news article in which a German quotation seeing the deployment of NATO troops in close proximity to Russia's borders could be seen as a provocation which was a breach of the NATO-Russia Founding Act – the viewpoint that Russia believes and propagates.

As another example, Russian influencing of the narrative plays on host nation population's concerns over the use of tax money while attacking the credibility of Canadian and NATO forces. This included a distortion of the facts surrounding NATO members being quartered in hotels instead of the base accommodations at Latvia's expense. This story was misappropriated by pro-Russian media to infer that Latvian barracks and amenities were not to the standard of other Western nations, who opted to appropriate luxury hotels for their own use and that Latvia was wasting taxpayers' money.[29]This hostile narrative, which played to Latvian fears that their government was hosting foreign military forces on the taxpayers' dime acted to bolster attacks on Latvian defence spending as a waste of money.[30]

---

[27] Chris Wattie, "Bringing a Knife to a Gun Fight: Canadian Strategic Communications and Information Operations in Latvia, Operation REASSURANCE 2019-2020," *Canadian Military Journal Vol. 21*, No. 1 (Winter 2020), 57.

[28] Sanda Svetoka, *Social Media as a Tool of Hybrid Warfare*…, 29

[29] Belen Carrasco Rodriguez, *Information Laundering in the Nordic-Baltic Region*…, 59

[30] Chris Wattie, "Bringing a Knife to a Gun Fight…", 59.

Canada made statements to the contrary in all these cases and condemned the actions of those entities which perpetrated these information operations, more needs to be done to discredit adversarial messaging. Although the narrative can be explained in a post-event news release or statement, persistent attacks in the information domain against a reactive target can go on for so long before credibility of the mission and the CAF begins to erode both within the host nation and in Canada. Even if disinformation fails to influence decision making of a target nation, persistent narratives can shape the public support of an adversary's population and ultimately limit NATO's freedom of action and credibility.[31]

NECESSITY OF INFORMATION OPERATIONS TO CANADA

Given the changing nature of conflict, Canada's allies and NATO partners have placed an emphasis on Strategic Communications (StratCom) and understand the importance of the information domain, particularly the United Kingdom (UK), the United States (US) and Lithuania. The UK understands that strategic compression is increasing and that coherent narratives are necessary to mitigate public scrutiny in media and cyberspace to enable favourable attitudes and behaviours of target audiences.[32] UK doctrine states that it is not simply creating just a compelling narrative but to have the delegation of authorities to allow for decentralized execution.[33] US Joint Doctrine stresses the importance of information operations in military operations, in that adversaries actively use information operations actions "as asymmetric warfare that can be used to thwart US military objectives that are heavily reliant on information systems."[34] Among information operations core capabilities, US doctrine highlights that

---

31 Keir Giles and Anthony Seaboyer, *The Russian Information Warfare Construct*…, 15

32 United Kingdom, Ministry of Defence, *Joint Doctrine Note 1/12 Strategic Communication: The Defence Contribution*, (Swindon, UK: Development, Concepts and Doctrine Centre, January 2012), 2-1 – 2-2. Strategic compression is a term to describe that tactical actions will have operational and strategic consequences more often.

33 Ibid., 2-12.

34 United States, Department of Defense, *Joint Publication 3-13 Information Operations*, Washington, D.C.: February 2006, I-10 – I-11.

psychological operations at the tactical level can have strategic effects.[35] The Lithuanian Armed Forces (LAF) developed their StratCom department to counter adversarial attempts to nullify their population's will to resist. Lithuanian StratCom asserts that information operations are aimed to discredit the LAF at the tactical level, and to intimidate society at the strategic level.[36] Therefore, LAF StratCom developed its processes to analyse and implement actions to educate and inform their population, thus building resilience to hostile narratives and to foster a strong relationship between the Lithuanian population and their armed forces.[37]

It is apparent that information operations are growing in intensity and importance in modern conflict. Though information is used as a weapon, it must be wielded carefully. The use of fake news and mass trolling by Canada to garner influence would be to the detriment of Canada's credibility[38] as Russia or other adversaries could use these against us much like we have of them. Rather, Canada must respond in ways to maintain the legitimacy of Op REASSURANCE in Latvia. On the basic level, effective communications and engagements with local elements and the population in Latvia will bolster credibility and image of CAF elements, while demonstrating pro-Russian messaging on Canada's intentions are false. In Latvia, a StratCom Cell at Task Force Latvia has been stood up to act as the eyes and ears of the Task Force Commander. The cell achieves this through the tracking of hostile narratives in the area, information attacks on NATO and Canada's credibility and upon Latvian support to both entities.[39] Owning and controlling the narrative in theatre is necessary to wrest the initiative from our adversaries' hands. A comprehensive strategic communications regime needs to be fostered to allow for denying information supremacy of our adversaries. However, the CAF's ability to

---

35 Ibid., II-2

36 Lieutenant Colonel Linas Idzelis, "Leveraging StratCom", *Special Warfare Vol 32*, Issue 3, (July-December 2019), 42

37 Ibid.

38 Maris Cepuritis and Austeris Keiss, "Hostile Narratives and their Impact…", 20.

39 Chris Wattie, "Bringing a Knife to a Gun Fight…", 58

conduct information operations and strategic communications is hampered by level of capabilities and emphasis placed on information domain enablers.[40] When compared to Canada's allies, there is a lack of emphasis and doctrine on StratCom despite mention of investments and importance in Canada's defence policy: *Strong, Secure, Engaged*.[41]

Canadian doctrine states the necessity to include information operations into the joint targeting process.[42]This process will enhance kinetic engagements or negate the need for them.[43]The joint targeting process is used to assign effects to targets and execute them to achieve the commander's objectives and end-states.[44] This was utilized for the employment of kinetic effects in Iraq during the early years of Operation IMPACT by Canadian forces.[45] Although non-kinetic effects can be assigned to targets, training and understanding of the targeting process does not make this readily apparent as a focus on conventional, kinetic effects in current planning processes, especially in Latvia.[46]Information operations can achieve the effects to deter an adversary's will to act and attack an adversary's power base to deny them the initiative.[47] In the case of Latvia, constant and accurate messaging and counter-messaging will aid in cementing the support of the local population and turn the tide against pro-Russian entities, thus eroding these entities' initiative in the information domain.

---

40 Ibid., 59-60.

41 Canada, Department of National Defence, *Strong, Secure, Engaged: Canada's Defence Policy.* (Ottawa, ON: 2017), 41. *Strong, Secure and Engaged* is Canada's Defence Policy document. This document outlines investment in joint capabilities, of which information operations capabilities form part.

42 Canada, Department of National Defence, CFJP 3-10 Information Operations, (Ottawa, ON: Joint Doctrine Branch, 2015), 3-4

43 ABCA, *Influence Activities Handbook,* (ABCA Publication 372, 2013), 1-5.

44 Canada, Department of National Defence, *CFJP 3-9 Targeting*, (Ottawa, ON: Joint Doctrine Branch, 2014), 1-1.

45 Canada. Department of National Defence. *Operation Impact*, accessed at https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-impact.html, last updated 21 May 2021.

46 Chris Wattie, "Bringing a Knife to a Gun Fight…", 59-60.

47 Canada, Department of National Defence, *CFJP 3-10 Information Operations*…, 1-6.

COUNTERING INFORMATION DOMAIN THREATS

Given the multitude of hybrid threats in the information domain, there are many methods to counteract hostile narratives and regain the initiative. These methods to counter hostile narratives are investing in currently deployed Information Operations cells, developing a more robust Whole of Government approach to counter hostile narratives, and the training of CAF soldiers in the information domain. Where Operation REASSURANCE is concerned, significant investment in terms of capital and personnel into the StratCom cell will enable future operations in this domain. Through this, analysis tools can be developed to detect adversarial messaging and propaganda and enable information operations staff to enact counter messaging and assess measures of performance and effectiveness.[48] Effective strategic communications is necessary to mitigate strategic compression and ensure credibility of Canada's deployed forces and objectives. As information operations act below the threshold of conflict, it is difficult to discern responsibility for deterrence or management, as hybrid threats "exploit the seams of responsibility between the armed forces and civilian agencies."[49] To this end, a Whole of Government approach must be embraced to counter threats in the information domain. As many agencies have capabilities to verify information and determine fact from falsehood, this will enable the credibility of Canada and its participation in international operations such as Operation REASSURANCE. To regain the initiative in this domain, Canada must be capable of focusing on the deceit behind the messaging and indicate that users "have been taken as fools by Russia, rather than engaging in dry and detailed explanations of how it was done."[50] Regarding training, it is imperative that the CAF embraces the understanding of the information domain.[51]

---

48 Chris Wattie, "Bringing a Knife to a Gun Fight…", 61-62.

49 Keir Giles and Anthony Seaboyer, *The Russian Information Warfare Construct*…, 21.

50 Ibid., 21-22.

51 Canada. HQ, Canadian Army, *Advancing With Purpose: The Canadian Army Modernization Strategy, 4th Edition*, (Ottawa, ON: December 2020), 52.

Given that information is wielded as a weapon, tactical actions can be exploited to make strategic consequences.[52] This understanding of the information domain can begin at the tactical level formation training, specifically the Developmental Period 2 (DP 2) area. Canadian Army courses like the Army Tactical Operations Course (ATOC), and especially the Army Operations Course (AOC) should incorporate topics on information operations and their importance on tactical level decisions.[53]

CONCLUSION

To deter the emerging threat in the information domain, Canada and its allies must out-manoeuvre adversarial actions in this domain. As Canada is a part of a strong conventional alliance, adversaries will seek to discredit Canada and other allies by driving a wedge in between allies or by simply influencing the will and perceptions of the population. Adversarial entities have used information operations to influence key stakeholders in targeted states, which enabled success in areas like Crimea. In order to disrupt hybrid threats and irregular tactics in the information domain, legitimacy amongst the population is paramount. This can be achieved by discrediting adversarial messaging and getting ahead of the curve to seize and retain the initiative in the information domain. Drawing on examples like Lithuania's StratCom, Canada can ensure that dominance in the information domain can be achieved, at the very least, by maintaining legitimacy of our population and those of the host nation in which we are conducting operations. As the world increasingly values information to shape perceptions and decisions it is becoming a vital resource that can be exploited by those who wish to do Canada harm. As information has

---

[52] LGen Mike Rouleau, "How We Fight: Commander CJOC's Thoughts", (Ottawa: Canadian Joint Operations Command, 10 Feb 19), 6

[53] Canada, Department of National Defence, *CFJP 3-10 Information Operations*…, 4-1 – 4-2. CAF Joint Doctrine mentions the necessity of integrating information operations into exercises. Though the information operations policy mentions a requirement for specialized individual training courses for staff, it does mention the general requirement to train all staff in a basic understanding of information operations.

become both a currency and a weapon, it is important that commanders and staff view the information domain as important as key terrain and vital ground in the conduct of operations.

BIBLIOGRAPHY

ABCA. *Influence Activities Handbook.* ABCA Publication 372, 2013.

Armistead, Edwin and Scott Starsman. "Perception Shaping and Cyber Macht: Russia and Ukraine." *International Conference on Cyber Warfare and Security* (2015): 14-19.

Canada. Department of National Defence. *B-GG-004-005/AF-010, CF Information Operations*. Ottawa, ON: Joint Doctrine Branch, 1998.

Canada. Department of National Defence. *CFJP 3-10 Information Operations*. Ottawa, ON: Joint Doctrine Branch, 2015.

Canada. Department of National Defence. *CFJP 3-9 Targeting*. Ottawa, ON: Joint Doctrine Branch, 2014.

Canada. Department of National Defence. *Operation Impact*, accessed at https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-impact.html, last updated 21 May 2021.

Canada, Department of National Defence, "Operation REASSURANCE", https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-reassurance.html, last updated 20 May 2021.

Canada. HQ, Canadian Army. *Advancing With Purpose: The Canadian Army Modernization Strategy, 4th Edition*. Ottawa, ON: December 2020.

Cepuritis, Maris and Austeris Keiss. "Hostile Narratives and their Impact: The Case of Latvia." *Russia's Footprint in the Nordic-Baltic Information Environment, Report 2019/2020*. Riga, Latvia: NATO Strategic Communications Centre of Excellence, November 2020.

Connable, Ben, Stephanie Young, et al. "Russia's Hostile Measures: Combating Russian Gray Zone Aggression Against NATO in the Contact, Blunt, and Surge Layers of Competition". *RAND Corporation*. Santa Monica, CA: 2020.

Geigerich, Bastian. "Hybrid Warfare and the Changing Character of Conflict." *Connections: The Quarterly Journal 15*, no. 2 (Spring 2016): 65-72.

Giles,Keir and Anthony Seaboyer. *The Russian Information Warfare Construct*. Toronto, ON: DRDC, March 2019.

Helmus, Todd C., Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman. *Russian Social Media Influence — Understanding Russian Propoganda in Eastern Europe*. Santa Monica, CA: RAND Corporation, 2018.

Idzelis, Lieutenant Colonel Linas. "Leveraging StratCom." *Special Warfare Vol 32,* Issue 3. (July-December 2019).

Karlsen, Geir Hågen. "Tools of Russian Influence: Information and Propaganda." In *Ukraine and Beyond: Russia's Strategic Security Challenge to Europe*, edited by Janne Haaland Matlary and Tormod Heier, 181-208. Cham: Palgrave Macmillan, 2016.

MacKinnon, Mark. "For many in Latvia's Russified east, Canada's 'Operation Reassurance' is anything but." *The Globe and Mail*. Toronto, ON: 15 April, 2017.

Monaghan, Sean. "Countering Hybrid Warfare: So What for the Future Joint Force?" *Prism 8*, no. 2 (4 October 2019): 95-103.

Moore, Dr. Cerwyn. "Russian Disinformation: The Case of Ukraine." Centre for Research and Evidence on Security Threats, March 2019.

North Atlantic Treaty Organization, "NATO's Enhanced Forward Presence", https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/2103-factsheet_efp_en.pdf, March 2021.

Svetoka, Sanda. *Social Media as a Tool of Hybrid Warfare*. Riga, Latvia: NATO StratCom COE, May 2016.

Roberts, James Q. "Maskirovka 2.0: Hybrid Threat, Hybrid Response". *Joint Special Operations University Centre for Special Operations Studies and Research*. December 2015.

Rodriguez, Belen Carrasco. *Information Laundering in the Nordic-Baltic Region*. Riga, Latvia: NATO StratCom COE, November 2020.

Rouleau, LGen Mike. "How We Fight: Commander CJOC's Thoughts." Ottawa: Canadian Joint Operations Command, 10 Feb 19.

Ruston, Scott. "Narrative & Strategic Communications." In *Russia's Footprint in the Nordic-Baltic Information Environment, Report 2019/2020*. Riga, Latvia: NATO Strategic Communications Centre of Excellence, November 2020.

Sanger, David E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York, NY: Broadway Books, 2018.

United States. Department of Defense. *Joint Publication 3-13 Information Operations*. Washington, D.C.: February 2006.

United Kingdom. Ministry of Defence. *Joint Doctrine Note 1/12 Strategic Communication: The Defence contribution.* Swindon, UK: Development, Concepts and Doctrine Centre, January 2012.

Wattie, Chris. "Bringing a Knife to a Gun Fight: Canadian Strategic Communications and Information Operations in Latvia, Operation REASSURANCE 2019-2020" *Canadian Military Journal Vol. 21*, No. 1 (Winter 2020): 55-62.