National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Imbalance of Policy and Threat: Social Media and the Canadian Armed Forces

Lieutenant-Commander Andrew J. Metz

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.

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

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.

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

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 DL – PCEMI 46 AD

2019 – 2021

SOLO FLIGHT

IMBALANCE OF POLICY AND THREAT: SOCIAL MEDIA AND THE CANADIAN ARMED FORCES

By Lieutenant-Commander A.J. Metz

"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."

IMBALANCE OF POLICY AND THREAT: SOCIAL MEDIA AND THE CANADIAN ARMED FORCES

The ability for Canada's adversaries to directly influence the cultural fabric of the Canadian Armed Forces (CAF) has never been as great as it is today. The ubiquitous use of social media (SM) platforms such as Twitter, Snapchat, Facebook, and TikTok are so prevalent, that most of Canadians are unaware of the source or validity of the online content they experience. Threats within this trojan horse have arrived virtually undetected, providing hostile actors with the ability to destabilize western democracy through deception, propaganda, and false information.[1] In other words, "our opponents have infiltrated our personal communication spaces, having already recruited many followers who spread their messages unwittingly."[2] This leaves the CAF facing an unprecedented challenge to its command-and-control capabilities stemming from a deluge of extremist propaganda that even the major social media platforms "are struggling to contain."[3]

With right-wing populism on the rise, incidents of radicalized and hateful conduct within the ranks will also continue to increase. Social media is no longer regarded solely as a space for friends to socialize and to share family vacation photos. It has become a powerful influencing tool; capable of being maliciously deployed against Canadian service personnel to obtain a wide variety of outcomes. Operatives, ranging from lone hackers to hordes of conscripts working in

---

[1]Jacob Davey, Mackenzie Hart, and Cécile Guerin, *An Online Environmental Scan of Right-wing Extremism in Canada* (Toronto: Institute for Strategic Dialogue, 2020), 4, https://www.isdglobal.org/wp-content/uploads/2020/06/An-Online-Environmental-Scan-of-Right-wing-Extremism-in-Canada-ISD.pdf.

[2]Bruce Forrester and Friederike Von Franqué, *Towards a Deception Detection Framework for Social Media (*Ottawa: Defence Research and Development Canada, December 2020), 4. https://cradpdf.drdc-rddc.gc.ca/PDFS/unc350/p812520_A1b.

[3]N. Velásquez, P. Manrique, R. Sear *et al,* "Hidden order across online extremist movements can be disrupted by nudging collective chemistry," *Scientific Reports 11,* (2021), 1, https://doi.org/10.1038/s41598-021-89349-3.

warehouse sized troll farms, employ unscrupulous tactics to infiltrate the accounts of unsuspecting members. Once established, they peddle ideologies, foster social discourse, and profit from identity and financial theft. Most of these attacks do not generate media headlines, as the process is often a gradual and largely undetectable. And while the affects are not often immediate, real damage is being done. For instance, recent hateful incidents demonstrate that the social values and opinions of CAF members are being "shaped and shared, because digital posts spawn commentary, sway views, and spur action."[4] Notable examples include the Proud Boys disruption of a Mi'kmaw ceremony in Halifax, Corey Hurren's attack on Rideau Hall, and the ongoing Patrik Mathews terrorism case.

Amarnath Amarasingam, a Senior Research Fellow at the Institute for Strategic Dialogue, described the CAFs initial response to these incidents as a clear indicator that the military does not have the appropriate tools to respond to SM inspired hateful conduct. He highlights the requirement for comprehensive policy, pointing out that CAF leadership "did not know what to do with suspected extremists in their ranks … and that they're still having a difficult time understanding far-right ideology and how to respond."[5] This paper will argue that while the Canadian Armed Forces demonstrates the will to eliminate hateful conduct, its current policies fail to effectively respond to the subversive power of social media within the cyber battle space.

Hateful conduct in the ranks is not new a new phenomenon; however, the methods by which it spreads have evolved. By its very nature, right wing populism is dynamic, unstable, and

---

[4]Matthew R Auer, "The Policy Sciences of Social Media." *The Policy Studies Journal 39, no. 4* (November 2011): 711, http://web.b.ebscohost.com.cfc.idm.oclc.org/ehost/pdfviewer/pdfviewer? vid=1&sid=877c0b31-3b48-484a-acce-60ce9c39a475%40pdc-v-sessmgr03.

[5]Karen Pauls and Ashley Burke, "Military conducted secret investigation of reservist Patrik Mathews as a possible terrorist threat," *CBC News*, last modified 15 March 2021, https://www.cbc.ca/news/politics/patrik-mathews-canadian-forces-neo-nazi-terrorist-1.5948202.

ephemeral in nature; often making it hard to detect and evaluate.[6] And with social media now readily available to virtually everyone on the planet, it has never been easier to recruit, program, and activate large numbers of individuals who may be susceptible to extremist ideologies. Barbara Perry, director of the Canadian Centre on Hate, Bias, and Extremism agrees, adding that there has been a notable escalation with online extremist activity in Canada in recent years. Her organization has identified over 6,600 Canadian websites and organizations that promote right-wing extremism across a number of SM sites; "sites which collectively reached over 11 million Canadian users."[7] An internal CAF report also confirms that members are being influenced online by terrorist and hate groups such as the Proud Boys, The Base, Atomwaffen Division, La Meute, Hammerskins Nation, III%, and Soldiers of Odin.[8] It is clear that extremism is making a resurgence in military culture, and that social media has become the weapon of choice.

Online foreign influence campaigns have become the new normal. American foreign policy adviser Jarred Prier, writes that "using social media to take command of a trend makes the spread of propaganda easier than ever before."[9] In other words, "he who controls the trend will control the narrative—and, ultimately, the narrative controls the will of the people."[10] The Canadian Centre for Cyber Security (CCCS) agrees, stating that influence operations often

---

[6]Steve J. Ropp, "Populism: The Strategic Implications of the Rise of Populism in Europe and South America," *Strategic Studies Institute, US Army War College* (2005): 31, https://www.jstor.org/stable/pdf/resrep11716.pdf?refreqid=excelsior%3Ae17e1ee6ebe3b33343108630b2e3e056.

[7]Elizabeth Thompson, "Facebook partners with Ontario university on 'global network' to counter rise in online hate," *CBC News*, last modified 28 July 2020, https://www.cbc.ca/news /politics/ facebook-hate-online-extremism-1.5664832.

[8]Stewart Bell and Mercedes Stephenson, "Canadian Armed Forces members linked to six hate groups: internal report," *Global News,* last modified 28 May 2019, https://globalnews.ca/news/ 5322011/canadian-armed-forces-members-linked-to-six-hate-groups-internal-report/.

[9]Jared Prier, "Commanding the Trend: Social Media as Information Warfare," *Air University Press, Strategic Studies Quarterly, Vol. 11, No. 4* (2017): 79, https://www.jstor.org/stable/10.2307/26271634.

[10]Ibid., 81.

succeed because they "exploit deeply rooted human behaviours and social patterns."[11] This was highlighted in media reports that suggested the convicted Rideau Hall extremist, Corey Hurren, was "sucked into some of the darker corners of the internet,"[12] and "influenced by QAnon conspiracy theories."[13]

Responding to several recent incidents of hateful conduct, the Canadian Anti-Hate Network released a statement that CAF leadership must react decisively to the significant threat of extremism in the ranks. Their report highlights the observation that "the military did not appear to view the increasing incidents as alarming."[14] Theses incidents have damaged the CAF's reputation, and must serve as a wake-up call that SM influenced propaganda has permeated military culture. Therefore, a comprehensive policy to detect, intercede, and deter the effects of harmful social media is required. Without a strategic vision and action plan to recognize and counter harmful SM, it is likely the CAF will continue to serve as a fertile breeding ground for extremists promoting violent transnational social movements.[15]

It could be argued that harmful events inspired by SM are rare, and that the probability of hate-based events reoccurring in the military remains low. While this is perhaps true, it is expected that our adversaries will continue to infiltrate the online presence of members to weaken military ethos, cohesion, and effectiveness. The Minister of National Defence agrees, stating "the internet is now at a crossroads, with countries like China and Russia pushing to

---

[11]Government of Canada, *National Cyber Threat Assessment 2020* (Ottawa: Canadian Centre for Cyber Security, 2020), 27, https://cyber.gc.ca/sites/default/files/publications/ ncta-2020-e-web.pdf.
[12]Alex Boutilier, "Accused in Rideau Hall gun incident has long history of being drawn to conspiracy websites," *Toronto Star*, last modified 11 July 2020, https://www.thestar.com/politics/federal/2020/07/11/accused-in-rideau-hall-gun-incident-has-long-history-of-being-drawn-to-conspiracy-websites.html?rf.
[13]Elizabeth Thompson.
[14]Stewart Bell and Mercedes Stephenson.
[15]Canadian Association for Security and Intelligence Studies Vancouver, "Right-Wing Extremism in the Canadian Armed Forces," last accessed 23 May 2021, https://casisvancouver.ca/ press-releases/right-wing-extremism-in-the-canadian-armed-forces/.

change the way it is governed, to turn it into a tool for censorship, surveillance, and control."[16] Further substantiation is provided in a 2020 CCCS report that confirms threats from open-source media are becoming increasingly sophisticated, and intrusive. The report outlines how influencers commonly use deep fake technology, troll farms, bots, and botnets, to achieve their aims.[17] Other deceptive techniques include identity masking, posing as trusted spokespersons or celebrities, and incrementally radicalizing messages over time with the aim to re-programme social views.

Social media has become a versatile weapon that influences and alters the viewer's belief systems and societal values. For example, actors can launch a narrative on Twitter with the potential of reaching 89 percent of all 340 million subscribers within only eight rounds of communication."[18] The Canadian Centre for Identity-Based Conflict (CCIBC) recommends this is a significant problem, as cleverly disguised SM "poses a serious threat to the safety and security of combat operations."[19] For example, by receiving unfettered misinformation from right-wing elements, members can fall victim to the "normalization of views that damaged the reputation of CAF as seen in the 1993 Somalia Affair."[20] In summary, well-crafted misinformation campaigns not only have the potential to undermine our international relationships, but also threatens unit safety, morale, and cohesion at home.

---

[16]Government of Canada, *National Cyber Threat Assessment 2020*, 2.
[17]Government of Canada, "Canadian Centre for Cyber Security Releases the Canadian National Cyber Threat Assessment 2020," last modified 18 November 2020, https://www.canada.ca/en/ communications-security/news/2020/11/canadian-centre-for-cyber-security-releases-the-canadian-national-cyber-threat-assessment-2020.html.
[18]Benjamin Doerr, Mamoud Fouz, and Tobias Fredrich, "Why Rumors Spread So Quickly in Social Networks," *Communications of the ACM* (2012): 71, https://cacm.acm.org/magazines/2012/6/149793-why-rumors-spread-so-quickly-in-social-networks/fulltext.
[19]Canadian Association for Security and Intelligence Studies Vancouver.
[20]Ibid.

State-sponsored cyber activity originating from Russia, North Korea, China, and Iran is currently the "most sophisticated threat to Canadians and Canadian organizations."[21] These actors destabilize western ideology to further their own ideological interests in part by "feeding conspiracy theories designed to alienate; laundering them through fringe sites and social media."[22] For example, the CCCS reports that Iranian and Russian-sponsored trolls commonly use fake media accounts to sew discourse amongst Canadians. They accomplish this by exaggerating false statements on highly charged political issues such as climate change, treaty rights, immigration, pipelines, and social programs. Recent examples include Russia's attempts to influence the 2019 federal election, steal COVID-19 research, and spread disinformation about the Canadian government's response to the pandemic.[23]

Although there is ample evidence substantiating foreign influencing activities, one might question to what degree recent incidents of hateful conduct in the CAF were influenced by social media. For example, one could argue that SM was never proven to be the mitigating factor with Corey Hurren's attack on Rideau Hall. Can this event be classified as a "one-off" event, and considered as an "expected" level of societal perversion? After all, members of the CAF are representative of Canadian society, and such cases occur throughout all cross sections of the population. While these arguments have merit, I posit that service members are indeed at a higher risk, as they are increasingly targeted with misinformation simply due to their membership within the CAF. An example of how online extremism can transition to real world violence is demonstrated with the recent storming of the US State Capitol Building. Here, US

---

[21]Government of Canada, *National Cyber Threat Assessment 2020*, 1.
[22]Sheera Frenkel and Julian E. Barnes, "Russians Again Targeting Americans with Disinformation, Facebook and Twitter Say," *The New York Times,* last modified 1 September 2020, https://www.nytimes.com/2020/09/01/technology/facebook-russia-disinformation-election.html.
[23]Government of Canada, *National Cyber Threat Assessment 2020*, 19.

military members (among many others) were seduced by extremist groups who had "used social media to coordinate activities."[24] A Canadian example dates to 2017 when CAF members stationed in Latvia were the target of Russian trolls attempting to sew discord among the local population with repeated fake news designed to discredit NATO forces.[25]

Many of Canada's adversaries do not share western values, including human rights, security, and privacy. If left unchecked, online deviation from the accepted international norms has the potential to foment "internal conflict over political, religious, and racial views that negatively impact unit cohesion and communication and ultimately negate CAF's ability to operate to its full potential."[26] To ensure their continued success, adversaries are developing novel ways infiltrate our communication channels. For example, new technologies such as China's 5G network will "permit domestic extremists to send and receive encrypted communications and to network with other extremists throughout the country and abroad; making it much more difficult for law enforcement to deter, prevent, or pre-empt a violent extremist attack."[27] This represents a clear advantage for those who wish to do us harm.

The CAF currently has an insufficient capacity to recognize and react to harmful SM information operations. It has been said that "if in the 20th century the greatest challenge was the battle for freedom of information, then in the 21st century the greatest challenge will be from states abusing freedom of information."[28] Former VCDS Jonathan Vance voiced his concern

---

[24]Velásquez, Manrique, Sear *et al,* 1.
[25]Tom Blackwell, "Russian fake-news campaign against Canadian troops in Latvia includes propaganda about litter, luxury apartments," *National Post*, last modified 17 November 2017, https://nationalpost.com/news/canada/russian-fake-news-campaign-against-canadian-troops-in-latvia-includes-propaganda-about-litter-luxury-apartments.
[26]Canadian Association for Security and Intelligence Studies Vancouver.
[27]United States, Department of Homeland Security Office of Intelligence and Analysis, *Right-wing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment,* (Homeland Environment Threat Analysis Division, 7 April 2009), 8, https://fas.org/irp/ eprint/rightwing.pdf.
[28]Peter Pomerantsev and Michael Weiss, "The Menace of Unreality: how the Kremlin Weaponizes Information, Culture and Money." *The Interpreter, Institute for Modern Russia* (2014): 40, https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf.

regarding the harmful effects of misinformation when discussing the CAF's lack of comprehensive policy to recognize and react to right wing extremism in the ranks.[29] Another way to contextualize the desire to control information is by examining Canadian philosopher Marshall McLuhan's theory that *the medium is the message*. If the medium is social media, then it logical to conclude that the victor of the information war will be those who control the message. If this is true, then the CAF requires a more robust policy on the use of social media and how it relates to hateful conduct.

Existing Policy

In 2018, the CAF released the *Official Use of Social Media* directive in Defence Administrative Order and Directive (DOAD) 2008-8. This instruction warns of the clear and present danger that social media presents to the institution. It cites that CAF members, are "vulnerable to predatory action by adversarial or criminal elements, who may seek to use social media to impersonate or appropriate their personal image and identity for nefarious purposes."[30] The CDS has provided amplification in CANFORGEN 016/18 stating "CAF members shall ensure that their online activity, whether on or off duty, does not reflect discredit on the CAF, or compromise the CAFs reputation."[31] While a positive step, this policy prohibiting the dissemination of harmful SM will be difficult to monitor or enforce. An exhaustive change initiative is required, placing priority on education, investigation, reporting, and responding.

---

[29]Alex Boutilier, "Right-wing extremism not welcome in Canadian Armed Forces – but 'clearly, it's in here,' says top soldier," *Toronto Star,* last modified 8 October 2018, https://www.thestar.com/ news/canada/2018/10/07/ right-wing-extremism-not-welcome-in-canadian-armed-forces-but-clearly-its-in-here-says-top-soldier.html.

[30]Government of Canada, "DAOD 2008-8, Official Use of Social Media," last modified 9 October 2018, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/2000-series/2008/2008-official-use-social-media.htm.

[31]Department of National Defence, "CANFORGEN 016/18, CDS Direction on Professional Military Conduct," last accessed 25 May 2021, http://vcds.mil.ca/apps/canforgens/ default-eng.asp?id=016-18&type=canforgen.

Without a significant effort in these four areas, generalized statements such as the ones included in DOAD 2008-8 and CANFORGEN 016/18 will likely have little effect.

The CAF reviewed its policy on conduct and performance deficiencies following recent incidents of SM induced hateful conduct by the likes of the Proud Boys. In mid 2020, DOAD 5019-0 was updated to include a definition for hateful conduct. The intent was to "put words into action on misconduct and inappropriate behaviour, and to eliminate hateful conduct from our institution."[32] The three environmental commands also weighed in by promulgating their own amplifying instructions in NAVGEN 15/20, CANAIRGEN 12/20, and CAO 11-82.[33] The CAF definition for hateful conduct now reads as "an act or conduct, including the display or communication of words, symbols or images… that constitute, encourage, justify or promote violence or hatred against a person or persons of an identifiable group..."[34] Vice-Admiral Haydn Edmundson, former Commander Military Personnel Command, suggested the goal of DOAD 5019-0 is to stamp out hateful conduct. While his statement defines the preferred end state, the details of *how* it will be achieved remains unknown.

The CAF is making steps towards addressing the problem of social media inspired misconduct in the ranks; however, some experts believe that the institution is falling short. Legal expert, Lieutenant-Colonel (retired) Rory Fowler suggests the addition of a hateful conduct definition in DAOD 5019-0 does not add much from a policy perspective. He points out that much of what is covered in the update has already been captured in DAOD 5012-0 for

---

[32]Government of Canada, "New CAF Administrative Order and Military Personnel Instruction on Hateful Conduct," last modified 24 July 2020, https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2020/07/new-caf-ao-mp-instruction-hateful-conduct.html.

[33]Government of Canada, "Canadian Army Order 11-82 Hateful Conduct," last modified 5 November 2020, http://www.army-armee.forces.gc.ca/en/policies/cao-11-82-hateful-conduct.page.

[34] Government of Canada, "DAOD 5019-0, Conduct and Performance Deficiencies," last modified 7 October 2020, https://www.canada.ca/en/department-national-defence/corporate/ policies-standards/ defence-administrative-orders-directives/5000-series/5019/5019-0-conduct-and-performance-deficiencies.html.

Harassment Prevention and Resolution. "At best, it reduces to writing, a policy expression that has already been captured in other legislation and policy."[35] Ottawa lawyer and retired Colonel Michel Drapeau, also offers a dour review of the policy update. He states, "under the new policy, the CAF has distanced itself from the criminal code, inviting commanding officers to treat any such wilful hateful conduct as an administrative, disciplinary matter."[36] Drapeau concludes by suggesting the policy enables COs to safeguard their units and potential offenders from criminal investigation.

One could argue that the CAF responded to these concerns by releasing CANFORGEN 169/20. This amplification to DOAD 5019-0 clarifies, that "when a unit disciplinary investigation is deemed necessary in accordance with article QR&O 106.02, such an investigation may only be conducted once it is determined that all police with jurisdiction to investigate the matter have declined to investigate."[37] But does this compel a unit to refer potential offenders for police investigation? I suggest it doesn't, as the onus remains on the chain of command to determine if an external investigation is warranted. Fowler warns that one of the biggest challenges will be to develop "a feasible means to address the ability of CAF personnel to avoid impunity."[38] In its current form, DAOD 5019-0 does not do this; providing a mechanism for units to continue to deal with members accused of hateful conduct or extremism from behind closed doors.

---

[35]Rory Fowler, **"**The Canadian Forces and 'Hateful Conduct,'" Kingston: Law Office of Rory G. Fowler, last modified 2019, http://roryfowlerlaw.com/the-canadian-forces-and-hateful-conduct/.

[36]Karen Pauls, "Canadian military says new hateful conduct policy will help weed out extremists in the ranks," *CBC*, last modified 16 July 2020, https://www.cbc.ca/news/canada/manitoba/canadian-military-tool-identifies-hateful-conduct-1.5652276.

[37]Government of Canada, "CANFORGEN 169/20, last modified December 2020, http://vcds.mil.ca/apps/canforgens/default-eng.asp?id=169-20&type=canforgen.

[38]Rory Fowler, "(It's) the Impunity, Stupid," Kingston: Law Office of Rory G. Fowler, last modified 2019, http://roryfowlerlaw.com/its-the-impunity-stupid/.

In the end, the current policy only supplies general guiding statements, without providing instruction for leadership to effectively identify, address, or prevent SM inspired hateful conduct. For example, from more than fifty cases of recent alleged hateful and extremist conduct in the ranks, only four cases resulted with disciplinary action.[39] It was reported that in many of these cases, "the military didn't even take remedial action … and when it did, members often faced official warnings or counselling and probation."[40] Without implementing substantial measures to counter the negative effect of SM, hateful incidents will continue to degrade the social cohesion of the military. This not only has a negative affect at the unit level but has the potential to undermine the CAF in the eyes of the Canadian public and the world.

Comprehensive policy is required

The Walt and Gilson policy analysis model suggests that policy writers often focus on the content of policy; occasionally neglecting other critical factors including the actors and the context.[41] As such, the CAF must develop a new social media policy framework that will optimize existing policy, while incorporating added mechanisms to improve the CAF's ability to react to the actors and context. It is recommended that the new policy include up to four lines of effort that include detection, education, reporting and responding.

Military intelligence requires a high level of confidence when identifying deceptive SM techniques. The first line of effort, *detection*, will enable the CAF to move from a defensive

[39]Ashley Burke, "Most cases of extremist conduct in Canadian military don't end in discipline, says document," *CBC News*, last modified 19 December 2019, https://www.cbc.ca/news/politics/caf-extremism-racism-cases-disciplined-1.5400747.
[40]Ibid.
[41]Gill Walt and Lucy Gilson, "Reforming the health sector in developing countries: the central role of policy analysis," Health Policy and Planning 9, no. 4 (1994): 355, http://cfc.idm.oclc.org/login?url=https://doi.org/10.1093/heapol/9.4.353.

posture to offensive readiness.[42] The CAF has begun to enhance the ability to detect by "creating a new Canadian Armed Forces Cyber Operator occupation."[43] The Canadian Forces Network Operations Centre (CFNOC) was also created with a mandate to "preserve cyber superiority within the DND/CAF's cyber area of operation."[44] CFNOC collaborates with the CCCS and the Communications Security Establishment (CSE) "to detect, defeat, and/or mitigate offensive and exploitive actions to maintain freedom of action."[45] And while progress has been made in the areas of enhancing infrastructure, defence specialists argue that much more needs to be done in the field of research and policy development.

Without an empirical-based detection mechanism, the CAF will remain at a competitive disadvantage in its ability to respond to SM attacks. Defence researchers, Bruce Forrester & Friederike Von Franqué suggest that the current SM analytic tools are not capable of such detection.[46] They propose the CAF adopts a Deception Detection Framework that will incorporate "models, indicators, and analytics to detect deception."[47] A recent American study has also applied a scientific approach to "elucidate the possible mechanics of extremist online growth by comparing a mathematical model of aggregation to empirical data."[48] Other areas of research include a Decision Analysis and Response Project within the Canadian Armed Forces Cyber Capital Program. With continued research, the CAF will improve its cyber threat

---

[42]Amanda Connolly, "Military fills first new 'cyber operator' jobs, with more to come," *iPolitics*, last modified 23 October 2017, https://ipolitics.ca/2017/10/23/military-fills-first-jobs-in-new-cyber-force-with-more-to-come/.
[43]Department of National Defence. "Strong Secure Engaged – Canada's Defence Policy," (Ottawa: 2017), 111, http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf.
[44] Department of National Defence, "IT Security vs. Defensive Cyber Operations: The evolution of CAF Cyber," *Powerpoint presentation by Master Warrant Officer Alex Arndt, Canadian Forces Network Operations Centre*, 1 November 2018, https://www.countermeasure.ca/wp-content/uploads/2018/01/documents_2018_presentations_Alex-Arndt-IT_Security_VS_Defensive_Cyber_Operations.pdf.
[45]Ibid.
[46]Forrester and Von Franqué, 21.
[47]Ibid., 21.
[48]Velásquez, Manrique, Sear *et al,* 3.

identification and incident response capabilities; enhancing its "ability to contain and eradicate threats from DND/CAF networks."[49]

Canada is trailing many of its allies in when it comes to defining a strategic vision for social media management. For example, the American Department of Defence is considering a SM pilot program designed to "monitor military personnel for concerning behaviors."[50] This project is not intended to screen all SM accounts but will serve as an additional means of conducting security clearances for current members going into key positions. While there are obvious ethical and privacy challenges to overcome, the Pentagon maintains there is value to "incorporating machine learning and natural language processing into social media screening platforms."[51] By adopting a similar approach, the CAF will achieve the mandate of *Strong Secure Engaged* initiative 65 that calls for "improved cryptographic capabilities, information operations capabilities, and cyber capabilities to include cyber threat identification and response."[52]

Canada's adversaries understand that by subversively capturing the attention of CAF members, they can deliver direct damage to the cohesion, morale, conduct, and reputation of the institution. Technological advancements will continue to progress at an ever-increasing speed, leaving our armed forces scrambling to comprehend and counter the multiple tools and techniques our enemies use to access and influence our social views. The CAF is demonstrating

---

[49]Government of Canada, "Joint Capabilities – Cyber Security," last modified 1 March 2021, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/main-estimates-2020-2021/joint-capabilities.html.

[50]Ken Klippenstein, "Pentagon Plans to Monitor Social Media of Military Personnel for Extremist Content," *The Intercept*, last modified 17 May 2021, https://theintercept.com/2021/05/17/military-pentagon-extremism-social media/?utm_medium=social&utm_source=twitter&utm_ campaign=theintercept&fbclid=IwAR0i9V-MbjwaOIqwz36hckw9HaiS4l5td WiC6CVTX8YQ8TM8RND_M1_WYlw.

[51]Ibid.

[52] Department of National Defence, "Strong Secure Engaged," 41.

the will to eliminate hateful conduct, but the current policies are only paying lip service to curtailing the subversive power of social media. Therefore, the development and implementation of robust comprehensive policy focussing on the areas of detection, education, reporting and responding is warranted.

Bibliography

Auer, Matthew R. "The Policy Sciences of Social Media." *The Policy Studies Journal 39, no. 4* (November 2011): 709-736. http://web.b.ebscohost.com.cfc.idm.oclc.org/ehost/pdfviewer/pdfviewer?vid=1&sid=877c0b31-3b48-484a-acce-60ce9c39a475%40pdc-v-sessmgr03.

Bell, Stewart and Mercedes Stephenson. "Canadian Armed Forces members linked to six hate groups: internal report." *Global News.* Last modified 28 May 2019. https://globalnews.ca/news/ 5322011/canadian-armed-forces-members-linked-to-six-hate-groups-internal-report/.

Blackwell, Tom. "Russian fake-news campaign against Canadian troops in Latvia includes propaganda about litter, luxury apartments." *National Post*. Last modified 17 November 2017. https://nationalpost.com/news/canada/russian-fake-news-campaign-against-canadian-troops-in-latvia-includes-propaganda-about-litter-luxury-apartments

Boutilier, Alex. "Accused in Rideau Hall gun incident has long history of being drawn to conspiracy websites." *Toronto Star*. Last modified 11 July 2020. https://www.thestar.com/politics/federal/2020/07/11/accused-in-rideau-hall-gun-incident-has-long-history-of-being-drawn-to-conspiracy-websites.html?rf.

Boutilier, Alex. "Right-wing extremism not welcome in Canadian Armed Forces – but 'clearly, it's in here,' says top soldier." *Toronto Star*. Last modified 8 October 2018. https://www.thestar.com/ news/canada/2018/10/07/right-wing-extremism-not-welcome-in-canadian-armed-forces-but-clearly-its-in-here-says-top-soldier.html.

Burke, Ashley. "Most cases of extremist conduct in Canadian military don't end in discipline, says document." *CBC News*. Last modified 19 December 2019. https://www.cbc.ca/news/politics/caf-extremism-racism-cases-disciplined-1.5400747.

Canadian Association for Security and Intelligence Studies Vancouver. "Right-Wing Extremism in the Canadian Armed Forces." Last accessed 23 May 2021. https://casisvancouver.ca/press-releases/right-wing-extremism-in-the-canadian-armed-forces/.

Connolly, Amanda. "Military fills first new 'cyber operator' jobs, with more to come." *iPolitics*. Last modified 23 October 2017. https://ipolitics.ca/2017/10/23/military-fills-first-jobs-in-new-cyber-force-with-more-to-come/.

Davey, Jacob, Mackenzie Hart, and Cécile Guerin. *An Online Environmental Scan of Right-wing Extremism in Canada.* Toronto: Institute for Strategic Dialogue, 2020. https://www.isdglobal.org/wp-content/uploads/2020/06/An-Online-Environmental-Scan-of-Right-wing-Extremism-in-Canada-ISD.pdf.

Department of National Defence. "CANFORGEN 016/18, CDS Direction on Professional Military Conduct." Last accessed 25 May 2021. http://vcds.mil.ca/apps/canforgens/default-eng.asp?id=016-18&type=canforgen.

Department of National Defence. "IT Security vs. Defensive Cyber Operations: The evolution of CAF Cyber." *Powerpoint presentation by Master Warrant Officer Alex Arndt, Canadian Forces Network Operations Centre*. Last modified 1 November 2018. https://www.countermeasure.ca/wp-content/uploads/2018/01/documents_2018_presentations_Alex-Arndt-IT_Security_VS_Defensive_Cyber_Operations.pdf.

Department of National Defence. "Strong Secure Engaged – Canada's Defence Policy." Ottawa: 2017. http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf.

Doerr, B., M. Fouz, and T. Fredrich. "Why Rumors Spread so Quickly in Social Networks." *Communications of the ACM* (2012): 70-75. https://cacm.acm.org/magazines/2012/6/149793 -why-rumors-spread-so-quickly-in-social-networks/fulltext.

Forrester, Bruce and Friederike Von Franqué. *Towards a Deception Detection Framework for Social Media.* Ottawa: Defence Research and Development Canada, December 2020. https://cradpdf.drdc-rddc.gc.ca/PDFS/unc350/p812520_A1b.pdf.

Fowler, Rory. "(It's) the Impunity, Stupid." Kingston: Law Office of Rory G. Fowler. Last modified 2019. http://roryfowlerlaw.com/its-the-impunity-stupid/.

Fowler, Rory. **"**The Canadian Forces and 'Hateful Conduct'" Kingston: Law Office of Rory G. Fowler. Last modified 2019. http://roryfowlerlaw.com/the-canadian-forces-and-hateful-conduct/.

Frenkel, Sheera and Julian E. Barnes. "Russians Again Targeting Americans with Disinformation, Facebook and Twitter Say." *The New York Times.* Last modified 1 September 2020. https://www.nytimes.com/2020/09/01/technology/facebook-russia-disinformation-election.html

Government of Canada. "Canadian Army Order 11-82 Hateful Conduct." Last modified 5 November 2020. http://www.army-armee.forces.gc.ca/en/policies/cao-11-82-hateful-conduct.page.

Government of Canada. "Canadian Centre for Cyber Security Releases the Canadian National Cyber Threat Assessment 2020." Last modified 18 November 2020. https://www.canada.ca/en/ communications-security/news/2020/11/canadian-centre-for-cyber-security-releases-the-canadian-national-cyber-threat-assessment-2020.html.

Government of Canada. "CANFORGEN 169/20 CMP 081/20 111211Z DEC 20. Last modified December 2020. http://vcds.mil.ca/apps/canforgens/default-eng.asp?id=169-20&type=canforgen.

Government of Canada. "DAOD 2008-8, Official Use of Social Media." Last modified 9 October 2018. https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/2000-series/2008/2008-official-use-social-media.htm.

Government of Canada. "DAOD 5019-0, Conduct and Performance Deficiencies." Last modified 7 October 2020. https://www.canada.ca/en/department-national-defence/corporate/policies-standards/ defence-administrative-orders-directives/5000-series/5019/5019-0-conduct-and-performance-deficiencies.html.

Government of Canada. "Joint Capabilities – Cyber Security." Last modified 1 March 2021. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/main-estimates-2020-2021/joint-capabilities.html.

Government of Canada. *National Cyber Threat Assessment 2020*. Ottawa: Canadian Centre for Cyber Security, 2020. https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf.

Government of Canada. "New CAF Administrative Order and Military Personnel Instruction on Hateful Conduct." Last modified 24 July 2020. https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2020/07/new-caf-ao-mp-instruction-hateful-conduct.html.

Klippenstein, Ken. "Pentagon Plans to Monitor Social Media of Military Personnel for Extremist Content." *The Intercept*. Last modified 17 May 2021. https://theintercept.com/2021/05/17/military-pentagon-extremism-social media/?utm_medium=social&utm_source=twitter&utm_ campaign=theintercept&fbclid=IwAR0i9V-MbjwaOIqwz36hckw9HaiS4l5td WiC6CVTX8YQ8TM8RND_M1_WYlw.

Pauls, Karen and Ashley Burke. "Military conducted secret investigation of reservist Patrik Mathews as a possible terrorist threat." *CBC News*. Last modified 15 March 2021. https://www.cbc.ca/news/politics/patrik-mathews-canadian-forces-neo-nazi-terrorist-1.5948202.

Pauls, Karen. "Canadian military says new hateful conduct policy will help weed out extremists in the ranks." *CBC*. Last modified 16 July 2020. https://www.cbc.ca/news/canada/manitoba/canadian-military-tool-identifies-hateful-conduct-1.5652276.

Pomerantsev, P. and M. Weiss. "The Menace of Unreality: how the Kremlin Weaponizes Information, Culture and Money." *The Interpreter, Institute for Modern Russia* (2014): 1-44. https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf.

Prier, Jared. "Commanding the Trend: Social Media as Information Warfare." *Air University Press, Strategic Studies Quarterly, Vol. 11, No. 4* (2017): 50-85 https://www.jstor.org/stable/10.2307/26271634.

Ropp, Steve J. "Populism: The Strategic Implications of the Rise of Populism in Europe and South America." *Strategic Studies Institute, US Army War College* (2005): 1-48. https://www.jstor.org/stable/pdf/resrep11716.pdf?refreqid=excelsior%3Ae17e1ee6ebe3b33343108630b2e3e056.

Thompson, Elizabeth. "Facebook partners with Ontario university on 'global network' to counter rise in online hate." *CBC News*. Last modified 28 July 2020. https://www.cbc.ca/news/politics/ facebook-hate-online-extremism-1.5664832.

United States. Department of Homeland Security Office of Intelligence and Analysis. *Right-wing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment.* Homeland Environment Threat Analysis Division, (7 April 2009): 1-9. https://fas.org/irp/ eprint/rightwing.pdf.

Velásquez, N., Manrique, P., Sear, R. *et al.* "Hidden order across online extremist movements can be disrupted by nudging collective chemistry." Scientific Reports 11, 9965 (2021): 1-11. https://doi.org/10.1038/s41598-021-89349-3.

Walt, Gill, and Lucy Gilson. "Reforming the health sector in developing countries: the central role of policy analysis." *Health Policy and Planning 9, no. 4* (1994): 353-370 http://cfc.idm.oclc.org/login?url=https://doi.org/10.1093/heapol/9.4.353.