





THE LITHUANIAN APPROACH TO MILITARY STRATEGIC COMMUNICATIONS TO COUNTER THREATS IN THE INFORMATION ENVIRONMENT: A MODEL FOR THE CAF?

Lieutenant-Commander J. Bruno Tremblay

JCSP 47

Service Paper

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2021.

PCEMI 47

Étude militaire

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2021.



CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 47 - PCEMI 47 2020 - 2021

SERVICE PAPER – ÉTUDE MILITAIRE

THE LITHUANIAN APPROACH TO STRATCOM TO COUNTER THREATS IN THE INFORMATION ENVIRONMENT: A MODEL FOR THE CAF?

By Lieutenant-Commander J. Bruno Tremblay

"This paper was written by a candidate attending the Canadian Forces College in fulfillment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

Word Count: 2,413

« La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »

Nombre de mots : 2.413

THE LITHUANIAN APPROACH TO STRATCOM TO COUNTER THREATS IN THE INFORMATION ENVIRONMENT: A MODEL FOR THE CAF?

AIM

1. This paper aims at assessing whether or not the Lithuanian approach to Military Strategic Communications (StratCom) could be adopted by the Canadian Armed Forces (CAF) and if so, at what level (tactical, operational, strategic), what conditions would have to be in place and what would be the components of a similar CAF StratCom capability.

INTRODUCTION

2. Over the past decade, Western nations have been routinely facing challenges regarding the spread of information disorder – whether misinformation, disinformation and malinformation – in their domestic information environment (IE)¹. In face of this growing threat, some nations have boosted their cognitive security capabilities, including the development of StratCom capabilities². Amongst the nations is Lithuania who has established StratCom Divisions³ across its governmental and military apparatus to counter Russian hostile narrative in its IE. At the military level, the Lithuanian Armed Forces (LAF) Military StratCom Division works actively with the other governmental and civilian StratCom agencies to foster resilience and resistance in face of the Russian threat⁴.

¹ The threat posed by information in an interconnect world bears many names: fake news, misinformation, disinformation, weaponization of information, manipulation of information, propaganda, and more. This paper favours the taxonomy proposed by Wardle and Derakhshan where *misinformation* means the unintentional spread of false information without the intent of causing harm, *disinformation* the deliberate and intentional spread of false information intending to harm or discredit a person, a group, an organization or a country, and *malinformation* the strategic use of factual information to cause harm, again either a person, a group, an organization or a country. These three malign uses of information are best regrouped under the term "information disorder". See C. Wardle, and H. Derakhshan. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making.* Report DGI(2017)09, 19.

² The term "cognitive security" refers to the act of "securitizing social cognition", that is "the ability of a population to make informed decisions based on accurate, corroborable and trusted information, ensuring self-determination, accountable representation, and healthy public deliberation". See Bruno Tremblay, *Democracy Under Attack: The Threat of Information Disorder*, Joint Command and Staff Program, Canadian Forces College (2020), 3.

³ The term "division" refers to a department within the LAF. It is not to be confuse with the army definition.

⁴ Linas Idzelis, "Leveraging StratCom: The Importance of Strategic Communications and How it is Implemented in the Lithuanian Armed Forces", *Special Warfare*, vol. 32, no. 3, (July-December 2019), 38; Jonas Mindaugas, "A History of Resilience", *Special Warfare*, vol. 32, no. 3, (July-December 2019), 28; Lithuania Special Forces. "Si Vis Paceum, Para Bellum: 'If You Want Peace, Prepare for War", *Special Warfare*, vol. 32, no. 3, (July-December 2019), 36; Lukas Andriukaitis, *International Partner's Lessons Learned on Building Resilience (Lithuanian Case)*, DRDC/Canadian Heritage/RMCC Virtual Symposium (16 September 2020).

3. Canada's IE is also marked by an increasing presence of information disorder, albeit from a different nature⁵. Contra to Lithuania, however, Canada has yet to take concrete measures to bolster its civilian and military capabilities to fight in the information domain.

DISCUSSION

Lithuania's Response to Information Disorder

- 4. As a Baltic state, Lithuania has a long history of conflict with Russia, both in the physical and cognitive domains⁶. Since Lithuania has joined NATO in 2004, the country has been the target of relentless and increasing informational and psychological attacks, mainly in the form of *disinformation*⁷. Analysts believe that Russia's intent behind these attacks is to compel Lithuanian decision-makers to act in favour of Russia by altering their perceptions of the world, especially their views on Russia; a strategy referred to as "Reflexive Control".
- 5. The Russian threat is not only cognitive: it is also physical. Indeed, considering that cognitive warfare and information confrontation is the precursor to a military phase in Russian's playbook, the Lithuanian Government considers very likely a potential territorial invasion by Russian forces to either secure better access to the Baltic Sea or disrupt NATO's centre of gravity: the cohesion of its members⁹. As such, countering disinformation in Lithuania has become a critical task not only for its Armed Forces but also for the whole Lithuanian society. From the Lithuanians' perspective, fighting Russia in the IE is a question of survival; it represents the opportunity "for every civilian to be a part of the nation's defence" 10.
- 6. It is in this context that the Government of Lithuania created a few years ago an "anti-disinfo environment strategy" which includes the active participation of

⁵ DRDC/DCI/RMC. Virtual Symposium: Building Resilience Against Disinformation – The Role of Government (16 September 2020).

⁶ Janice Burton, "A Legacy of Resistance", *Special Warfare*, vol. 32, no. 3, (July-December 2019), 12; Jonas Mindaugas, "A History of Resilience".... 28.

⁷ Linas Idzelis, "Leveraging StratCom: The Importance of Strategic Communications and How it is Implemented in the Lithuanian Armed Forces"..., 38; Jonas Mindaugas, "A History of Resilience"..., 28; Lithuania Special Forces. "Si Vis Paceum, Para Bellum: 'If You Want Peace, Prepare for War"..., 36; Lukas Andriukaitis, *International Partner's Lessons Learned on Building Resilience (Lithuanian Case)*.

⁸ François Du Cluzel, *Cognitive Warfare* (NATO Innovation Hub, June-November 2020), 26; Linas Idzelis, "Leveraging StratCom: The Importance of Strategic Communications and How it is Implemented in the Lithuanian Armed Forces"..., 39-40.

⁹ Valery Gerasimov, "The Value of Science is in the Foresight", *Military Review*, vol. 96, no. 1 (January 2016), 28; François Du Cluzel, *Cognitive Warfare* (NATO Innovation Hub, June-November 2020), 26; Linas Idzelis, "Leveraging StratCom: The Importance of Strategic Communications and How it is Implemented in the Lithuanian Armed Forces"..., 38-40.

Jonas Mindaugas, "A History of Resilience"..., 28; Lithuania Special Forces. "Si Vis Paceum, Para Bellum: 'If You Want Peace, Prepare for War"..., 36; Sinevičienė, Luka. "The Whole-of-Society Approach", Special Warfare, vol. 32, no. 3, (July-December 2019), 30.

governmental, civil society and media organizations¹¹. At the governmental level, Lithuania created three StratCom divisions, one within the Ministry of Foreign Affairs, one within the Ministry of Defence (MoD) and one within the LAF. The latter, called LAF Military StratCom Division (LMSD), is tasked to fight Russian narratives in the Lithuanian IE, trying to win narrative superiority by planning and executing different communication campaigns and activities as well as resilience programs ¹². The LMSD is purposed-build for the task. It is divided into four separate sections, which are closely interrelated and work in coordination: IE Assessment (IEA), Military Public Affairs (MPA), Information and Psychological Operations (Info Ops) and Citizenship Education (also called Engagement)¹³. As illustrated in Figure 1, the LMSD is located within the LAF at the military-strategic level (L0 in Canadian parlance) but works closely with all levels of command to ensure the overall coherence of actions and messaging across the LAF¹⁴. Below the strategic level, different capabilities are present at different levels of war. For instance, MPA is present at all levels, Info Ops only at the operational level, and PsyOps only at the tactical level¹⁵. The LMSD favours the "mission command" philosophy where operations are centrally coordinated and de-centrally executed 16. It is worth noting as well that the Lithuanian IE is considered as a lawful theatre of operations by the LAF and the Lithuanian people.

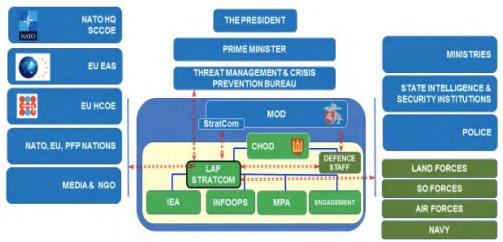


Figure 1 – LAF StratCom Composition and Structure

Source: Algirdas Mackonis, *Lithuanian Armed Forces Strategic Communications Division – A Summary*. Provided to LCdr Bruno Tremblay on 29 January 2021.

¹¹ Lukas Andriukaitis, *International Partner's Lessons Learned on Building Resilience (Lithuanian Case)*...

¹² Linas Idzelis, "Leveraging StratCom: The Importance of Strategic Communications and How it is Implemented in the Lithuanian Armed Forces"..., 40-42; Algirdas Mackonis, *Lithuanian Armed Forces Strategic Communications Division – A Summary...*, 1-2.

¹³ It is worth mentioning here that Lithuania adheres to NATO's understanding of StratCom where all information-related capabilities (IRCs) and staff functions (Public Diplomacy, Public Affairs, Military Public Affairs, Psychological Operations, and Information Operations) are integrated under one chain of command. See NATO. *NATO Military Policy on Strategic Communications* (Belgium: Supreme Headquarters Allied Powers Europe, 2017), 4.

Algirdas Mackonis, Lithuanian Armed Forces Strategic Communications Division – A Summary..., 1.
Ibid.

¹⁶ *Ibid*, 4.

- 7. Each section of the LMSD brings a different capacity to the unit. The MPA section is responsible for shaping positive public opinion by planning, coordinating and executing public affairs campaigns and activities across the LAF. The IEA section monitors and assesses Hostile StratCom activities in the Lithuanian IE, and provide timely and accurate situational awareness to the LAF leadership to inform potential responses. The Citizenship Education section works to ensure the long-term prevention and public resilience in dealing with hostile information threats. Finally, the Info Ops section plans and implements various information operations plans and strategies for the MoD and the LAF, and supports other governmental authorities in dealing with information threats¹⁷.
- 8. Finally, the LMSD staff consists mostly of military personnel coming from the field of intelligence, military public affairs, information operations, and psychological operations, supported by civilian staff from other fields such as social sciences, translation and information technologies¹⁸.

Canada's Response to Information Disorder

- 9. The nature and scale of information disorder in Canada are quite different. First, the most significant threats in the Canadian IE have more to do with *misinformation* and *malinformation* than foreign-based disinformation¹⁹. The latter does occur, but at a smaller scale and less frequently than the two other forms of information disorder²⁰. For instance, it was reported that the 2019 federal election has been "largely clean" of disinformation attempts compared to other Western nations²¹. Second, as discussed in the 2019 Annual Report of the National Security and Intelligence Committee of Parliamentarians, the nature of foreign influence or interference in Canada is rather a matter of person-to-person interference than IE or cyber-based²².
- 10. Overall, Canada's response to information disorder could be characterized as being *ad hoc* and uncoordinated. Truth to be told, the Government of Canada has yet to officially recognize information disorder as a tangible threat to national security²³. While

¹⁷ Linas Idzelis, "Leveraging StratCom: The Importance of Strategic Communications and How it is Implemented in the Lithuanian Armed Forces"..., 40-43.

¹⁸ *Ibid.*, 42.

¹⁹ DRDC/DCI/RMC. Virtual Symposium: Building Resilience Against Disinformation – The Role of Government (16 September 2020).

²⁰ National Security and Intelligence Committee of Parliamentarians, *Annual Report 2019* (Ottawa: Her Majesty the Queen in Right of Canada, 2020), 55-56.

²¹ The Canadian Press. "So far, federal election has had little misinformation or disinformation: researchers", *National Post* (10 October 2019), https://nationalpost.com/news/politics/election-2019/election-has-been-mostly-free-of-mis-and-disinformation-research-shows?r

²² National Security and Intelligence Committee of Parliamentarians, *Annual Report 2019...*, 55-56.

²³ While the 2017 Defence Policy characterized the use of information to affect or disrupt Canada's domestic affairs as a "vulnerability", there is no reference to information-based threat in Canada's National Security portfolio. See Government of Canada, *National Security*. Last modified 26 November 2020. https://www.canada.ca/en/services/defence/nationalsecurity.html Government of Canada, *Strong. Secure. Engaged, Canada's Defence Policy* (Ottawa, 2017), 49.

several governmental departments, agencies, private and civilian organizations have taken initiatives to address misinformation issues in Canada, there is no governmental-wide plan to counter the threat with force, even less a whole-of-society strategy²⁴. Additionally, Canada possesses no concept for StratCom has a cognitive capability, civilian or military, NATO or others.

11. On the military front, the CAF has no legal jurisdiction with regards to protecting Canadians' social cognition. Within Defence, the only organization authorized to act in the Canadian IE is the civilian-led Assisting Deputy Minister (Public Affairs), sitting on the civilian-side of the Department of National Defence (DND), not the military-side (CAF). Furthermore, ADM (PA)'s mandate is tightly restricted to solely informing Canadians about defence projects, activities, priorities, and policies²⁵. It has no responsibility to plan and execute cognitive operations on the domestic front. On the CAF side, no organization has been mandated to act against hostile actions in the IE. As such, the sole role of the military in fighting information disorder, like any other government department, is limited to two aspects: countering potential misinformation about military activities in accordance with ADM PA's guidance and building CAF members' resilience against information disorder.

Comparative Analysis

12. When comparing Lithuania and Canada's cases, it is evident that the Lithuanian approach to fighting information disorder would be very difficult to implement in Canada. Firstly, the strategic culture in Canada is rebarbative to any form of influence from the CAF on the domestic front; simple rumours of military activities made to influence Canadians turn into political headaches. The October 2020 outcry in the media about the alleged conduct of an information operations campaign in Canada by the CAF is a prime example of that harsh reality²⁶. Contrary to Lithuanians, Canadians do not perceive their IE to be a valid military theatre of operations. If it is appropriate for the CAF to act in the physical domains (land, aerospace and territorial waters), it is not in the information domain. In other words, Canadians accept that civilian and military Public Affairs Staff communicates to them factual information about the CAF, but refuse that the military acts beyond the basic democratic necessity of informing the population. There is

²⁴ For examples, the Canadian Security Intelligence Service now routinely sends awareness messages about disinformation and misinformation. Heritage Canada has created the *Digital Citizen Initiative* to sponsor numerous public and private initiatives that aims at countering online misinformation and increasing digital awareness online. Radio-Canada's special investigation team, les Décrypteurs, regularly publishes stories about information disorder and its related issues. Canadian Security Intelligence Service's Twitter page; Heritage Canada, *Digital Citizen Initiative*. Last modified on 12 August 2020. https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html; Société de Radio-Canada, *Les Décrypteurs*. No Date, https://ici.radio-canada.ca/decrypteurs.

²⁵ National Defence Headquarters. *Assisting Deputy Minister (Public Affairs) Mandate*. 3 March 2020. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/defence-101/2020/03/defence-101/adm-pa.html

²⁶ David Scanlon, "Fight the Information War Without Sacrificing Canadian Values", Defence Watch, *Ottawa Citizen*. Last modified on 27 October 2020. https://ottawacitizen.com/news/national/defence-watch/fight-the-information-war-without-sacrificing-canadian-values?

no indication that the strategic culture in Canada would change in that regard, unless a significant incident happens, such as an imminent physical threat to Canada's territory, which, let's face it, is very unlikely.

- 13. In Lithuania, the strategic culture is otherwise. The history of the Baltic States is one of relentless invasions²⁷. As a result, Lithuanians strongly believe in defence both territorial and cognitive. Furthermore, beyond the actions of the Armed Forces in all domains, Lithuanians also believe that every citizen has a role to play in defending their nation's rights. As the US Special Operations Forces Command Europe has observed, "Resistance is not theoretical in the Baltics, [it] is ingrained in the DNA of the people in the Baltics, [it] is a way of life for the people in these countries"²⁸. In this context, not only the Lithuanians do understand that the cognitive fight in the IE against Russia is essential to the nation's survival, but they also actively participated in it²⁹.
- This brings up the second reason why the LAF StratCom framework would be difficult to implement in Canada: considering the strategic culture in Canada, the nature of the threat and the security context is not perceived as serious enough to justify the creation of a similar capability. Of all the three forms of information disorder, disinformation is the least concerning to Canadians while being the main one for Lithuanians. Additionally, Canada does not fear a land invasion from a neighbouring country and is located way outside the area of influence of the main users of hybrid tactics (namely Russia, China, North Korea, and Iran³⁰) to be overly concerned by information confrontation being the precursor of a military phase. On this point, studies have demonstrated that hybrid tactics must meet very specific conditions to show any tangible result: (1) the belligerent must have local escalation dominance; (2) he must seek to revise the status quo; (3) the targeted state must be perceived as a weaker state with local ethnic or linguistic cleavages that can be exploited; and (4) this state must have ethnic and/or linguistic ties to the belligerent³¹. As such, information attacks against Canada have limited effects and serve mostly as attempts to disrupt NATO's political cohesion.
- 15. As illustrated at Figure 2, the creation of a military StratCom capability in Canada would need to meet certain conditions. While these conditions are present in Lithuania, they are not in Canada, at least not for now. In other words, considering Canada's strategic culture, the lack of physical threat to Canada does not support the creation of an active military StratCom capability to *act* in the Canadian IE like it is for Lithuania.

6/10

²⁷ Janice Burton, "A Legacy of Resistance"..., 12; Nick B. Israel, "Resistance, Resilience and Everyday Citizens as an Element of National Power", *Special Warfare*, vol. 32, no. 3, (July-December 2019), 22-23.

²⁸ Janice Burton, "A Legacy of Resistance"..., 12; Jonas Mindaugas, "A History of Resilience"..., 28-29.

²⁹ Lukas Andriukaitis, *International Partner's Lessons Learned on Building Resilience (Lithuanian Case)...*

³⁰ NATO Strategic Communications Centre of Excellence. *Hybrid Threats: A Strategic Communications Perspective*, Riga (2019), 14-16.

³¹ Alexander Lanoszka, "Russian hybrid warfare and extended deterrence in eastern Europe", *International Affairs*, vol. 92, no. 1 (2016), 176.

Conditions to be met	Lithuania / LAF	Canada / CAF
Presence of physical threats to the state survival	Yes	No
Presence of Information Confrontation in the IE	Yes	Limited
Information disorder being considered as a threat	Yes	No
to national security		
Possess clear concepts and definitions for	Yes	No
StratCom and related capabilities and functions		
Whole-of-society strategy to counter information	Yes	No
disorder		
Strategic culture is supportive of the military	Yes	No
actions in the cognitive domain		
Domestic IE is considered being a lawful	Yes	No
military theatre of operations		
Military officially mandated to monitor, assess	Yes	No
and act in the domestic IE		

 $\label{eq:Figure 2-Summary of the conditions needed} \ to \ justify \ the \ creation \ of \ a \ military \ StratCom \ Capability$

Source: Author's representation.

- 16. While the LAF model is not a good fit for CAF as is, it does not mean that Canada could not develop its own StratCom model, one that better fits its strategic culture, using parts of it. First of all, a domestic Canadian Military StratCom capability would be strictly limited in terms of capabilities. Its core tasks would more likely be (1) IE Assessment, (2) Narrative Design and Management, (3) MPA, and (4) coordination of Cognitive Effects within the CAF.
- 17. Second, like in Lithuania, and contrary to what others have recommended³², a Canadian Military StratCom capability would be best located within the military-strategic level (L0 or Strategic Joint Staff [SJS]). This is where it would be the most effective in coordinating CAF efforts in the cognitive domain in coordination with ADM PA and other federal departments and agencies. This would not preclude having a Military StratCom capability at the operational level, regrouping all IRCs under one chain of command, but any operational capability would need to be strictly limited to expeditionary operations only, which is easier to be said than done since the Canadian Joint Operations Command (CJOC) is built to operate both domestically and internationally at the same time.
- 18. Finally, for a CAF Military StratCom capability to have "teeth", two other requirements would need to be met. First, on the doctrinal front, the CAF would need to adopt clear definitions for what Military StratCom is and does, including all subordinated capabilities and functions (MPA, IO, PsyOps, and so forth.). The lack of clear doctrine in the cognitive domain right now is, arguably, the most important hindrance to operate in

7/10

³² Krzysztof Stachura. Canadian Joint Operations Command: Canadian Armed Forces Joint Information Operations Operational Authority, Joint Command and Staff Program, Canadian Forces College (2018), 11.

the IE, domestically and expeditionary. Second, the CAF would need to develop the ability to force generate "Military StratComers", including force development, force generation and force employment models for all IRCs. Unfortunately, the recently failed enterprise to modernize the Public Affairs Branch has shown limited appetite in the CAF for such endeavour.

CONCLUSION

- 19. By comparing both Lithuania's and Canada's security and social contexts, the nature of the threats they are facing in the IE, and their strategic culture, this paper concludes that the LAF approach to Military StratCom is not a model that can be adopted by the CAF as is. First, the level of threat faced in the IE is not high enough to justify having the CAF monitor, assess and more importantly act in the IE as the LAF does. In this context, the CAF has no mandate to do so. Second, Canadians do not believe that the IE is a valid domestic theatre of operations and would more likely strongly object that such a mandate be given to the military.
- 20. It does not mean that CAF should not do more to better respond to cognitive threats, but the solution would not be found in mimicking Lithuania's framework. The solution would have to be more aligned on the Canadian strategic culture and within the current DND structure and frameworks.

RECOMMENDATIONS

- 21. As for the matter concerned by this paper, it is NOT recommended that the CAF adopt the LAF military StratCom approach as is.
- 22. Nonetheless, if the CAF desires to become a more relevant and agile actor in the domestic IE, providing new capabilities to the Government of Canada, it is recommended that the CAF:
 - a. Officially adopts the NATO Policy regarding Military Strategic Communications;
 - b. Endeavours once for all to develop clear doctrines, definitions, concepts and procedures for all CAF IRCs (StratCom, PA, MPA, PsyOps, IO, Civil-Military Cooperation, Electronic Warfare, and Cyber);
 - c. Establish a Military StratCom Section within SJS, as described in this paper; and
 - d. Create military occupations for all CAF IRCs.

BIBLIOGRAPHY

- Andriukaitis, Lukas. *International Partner's Lessons Learned on Building Resilience* (*Lithuanian Case*), DRDC/Canadian Heritage/RMCC Virtual Symposium (16 September 2020).
- Burton, Janice. "A Legacy of Resistance", *Special Warfare*, vol. 32, no. 3, (July-December 2019): 12-13.
- Canada. Government of Canada, *National Security*. Last modified 26 November 2020. https://www.canada.ca/en/services/defence/nationalsecurity.html
- Canada. Government of Canada, *Strong. Secure. Engaged, Canada's Defence Policy*, Ottawa (2017).
- Canada. Canadian Security Intelligence Service's Twitter page, https://twitter.com/csiscanada?lang=eng
- Canada. Heritage Canada. *Digital Citizen Initiative*. Last modified on 12 August 2020. https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html
- Canada. National Security and Intelligence Committee of Parliamentarians. *Annual Report 2019*, Ottawa: Her Majesty the Queen in Right of Canada (2020).
- Canada. National Defence Headquarters. *Assisting Deputy Minister (Public Affairs) Mandate*. 3 March 2020. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/defence-101/2020/03/defence-101/adm-pa.html
- DRDC/DCI/RMC. Symposium: Building Resilience Against Disinformation The Role of Government (16 September 2020).
- Du Cluzel, François. Cognitive Warfare, NATO Innovation Hub (June-November 2020).
- Idzelis, Linas. "Leveraging StratCom: The Importance of Strategic Communications and How it is Implemented in the Lithuanian Armed Forces", *Special Warfare*, vol. 32, no. 3, (July-December 2019): 38-43.
- Israel, Nick B. "Resistance, Resilience and Everyday Citizens as an Element of National Power", *Special Warfare*, vol. 32, no. 3, (July-December 2019): 22-25.
- Hybrid Threats: A Strategic Communications Perspective, Riga: NATO Strategic Communications Centre of Excellence (2019).
- Lanoszka, Alexander. "Russian hybrid warfare and extended deterrence in eastern Europe", International Affairs, vol. 92, no. 1 (2016): 175–195.

- Layti, Mark. Public Affairs Working Group, Rome, September 2017.
- Lithuania Special Forces. "Si Vis Paceum, Para Bellum: 'If You Want Peace, Prepare for War", *Special Warfare*, vol. 32, no. 3, (July-December 2019): 36-37.
- Mackonis, Algirdas. *Lithuanian Armed Forces Strategic Communications Division A Summary*. Provided to LCdr Bruno Tremblay on 29 January 2021.
- Mindaugas, Jonas. "A History of Resilience", *Special Warfare*, vol. 32, no. 3, (July-December 2019): 27-29.
- NATO. *NATO Military Policy on Strategic Communications*, Belgium: Supreme Headquarters Allied Powers Europe (2017).
- NATO Strategic Communications Centre of Excellence. *Hybrid Threats: A Strategic Communications Perspective*, Riga (2019).
- Scanlon, David, "Fight the Information War Without Sacrificing Canadian Values", Defence Watch, *Ottawa Citizen*. Last modified on 27 October 2020. https://ottawacitizen.com/news/national/defence-watch/fight-the-information-war-without-sacrificing-canadian-values
- Société de Radio-Canada, *Les Décrypteurs*. No Date, https://ici.radio-canada.ca/decrypteurs
- Sinevičienė, Luka. "The Whole-of-Society Approach", *Special Warfare*, vol. 32, no. 3, (July-December 2019): 30-31.
- Stachura, Krzysztof. Canadian Joint Operations Command: Canadian Armed Forces Joint Information Operations Operational Authority, Joint Command and Staff Program, Canadian Forces College (2018).
- The Canadian Press. "So far, federal election has had little misinformation or disinformation: researchers", *National Post* (10 October 2019). https://nationalpost.com/news/politics/election-2019/election-has-been-mostly-free-of-mis-and-disinformation-research-shows?
- Tremblay, Bruno. *Democracy Under Attack: The Threat of Information Disorder*, Joint Command and Staff Program, Canadian Forces College (2020).
- Wardle, C., and H. Derakhshan. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Report DGI(2017)09. Strasbourg: Council of Europe (2017). https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c