National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Populism: People Power and the Canadian Armed Forces

Major Jean-François Legault

JCSP 48

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 48

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 48 – PCEMI 48
2021 – 2022

Exercise Solo Flight – Exercice Solo Flight

Populism: People Power and the Canadian Armed Forces

Major Jean-François Legault

"This paper was written by a student attending the Canadian Forces College in fulfilment 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."

"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."

INTRODUCTION

Information has been an instrument of power since the dawn of humankind. Control of it was and is still essential to gaining power and maintaining it. For example, a tribe leader who knew how to make fire or where to hunt exerted power over his tribe. As societies developed in more complex organizations, maintaining control over knowledge, information and communication became essential in maintaining order and power. The monumental pyramids are an example of a statement of power and control. Whether the pharaohs did great things for the Egyptians is irrelevant, the monument conveys the information of prosperity, greatness and accomplishment through time.[1] What remained was a testament to power and a reminder to the general population of whom was the leader and who controlled power. In Foucauldian terms knowledge emanates from power but what is knowable is also dictated by power.[2] But what comes first, knowledge or power? This special relation between information and power, highlighted in most of Michel Foucault's work, is at the epicentre of today's battle for power and for what the *right* information is. To gain the upper hand in the information domain everything is permited to gain or maintain power. Whether that power is for good or not.

Because knowledge is one of the building blocks of power, humans easily fall in the trap of corrupting that knowledge in order to gain fame, attention or more. Before the printing press was invented, the earliest trace of information fabrication can be traced back to the "sixth century AD [when] Procopius of Caesarea (500—ca. AD 554), the

[1] Joanna M. Burkhardt, "History of Fake News," *Library Technology Reports* 53, no. 8 (December 2017): 5.

[2] Michel Foucault, "The Subject and Power." *Critical Inquiry* 8, no. 4 (Summer, 1982): 777. https://www.proquest.com/scholarly-journals/subject-power/docview/1297306604/se-2?accountid=9867.

principal historian of Byzantium, used fake news to smear the Emperor Justinian."[3] Procopius probably needed to distance himself from the deceased emperor to gain or maintain a form of power with the new emperor in place. This early example lets us make the probable assumption that falsehood and disinformation have always been part of power building. In the printing press era, the newspaper was the tool of the day to propagate lies, rumours and disinformation, especially for political aspirations. This was an affliction denounced by Jonathan Swift, author of Gulliver's Travels, in this quote of his: "Falsehood flies, and truth comes limping after it, so that when men come to be undeceived, it is too late; the jest is over, and the tale hath had its effect."[4] As mass media was established in the late 19th century, there were multiple accounts of "fake news" that created some commotion. One of the most famous is the fake radio news report based on Orson Welles's "The War of the Worlds" novel in 1938. Even if the novel had been published forty years earlier (1898) and a warning issued before the broadcast, those who tuned in late or were not into science fiction thought that the world was under attack from space-faring aliens. As the technology evolved so did the speed and volume at which information could be transmitted. The Internet created a space where information could be created by almost anyone and available to all the connected souls instantaneously. Because of the sheer amount of available news material[5] and the difficulty to verify all the

[3] "Internet History Sourcebooks Project," accessed May 4, 2022, https://sourcebooks.fordham.edu/basis/procop-anec.asp.

[4] "Issue 14 of 'The Examiner' 9/11/1710," accessed May 4, 2022, https://www.ourcivilisation.com/smartboard/shop/swift/examiner/chap14.htm.

[5] Samuli Laato et al., "What Drives Unverified Information Sharing and Cyberchondria during the COVID-19 Pandemic?," *European Journal of Information Systems* 29, no. 3 (May 3, 2020): 288, https://doi.org/10.1080/0960085X.2020.1770632.

sources, this media environment was perfect for those with the goal of manipulating masses with false information.

The more recent publicization of the term "fake news" was done by the former president Donald J. Trump during his campaign and presidency. His assumed goal was to seed the doubt about *everything* in people's minds in order to assert his power. But what is "fake news"? Throughout the research of the subject, done by scholars of different horizons, the there is a spectrum of definitions to the phenomena. Golbeck et al. defines fake news as "information, presented as a news story that is factually incorrect and designed to deceive."[6] On the other hand, Weis et al. provides a broader and more valuable definition of "fake new" for this essay. They define it as:

> The phenomenon of information exchange between an actor and acted upon that primarily attempts to invalidate generally accepted conceptions of truth for the purpose of altering established power structures. There are a couple of points to consider. First, we believe that this attempt to invalidate what is true can be either intentional (as in the case of misinformation and disinformation) or unwitting (as in the case of mistaken beliefs); and, second, affected power structures can be altered either through subverting them or by fortifying them. In other words, fake news is a double-edged sword, capable of helping or harming established power structures while also being applied to both aggressor and victim.[7]

We note in this definition discernment between *intentional* and *unwitting*. The first type of "fake new" is the one that this essay will be more concerned with because it is directly linked to actors that wish to alter power structures to their advantage, whether internal or external to the state. But we cannot put aside the unwitting spread of "fake news" since

[6] Jennifer Golbeck et al. (2018). Fake news vs satire: A dataset and analysis. In Proceedings of the 10th ACM Conference on Web Science, pp. 17–21

[7] Andrew P. Weiss et al., "Surveying Fake News: Assessing University Faculty's Fragmented Definition of Fake News and Its Impact on Teaching Critical Thinking," *International Journal for Educational Integrity* 16, no. 1 (February 2020), http://dx.doi.org.cfc.idm.oclc.org/10.1007/s40979-019-0049-x.

intentional spread of disinformation is often compounded by throngs of consumers of media that spread it unwittingly either because of information overload,[8] lack of knowledge or simple naiveté. The unwitting masses are the fuel that propels disinformation from nefarious actors and the world's interconnectedness through social media platforms is the lubricant to this *power* altering engines.

The aim of this essay is to argue that the Canadian government needs to shift its paradigm in regards to information warfare in order to remain relevant as a state power to its citizens and to the world. To this end, the essay begins with a review of the notion of power in regards to knowledge and information. Then address the different theories and technologies that compound information manipulation in the Internet era. This will be followed by a review of the successful Lithuanian counter information operation against Russian aggression. In light of this information, the argument will be made that the government of Canada requires a unified communication strategy, legislation in line with this strategy and a revitalization Canada's own media apparatus, the Canadian Broadcasting Corporation and Radio Canada (CBC), in order to offer a beacon of trusted information to Canadians and the world.

POWER, KNOWLEDGE AND INFORMATION

As stated in the introduction, there is a special relation between power, knowledge and information. According to most academics and in a general sense, power is defined as "the ability to affect others to obtain the outcomes you want."[9] In that sense information

[8] Samuli Laato et al., "What Drives Unverified…": 288, https://doi.org/10.1080/0960085X.2020.1770632.
[9] Joseph S. Nye, "Public Diplomacy and Soft Power," *The ANNALS of the American Academy of Political and Social Science* 616, no. 1 (March 1, 2008): 94, https://doi.org/10.1177/0002716207311699.

that is provided or is available to people, organization or states guide their decisions. Thus if the information actor B is provided by actor A forms actor B's knowledge of a situation and pushes it in a direction desired by actor A, then actor A has power through information.

Thus information is a tool that can help actors gain power over others. Joint Publication 1, Doctrine fro the Armed forces of the United States, defines four instruments of national power: diplomatic, informational, military and economic (DIME). Information is a key element as it is both offensive and defensive. It also serves as a coordinating and synchronization element of all the other instruments.[10] But information as an instrument of power is difficult to control as it comes from infinite sources and humans can react differently when subjected to the same information. At the collective level, modifying the actions of an organization becomes that much more difficult unless you control all sources of information, which in our current era is practically impossible.

According to Foucault, the link between power and knowledge is even more elusive.[11] To his account, power flows from everything not just top down in a hierarchical fashion. Our knowledge and relation to our environment create power. For example, the concept of classroom with rows and where the students and teachers are placed physically dictates the relation of power in that space. In addition, Foucault advocates that power creates knowledge and vice versa. Althoug his concept is very philosophical, the important aspect of his theory is that if actor A understands what elements of the environment of actor B provides power and can influence it to his advantage, actor A

[10] Departement of Defense, "Doctrine for the Armed Forces of the United States," *Joint Publication 1*, (July 12, 2017): I-12.
[11] Michel Foucault, "The Subject and Power," *Critical Inquiry* 8, no. 4 (Summer 1982): 777–95.

could possibly highjack the flow of power of actor B. An example of that is the democratic structure of most western states that are particularly vulnerable to the power of public opinion that could be modified through intentional "fake news" as defined in the introduction.

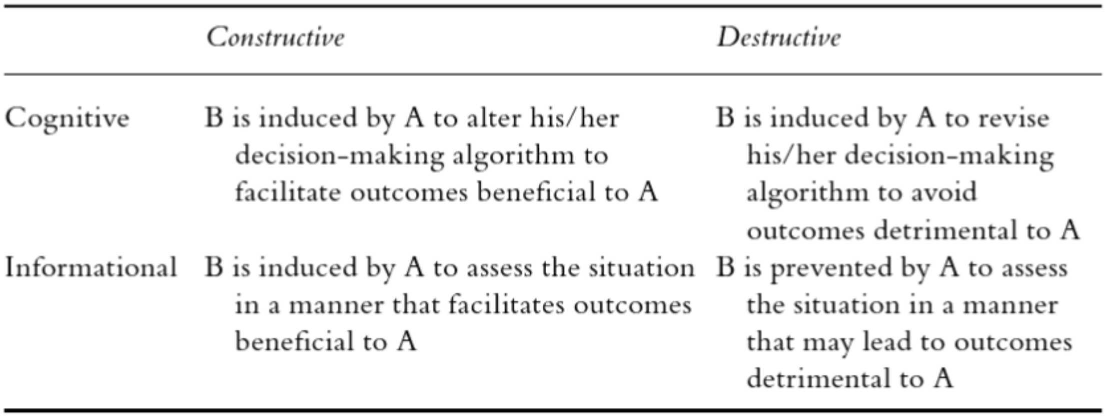
In summary information creates knowledge and define power relations. Information also drives decisions and if information is controlled the right way it is possible to make other act in a desired way even if it's against their interest. Although information is an instrument of power, it is a difficult instrument to wield. But with all the technological advancement and hyper social connectivity of the 21st century we will see that the difficulty level of this instrument of power has been lowered significantly and this threat needs to be addressed to maintain the current power structures in place.

INFORMATION MANIPULATION THEORY AND ENABLING TECHNOLOGIES

As mentioned previously, using information in itself to get an opponent to do something that goes against his interest is erratic and unpredictable. But the latest advances in technology combined with the growing social media use for everyday life makes it possible to sway certain groups. If you combine this with how power flows in democracies, you have a way to attack the foundations of the western states and institutions. Below are some of the elements that help understand what makes this information manipulation possible.

Reflexive Control

Reflexive control (RC) is a doctrine in information warfare that is used by Russian intelligence service. The idea is to prepare and send specially crafted information to a target "to incline him to voluntary make the predetermined decision desired by the initiator of the action."[12] This doctrine is not new and has been in continual refinement. Even if the theory seems simple, the application is not. As mentioned in the previous section information comes from every horizon and people react differently to the same stimulus. Nonetheless this theory is the basis of the disinformation campaign conducted by Russia. RC theory separates in two types of information control, constructive and destructive. As seen in figure 1, Constructive RC seeks to induce the opponent to voluntarily chose an option favourable to the initiator while destructive RC seeks to deny choices detrimental to the initiator.



	Constructive	*Destructive*
Cognitive	B is induced by A to alter his/her decision-making algorithm to facilitate outcomes beneficial to A	B is induced by A to revise his/her decision-making algorithm to avoid outcomes detrimental to A
Informational	B is induced by A to assess the situation in a manner that facilitates outcomes beneficial to A	B is prevented by A to assess the situation in a manner that may lead to outcomes detrimental to A

Figure 1—Processes and Outcomes of Reflexive Control
Source: Bjola, Corneliu, and Pamment, James, eds. Countering Online Propaganda and Extremism: The Dark Side of Digital Diplomacy. Milton: Taylor & Francis Group (2018): 16.

Fortunately, to apply this theory tactically it requires to know the target (target audience) well enough to tailor the information precisely to achieve the manipulation goal. Figure 2 represents the concept graphically. We see that actor "A uses information *i* about B's

[12] TIMOTHY THOMAS, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Military Studies* 17, no. 2 (June 1, 2004): 237, https://doi.org/10.1080/13518040490450529.

cognitive filters and 'weak links' to induce B via information *j* to take decisions in line with A's goals."[13]

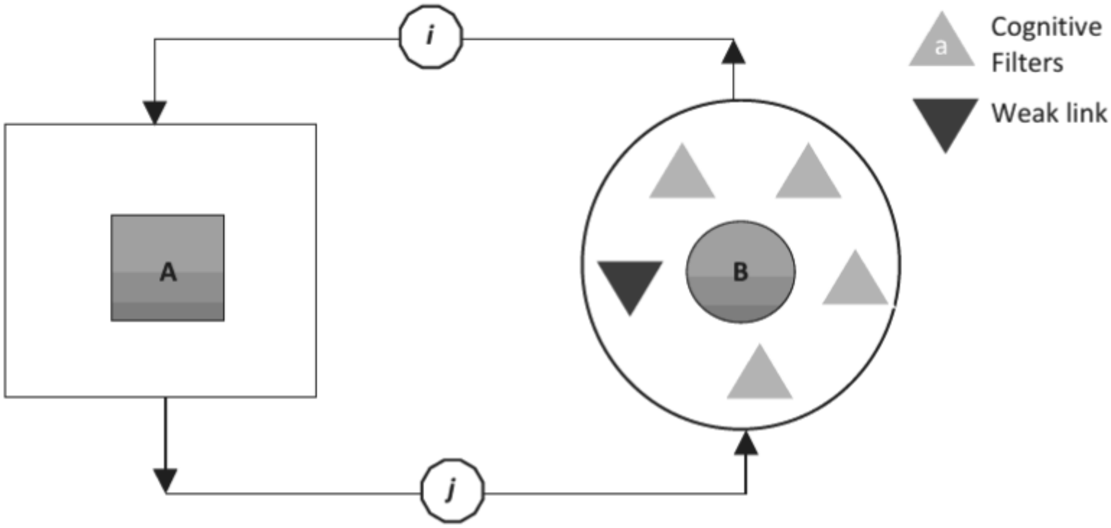


Figure 2—Tactical Model of Reflexive Control
Source: Bjola, Corneliu, and Pamment, James, eds. Countering Online Propaganda and Extremism: The Dark Side of Digital Diplomacy. Milton: Taylor & Francis Group (2018): 18.

RC theory also has to be delivered in a way that does not alert the target that it is being manipulated otherwise the effect can be reversed and the target can develop resilience against further attacks.

In the era of social media, this theory is useful because it can be used to spread specific "fake news" that seeks to take advantage of a weak link in the cognitive filters of a target audience in order to get them to act or think a certain way. For example, if the goal of actor A is to undermine a nations unity and sow division among the population, one of the possibilities would be to take an already pre-existing controversy or point of tension and to blow it out of proportion. This would have an effect of polarizing views

[13] Bjola, Corneliu, and Pamment, James, eds. Countering Online Propaganda and Extremism : The Dark Side of Digital Diplomacy. Milton: Taylor & Francis Group, (2018): 16.

and exacerbate tensions. The use of pre-existing controversy (the weak link in the cognitive filters) gives A a better chance of maintaining the camouflage and preventing the increased resiliency of B.

That being said, this application of RC is not possible without in-depth information on the targets cognitive filters like threads of conversations, networks, demographics and psychographics.[14] And one of the new ways to get this information is through the use of social media big data and artificial intelligence (AI).

Big Data and AI

Populations have become much more connected. From our schedules, daily transits, purchasing habits, browsing history, power consumption and streaming interests, everything is stored online and paints a picture of our digital selves and an extrapolation of our real life. This gigantic amount of data is used every day by AIs to accelerate our searches online, propose new media content that would keep us scrolling, get us to buy things that we didn't know we needed and more.

The most useful tools in AI to find useful information on cognitive filters (and weak points to target) are "unsupervised learning" and "K-mean clustering." "Unsupervised machine learning uses machine learning algorithms to analyze and cluster unlabelled data sets. These algorithms discover hidden patterns or data groupings without the need for human intervention."[15] Hence it can find the common points of a group of digital identities relatively quickly among massive amounts of data. This enables a better

[14] *Ibid*, 20-21.

[15] "What Is Unsupervised Learning?," March 31, 2022, https://www.ibm.com/cloud/learn/unsupervised-learning.

targeting and tailoring of disinformation to be sent. “The K-means algorithm is the most widely used clustering algorithm that uses an explicit distance measure to partition the data set into clusters.”[16] It can represent different elements of a data cluster as a vector and represent networks of people graphically based on different factors as represented in figure 3. This enables nefarious actors to easily visualize groups to target with specific “fake news” that will be effective.

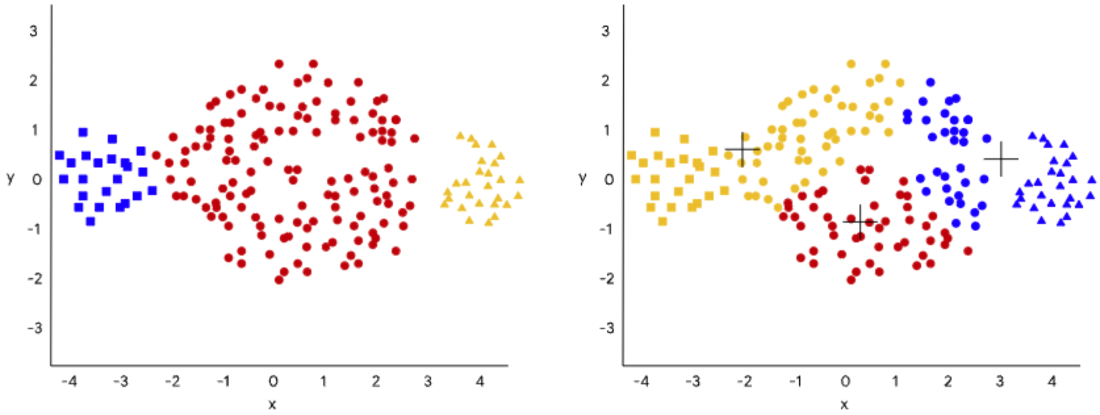


Figure 3—Ungeneralized k-mean example
Source: https://developers.google.com/machine-learning/clustering/algorithm/advantages-disadvantages

Social media

The most important element that enables the propagation of “fake new” is social media. Not only is it a perfect environment for misinformation and disinformation to be disseminated but it is also a virtual space that promotes it. This promotion is allowed to continue in most parts because of revenue prospects. Before we continue it is important to mention that misinformation and disinformation is often used interchangeably but there is a difference between the two. Misinformation is false information propagated by individuals that do not recognize the information as being false. Disinformation is a

[16] “IBM Docs,” July 7, 2021, https://prod.ibmdocs-production-dal-6099123ce774e592a519d7c33db8265e-0000.us-south.containers.appdomain.cloud/docs/en/db2oc?topic=procedures-k-means-clustering.

deliberate and organized publication of false content in order to achieve a specific objective.[17] None the less, both contribute to a confusing information environment on social media platforms.

Profits and Sensationalist

Simply put media platforms are driven by profits. The revenue is provided by advertisement that need to be seen by the users. In order to maximize the number of ads seen and get more revenue, media platforms devised AI algorithms that compiles and analyze our network habits in order to present to us content that will most likely catch our attention and maximize our screen time. Since most social human is attracted to controversies and gossip,[18] those algorithms detect our inclinations and they feed us with more and more stories that will maintain our attention. No effort is made to verify the source of the information. This sensationalist strategy of mainstream media is not new but nowadays there are people whose sole purpose is to create controversial news, ”fake new,” in order to attract views and gain profits from advertisements.

Filter Bubbles, Echo Chambers, and Bots

“Filter bubbles” is a phenomenon created by the previously mentioned algorithms that strive to personalize the viewing experience on our social media, search engines or entertainment streaming platforms. Our preferences are saved and analyzed by the algorithms in order to present similar information later on. Over time, the customization algorithms eliminate most if not all information that are opposed to our preferences. The

[17] Innocent E. Chiluwa and Sergei A. Samoilenko, *Handbook of Research on Deception, Fake News, and Misinformation Online* (Hershey, UNITED STATES: IGI Global, 2019): 17. http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=5783775.

[18] Helena Alicart, David Cucurell, and Josep Marco-Pallarés. "Gossip Information Increases Reward-Related Oscillatory Activity." NeuroImage 210, (Apr 15, 2020).

result is that we are never confronted with opposed views and different angles of information and news. The combined work of all those algorithms create a cyber-bubble around users that filter the information presented. As shown in figure 4,[19] this contributes to the isolation of world views and opinions. It also contributes to the polarizations of issues and limits curiosity.[20]

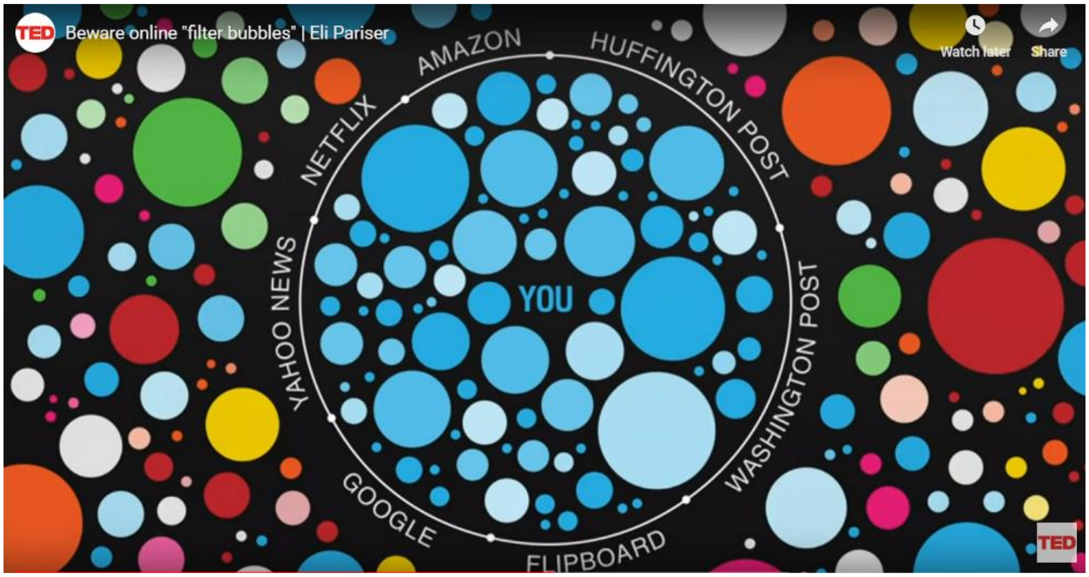


Figure 4—Graphic representation of a filter bubble
Source: *Pariser, Beware online "filter bubbles" TED* video.

"Echo chambers" in social media is a phenomenon that regroups people with the same opinions. The combination of "echo chambers" and "filter bubbles" (the consequence of algorithms that personalize our feed to what we like to see and we usually spend more time on reading posts from people that agree with us) create network groups that are very homogenous. The discussion in those homogenous groups resembles "echo chamber" because every member of that group echoes the opinion of others. This

[19] « Pariser Eli: Beware online filter bubbles », TED video (march 2011). https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=en
[20] Spohr, Dominic. "Fake News and Ideological Polarization: Filter Bubbles and Selective Exposure on Social Media." Business Information Review 34, no. 3 (September 2017). p. 150–60. https://doi.org/10.1177/0266382117722446 .

amplifies polarization on controversial subjects and can sometimes contribute to the radicalization of views. Figure 5 is a graphic representation of links between users on the subject of #beefban. You can see that there is very little links between the two opposed views.

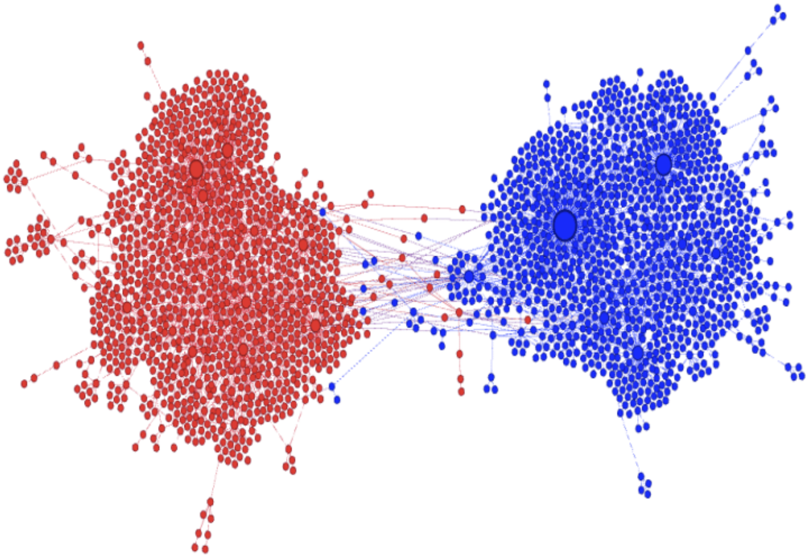


Figure 5—Echo chamber graphic representation
Source : https://www.researchgate.net/figure/Social-media-platforms-can-produce-echo-chambers-which-lead-to-polarization-and-can_fig4_322971747
.

"Trolls" designate users that post information that is deliberately provocative and misleading in order to create conflicts or useless discussions. Some "trolls" do it to amuse themselves, others have precise objectives. "Opinion manipulation trolls" are "trolls" that are paid to participate in virtual discussions in order to sway public opinion on a subject, promote a specific topic or to defend a particular point of view.[21]

"Bots" is an abbreviation that designates automated programs that accomplish specific tasks in cyberspace. There are multiple types of "bots" like the "machinic bot"

[21] Innocent E., Handbook of Research on Deception, Fake News, and Misinformation Online (Hershey, UNITED STATES: IGI Global, 2019): 32.

who accomplishes specific tasks. It is easily identifiable online by its robotic responses and lack of flexibility. The “social bot” is the most relevant for this research. It produces content automatically, interacts with users and can respond realistically. Its goal is usually to gain followers and gain access to specific network of social media users. They are usually inserted in specific “filter bubble” and react to discussions with the aim of promoting a product or an idea within the parameters of its program. In the context of “fake news” and information manipulation, “social bots” are useful to bolster the transmission of false information and amplify the network interest of certain subjects by automated sharing and commenting to create a controversy. Lastly, there are “bot-assisted person” which is really a strategy that some social media personalities use concentrate on content creation while the “bot” does the tedious work bolstering the personality’s presence on social media by “likes,” “shares” and even commenting. A “troll” could use that kind of “bot” to augment the visibility of his social media pages while he is busy “trolling.”[22]

Information Overload and Doubt

As previously mentioned, effective controlling information to assert power in a specific way is not easy. One of the ways that the Russians have gone around the problem is by overloading the network with easily recognizable “fake news,” mixing “fake new” with true and promoting specific truths. This has the effect of seeding doubt in most readers. Since most of us do not have the time to verify all media we consume we either blindly trust the news that is fed to us, doubt everything or somewhere in the middle. This

[22] Ibid.

has the unfortunate effect of eroding the trust in the press and the press's will to uncover the truth,[23] an essential part of the democratic process.

Summary

Social medial with all of its current mechanics promote the spread of "fake news." Some efforts are made by certain media platforms to identify and limit the spread but often it is too little, too late. With information overload and our inclination towards controversial gossip, most users will remember the first thing they read or listened to even if this "fake news" is debunked afterwards. The amount of information that we divulge about ourselves online and the abuse of the current social media power structures by nefarious actors makes this cyber environment the ideal vector to manipulate our knowledge of the world.

THE LITHUANIAN EXPERIENCE AND COUNTERACTIONS

Lithuania has always been under some sort of Russian information influence. It has been occupied by the Soviet on two occasions (1940–1941 and 1944–1990) and most of its population was used to the regime's propaganda. Some believed in it but most learned to acknowledge and read between the lines of the Party. Following the 2014 Russian invasion and annexation of the Crimea, the information operations targeting neighbouring states increased. Although the information manipulation coming from the Kremlin had always been there for Lithuania, it's government identified this propaganda

[23] A. B. C. News, "Journalists Despair over Toll of Disinformation on Jobs," ABC News, accessed May 8, 2022, https://abcnews.go.com/Entertainment/wireStory/journalists-despair-toll-disinformation-jobs-84086061.

as a national security threat following the Crimea annexation.[24] Four goals were identified in the Russian information attack against Lithuanians:

1. Create tensions between different groups;
2. Damage Lithuania's image towards allies and partners;
3. Promote support towards Russia; and
4. Undermine the state's legitimacy in the eyes of its citizens.[25]

Most of this information warfare was done through "fake news" transmitted via Russian television channels and Facebook social media platforms.

Counter actions

The immediate reaction to the Russian offensive in Lithuania was similar to what most democracies do in the same context. They increased monitoring of media, augmented strategic communications capabilities and bolstered media literacy and awareness programs. The Lithuanians had two objectives in the wake of the Russian information threat: "to reduce the amount of Russian disinformation and to neutralize its negative impact as quickly as possible."[26] But the Lithuanian government had to find a way to weather this information operation on the long run. They had to boost the overall resilience of Lithuanian institutions and society as a whole against Russian propaganda.

The concrete actions of Lithuanians against the Russian information threat was done on multiple fronts. The fight was not only through government legislation and

[24] VYTAUTAS KERŠANSKAS, Hybrid CoE Paper 6: Deterring disinformation? Lessons from Lithuania's countermeasures since 2014 (Helsinki, Finland: Hybrid CoE, April 2021): 7. https://www.hybridcoe.fi/wp-content/uploads/2021/04/20210427_Hybrid-CoE-Paper-6_Deterring_disinformation_WEB.pdf

[25] *Ibid*:9.

[26] *Ibid*: 10.

monitoring but also through private sector initiatives down to the volunteering of citizens to act as “Elves” to counter the army of Russian “Trolls.”[27] As we can see in figures 6 and 7 the numbers of actions undertaken were numerous and broad. They not only originated from the government but also from multiple non-governmental initiative.

[27] “‘We’Re at War’: The ‘Lithuanian Elves’ Who Take on Russian Trolls Online,” n.d., https://www.france24.com/en/europe/20220123-we-re-at-war-the-lithuanian-elves-who-take-on-russian-trolls-online.

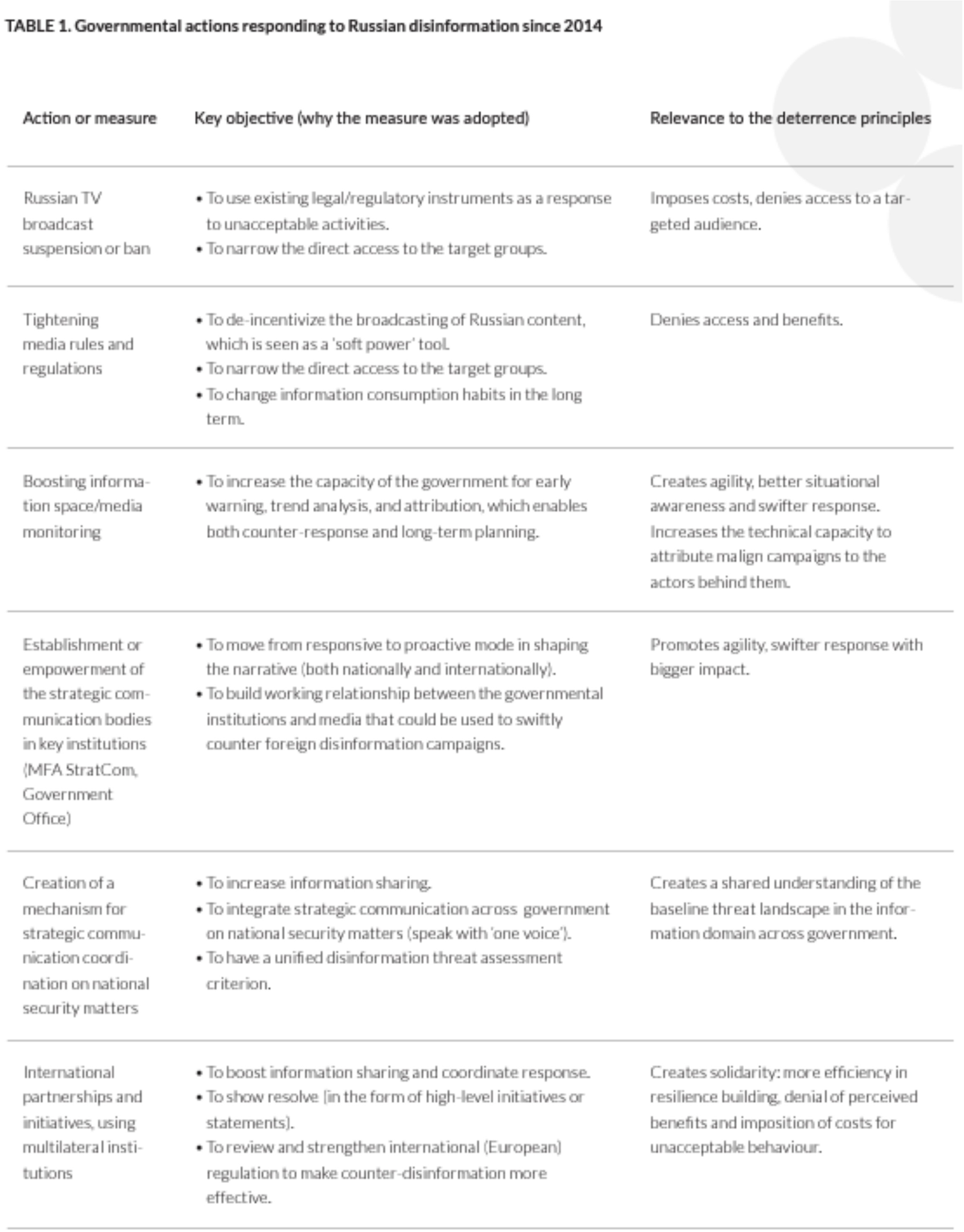


TABLE 1. Governmental actions responding to Russian disinformation since 2014

Action or measure	Key objective (why the measure was adopted)	Relevance to the deterrence principles
Russian TV broadcast suspension or ban	• To use existing legal/regulatory instruments as a response to unacceptable activities. • To narrow the direct access to the target groups.	Imposes costs, denies access to a targeted audience.
Tightening media rules and regulations	• To de-incentivize the broadcasting of Russian content, which is seen as a 'soft power' tool. • To narrow the direct access to the target groups. • To change information consumption habits in the long term.	Denies access and benefits.
Boosting information space/media monitoring	• To increase the capacity of the government for early warning, trend analysis, and attribution, which enables both counter-response and long-term planning.	Creates agility, better situational awareness and swifter response. Increases the technical capacity to attribute malign campaigns to the actors behind them.
Establishment or empowerment of the strategic communication bodies in key institutions (MFA StratCom, Government Office)	• To move from responsive to proactive mode in shaping the narrative (both nationally and internationally). • To build working relationship between the governmental institutions and media that could be used to swiftly counter foreign disinformation campaigns.	Promotes agility, swifter response with bigger impact.
Creation of a mechanism for strategic communication coordination on national security matters	• To increase information sharing. • To integrate strategic communication across government on national security matters (speak with 'one voice'). • To have a unified disinformation threat assessment criterion.	Creates a shared understanding of the baseline threat landscape in the information domain across government.
International partnerships and initiatives, using multilateral institutions	• To boost information sharing and coordinate response. • To show resolve (in the form of high-level initiatives or statements). • To review and strengthen international (European) regulation to make counter-disinformation more effective.	Creates solidarity: more efficiency in resilience building, denial of perceived benefits and imposition of costs for unacceptable behaviour.

Figure 6—Lithuanian Government Actions

Source: Hybrid CoE Paper 6: Deterring disinformation? Lessons from Lithuania's countermeasures since 2014, https://www.hybridcoe.fi/wp-content/uploads/2021/04/20210427_Hybrid-CoE-Paper-6_Deterring_disinformation_WEB.pdf

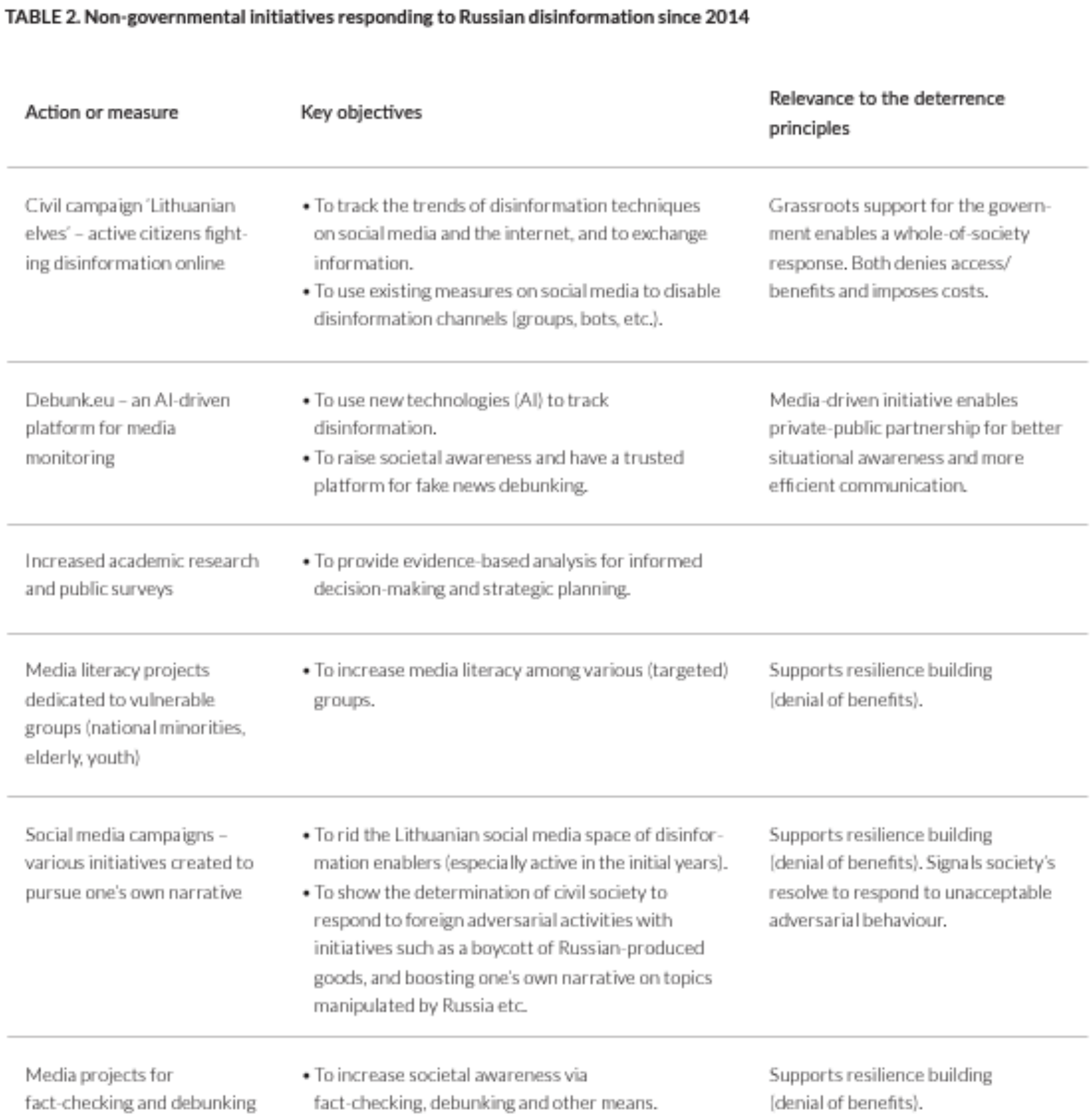


TABLE 2. Non-governmental initiatives responding to Russian disinformation since 2014

Action or measure	Key objectives	Relevance to the deterrence principles
Civil campaign 'Lithuanian elves' – active citizens fighting disinformation online	• To track the trends of disinformation techniques on social media and the internet, and to exchange information. • To use existing measures on social media to disable disinformation channels (groups, bots, etc.).	Grassroots support for the government enables a whole-of-society response. Both denies access/ benefits and imposes costs.
Debunk.eu – an AI-driven platform for media monitoring	• To use new technologies (AI) to track disinformation. • To raise societal awareness and have a trusted platform for fake news debunking.	Media-driven initiative enables private-public partnership for better situational awareness and more efficient communication.
Increased academic research and public surveys	• To provide evidence-based analysis for informed decision-making and strategic planning.	
Media literacy projects dedicated to vulnerable groups (national minorities, elderly, youth)	• To increase media literacy among various (targeted) groups.	Supports resilience building (denial of benefits).
Social media campaigns – various initiatives created to pursue one's own narrative	• To rid the Lithuanian social media space of disinformation enablers (especially active in the initial years). • To show the determination of civil society to respond to foreign adversarial activities with initiatives such as a boycott of Russian-produced goods, and boosting one's own narrative on topics manipulated by Russia etc.	Supports resilience building (denial of benefits). Signals society's resolve to respond to unacceptable adversarial behaviour.
Media projects for fact-checking and debunking	• To increase societal awareness via fact-checking, debunking and other means.	Supports resilience building (denial of benefits).

Figure 7—Lithuanian Nongovernment Actions

Source: Hybrid CoE Paper 6: Deterring disinformation? Lessons from Lithuania's countermeasures since 2014, https://www.hybridcoe.fi/wp-content/uploads/2021/04/20210427_Hybrid-CoE-Paper-6_Deterring_disinformation_WEB.pdf

Overall the combined efforts of governmental and non-governmental actors contributed to the resilience of the Lithuanians against Russian "fake news."

Results

Through a combined action plan, the Lithuanian counter information operation can be assessed as successful. They not only created a greater resiliency but also had a deterrent effect against any future offensive. This is not to say that Russian backed “trolls” will cease operations but by increasing the cost of such actions they made the endeavour less efficient. By limiting television air time of delinquent networks and encouraging voluntary “elves” to counter paid “trolls.” The Lithuanian couter made information operation expensive.

That being said, some would argue that some of the actions taken by the government of Lithuania was going against free speech, one of the corner stone of liberal democracies. There will always be a fine line between civil liberties and controlling information for the greater good. But who determines what is good and bad information for others? If the Lithuanian governmental apparatus did not have the power structure in place to dictate what information was constructive and detrimental to the unity of the state, none of this could have been possible. The Lithuanians navigated this fine line according to their own reality. They identified their own cognitive filters and addressed their week links decisively, but we cannot assume that the same actions would have worked in a different country.

CANADA’S INFORMATION ENVIRONMENT

Compared to Lithuania, Canada’s information environment differs greatly. There are currently no immediate generally recognized threat. Nothing compared to the Russia-Lithuania threat. But distance from our possible opponents does not mean that there is no threat or impact from “fake news” as defined previously. As a North Atlantic Treaty

Organisation (NATO) member Canada is a target for Russia. Even more so since the Canadian Armed Forces (CAF) leads NATO's presence in Lithuania and was up to recently an important actor in the training of Ukrainian forces. Some notable examples of Russian misinformation targeting Canada include the use of the actions of Russel Williams out of context to demonstrate the depravation of CAF leadership[28], promote anti-immigration following the attack of the Quebec City mosque[29] and even artificially create a trend on social media about the possible separation of Alberta province from Canada at the eve of federal elections.[30] All of these examples have one thing in common, the exploitation of weak links in the cognitive filters of the Canadian society. This shows that the biggest threat Canada faces in the information realm comes from within. Conspiracy theorists and extremists spreading "fake news" and recruiting people that would be otherwise moderate on social media is a real threat to the power of democratic institutions. The reality of that threat was demonstrated by the attack on the American Capitol in January 2021. It was qualified as an attack on democracy in a report from the American Senate.[31] The more recent occupation of Parliament Hill in Ottawa by the "Freedom Convoy" is another example of how disinformation and social media echo chambers can amplify and radicalize points of view to the point of civil unrest. The role of "fake news" and other cyber enablers in the Ottawa occupation is under investigation

[28] "Vesti.Lv: NATO's 'Blue Division' Dug in in Latvia. Waiting for Reinforcements," accessed May 8, 2022, https://web.archive.org/web/20170617002913/http:/vesti.lv/news/golubaya-diviziya-nato-okapyvaetsya-v-latvii-zhdut-podkrepleniya.

[29] Roberto Rocha and Jeff Yates · CBC News ·, "Twitter Trolls Stoked Debates about Immigrants and Pipelines in Canada, Data Show | CBC News," CBC, February 12, 2019, https://www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.5014750.

[30] "Canada, Wexit, and the Federal Election Targeted in Russian Disinformation Campaign, Academics Say," calgaryherald, accessed May 9, 2022, https://calgaryherald.com/news/local-news/canada-wexit-and-the-federal-election-targeted-in-russian-disinformation-campaign-academics-say.

[31] U.S. Senate, Examining the U.S. Capitol Attack A Review of the Security, Planing and Response Failures on January 6 (8 june 2021). P. 95.

University of Ottawa's Information Integrity Lab.[32] But due to the limited resources of the laboratory the result might not be known in the near future.

Canada's Current Strategy

The Canadian government's strategic communication directive[33] is clearly articulated but lacks specific details in terms of response to "fake news." The Privy Council Office sets the communication priorities and themes and delegate most of the actions to the different ministers and departments. Social media and web communication strategy is mentioned in the directive and is also delegated to heads of communication of each department. For obvious reason the complete social media strategy is only accessible from the government of Canada's internal network.

The current response of the Canadian government to the misinformation and disinformation is reactive, regardless of the source. For example, the plan to protect Canada's democracy[34] includes multiple measures like enhancing citizen preparedness, reporting procedures, bolstering organizational readiness and combatting foreign interference through the Secutity and Intelligence Threat to Election (SITE) Task Force[35] and the G7 Rapid Response Mechanism.[36] This program has two flaws. First most of those measures are not advertised enough to be effective. Second, all of it is focused on

[32] "New UOttawa Project Probes Disinformation Driving 'Freedom Convoy' and Other Socio-Political Crises," ottawacitizen, accessed May 9, 2022, https://ottawacitizen.com/news/local-news/new-uottawa-project-probes-disinformation-driving-freedom-convoy-and-other-socio-political-crises.

[33] "Directive on the Management of Communications," accessed April 25, 2022, https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=30682&section=HTML.

[34] Democratic Institutions, "Protecting Democracy - Democratic Institutions - Canada.Ca," August 10, 2021, https://www.canada.ca/en/democratic-institutions/services/protecting-democracy.html.

[35] Democratic Institutions, "Security and Intelligence Threats to Elections (SITE) Task Force," August 3, 2021, https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html.

[36] Democratic Institutions, "G7 Rapid Response Mechanism," backgrounders, January 30, 2019, https://www.canada.ca/en/democratic-institutions/news/2019/01/g7-rapid-response-mechanism.html.

foreign threats. Multiple other plans like this one are spread across different departments all with their own piece of the action. As mentioned by Simon Fraser University associate professor Nicole J. Jackson in an International Journal essay, "disinformation is on the Canadian government's radar. Since 2014, the federal government has increased its awareness of foreign disinformation in response to perceived threats, but without a coherent policy." It is obvious that "fake news" has been a challenge to define and understand for all democracies including Canada. The result has been a fragmented action that is more reactive than proactive.

Recommendations

Taking into account the Lithuanian lessons learned, the recommendations to address the "fake news" problem is two-fold.

First, the policy needs to shift its focus to a more domestic threat. Canadians need to understand their cognitive filters and weak links that need to be protected. This policy needs to be unified and funded adequately in order to be effective. It will have to bring on board the private sector and citizen on board. Legislation will have to be created to enforce responsible practices from social media platforms in order to limit the spread of "fake news" and mitigate the phenomenon of "echo chambers." Fostering information literacy should be part of school curriculum throughout the country, giving the youth of the country the ability to do its own fact checking.

Second, we have seen that it is difficult to debunk a story. Mainly because humans have a tendency to retain controversies and not pay attention to corrections or fact checking. We also know that access to trusted and unbiased news is one of the essential elements of liberal democracy societies. To that effect, the government of Canada needs to provide Canadians and the rest of the world a beacon of reliable and trusted information. This could be done by augmenting the funding of CBC and RC news department to increase its presence internationally and on every media type.

CONCLUSION

This essay sought to prove that “fake news” especially in the internet age is an important threat to liberal democracies. Canada is not an exception and the Canadian government needs to recognize, understand and act on the threat commensurate to its impact in order to maintain its relevance as a state power to its citizens and to the world.

The relation between information, knowledge and power fosters its manipulation to maintain, gain or reduce other’s powers. This manipulation is enabled by RC theory, big data, AI and social media mechanics.

The Lithuanians reacted promptly and effectively to a specific informational threat. They fostered societal resiliency by including the private sector and individual citizens actions. They also successfully created a deterrence effect by raising the cost of Russian information operations in Lithuania. That being said, the Lithuanian reacted to a specific threat in their very specific societal situation and they have threaded on a very thin line between free speech, civil liberties and information control.

In Canada, foreign informational threat is present but they mainly thrive on the weak links of our cognitive filters. Thus, the threat to Canadian power structures mainly comes from the inside. The current government actions against “fake news” is mainly focused on foreign threat. The policy to address disinformation and misinformation is fragmented and mainly reactive.

The Canadian government needs to shift it paradigm on information warfare by attacking it from inside outwards. To do that in need a comprehensive policy, focused on resiliency, deterrence and the provision of a trusted source of information nationally and internationally through CBC and RC.

BIBLIOGRAPHY

A, Romanova T., Sokolov N. I, and Kolotaev Y. Y. “Disinformation (Fake News, Propaganda) as a Threat to Resilience: Approaches Used in the EU and Its Member State Lithuania.” *Baltic Region* 12, no. 1 (March 1, 2020): 53–67. https://doi.org/10.5922/2079-8555-2020-1-4.

Bjola, Corneliu, and Pamment, James, eds. 2018. *Countering Online Propaganda and Extremism : The Dark Side of Digital Diplomacy*. Milton: Taylor & Francis Group. Accessed May 5, 2022. ProQuest Ebook Central.

Burkhardt, Joanna M. “History of Fake News.” Library Technology Reports 53, no. 8 (December 2017): 5.

Calgaryherald. “Canada, Wexit, and the Federal Election Targeted in Russian Disinformation Campaign, Academics Say.” Accessed May 9, 2022. https://calgaryherald.com/news/local-news/canada-wexit-and-the-federal-election-targeted-in-russian-disinformation-campaign-academics-say.

Chiluwa, Innocent E., and Sergei A. Samoilenko. *Handbook of Research on Deception, Fake News, and Misinformation Online*. Hershey, UNITED STATES: IGI Global, 2019. http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=5783775.

Departement of Defense, “Doctrine for the Armed Forces of the United States,” *Joint Publication 1*, (July 12, 2017).

Golbeck, Jennifer, Matthew Mauriello, Brooke Auxier, Keval H. Bhanushali, Christopher Bonk, Mohamed Amine Bouzaghrane, Cody Buntain et al. (2018). Fake news vs satire: A dataset and analysis. In Proceedings of the 10th ACM Conference on Web Science, https://doi.org/10.1145/3201064.3201100.

Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats. “Hybrid CoE Paper 6: Deterring Disinformation? Lessons from Lithuania’s Countermeasures since 2014.” Accessed May 8, 2022. https://www.hybridcoe.fi/publications/deterring-disinformation-lessons-from-lithuanias-countermeasures-since-2014/.

“IBM Docs,” July 7, 2021. https://prod.ibmdocs-production-dal-6099123ce774e592a519d7c33db8265e-0000.us-south.containers.appdomain.cloud/docs/en/db2oc?topic=procedures-k-means-clustering.

“Internet History Sourcebooks Project.” Accessed May 4, 2022. https://sourcebooks.fordham.edu/basis/procop-anec.asp.

“Issue 14 of ‘The Examiner’ 9/11/1710.” Accessed May 4, 2022. https://www.ourcivilisation.com/smartboard/shop/swift/examiner/chap14.htm.

Laato, Samuli, A. K. M. Najmul Islam, Muhammad Nazrul Islam, and Eoin Whelan. "What Drives Unverified Information Sharing and Cyberchondria during the COVID-19 Pandemic?" *European Journal of Information Systems* 29, no. 3 (May 3, 2020): 288–305. https://doi.org/10.1080/0960085X.2020.1770632.

"Lessons From Lithuania in Tackling Disinformation," n.d. https://eeradicalization.com/lessons-from-lithuania-in-tackling-disinformation/.

News, A. B. C. "Journalists Despair over Toll of Disinformation on Jobs." ABC News. Accessed May 8, 2022. https://abcnews.go.com/Entertainment/wireStory/journalists-despair-toll-disinformation-jobs-84086061.

Nye, Joseph S. "Public Diplomacy and Soft Power." *The ANNALS of the American Academy of Political and Social Science* 616, no. 1 (March 1, 2008): 94–109. https://doi.org/10.1177/0002716207311699.

Ottawacitizen. "New UOttawa Project Probes Disinformation Driving 'Freedom Convoy' and Other Socio-Political Crises." Accessed May 8, 2022. https://ottawacitizen.com/news/local-news/new-uottawa-project-probes-disinformation-driving-freedom-convoy-and-other-socio-political-crises.

Rocha, Roberto, and Jeff Yates · CBC News ·. "Twitter Trolls Stoked Debates about Immigrants and Pipelines in Canada, Data Show | CBC News." CBC, February 12, 2019. https://www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.5014750.

THOMAS, TIMOTHY. "Russia's Reflexive Control Theory and the Military." *The Journal of Slavic Military Studies* 17, no. 2 (June 1, 2004): 237–56. https://doi.org/10.1080/13518040490450529.

U.S. Senate, Examining the U.S. Capitol Attack A Review of the Security, Planing and Response Failures on January 6 (8 june 2021).

"Vesti.Lv: NATO's 'Blue Division' Dug in in Latvia. Waiting for Reinforcements." Accessed May 9, 2022. https://web.archive.org/web/20170617002913/http:/vesti.lv/news/golubaya-diviziya-nato-okapyvaetsya-v-latvii-zhdut-podkrepleniya.

VYTAUTAS KERŠANSKAS, Hybrid CoE Paper 6: Deterring disinformation? Lessons from Lithuania's countermeasures since 2014 (Helsinki, Finland: Hybrid CoE, April 2021). https://www.hybridcoe.fi/wp-content/uploads/2021/04/20210427_Hybrid-CoE-Paper-6_Deterring_disinformation_WEB.pdf

Weiss, Andrew P., Ahmed Alwan, Eric P. Garcia, and Julieta Garcia. "Surveying Fake News: Assessing University Faculty's Fragmented Definition of Fake News and Its Impact on Teaching Critical Thinking." International Journal for Educational Integrity 16, no. 1 (February 2020). http://dx.doi.org.cfc.idm.oclc.org/10.1007/s40979-019-0049-x.

"What Is Unsupervised Learning?," March 31, 2022. https://www.ibm.com/cloud/learn/unsupervised-learning.

Institutions, Democratic. "Protecting Democracy - Democratic Institutions - Canada.Ca," August 10, 2021. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy.html.

Security, Canadian Centre for Cyber. "Canadian Centre for Cyber Security." Canadian Centre for Cyber Security, August 15, 2018. https://cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300.

Canada, Global Affairs. "Rapid Response Mechanism Canada - Protecting Democracy." GAC, August 13, 2019. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/rrm-mrr.aspx?lang=eng.

Institutions, Democratic. "Security and Intelligence Threats to Elections (SITE) Task Force," August 3, 2021. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html.

Institutions, Democratic. "G7 Rapid Response Mechanism." Backgrounders, January 30, 2019. https://www.canada.ca/en/democratic-institutions/news/2019/01/g7-rapid-response-mechanism.html.