Countering Russian Subversion during Federal Elections in Canada in the Era of Social Media and Fake News

By Julia M. Hodgins

ITSS Verona Magazine, Vol. 1, no. 1

Spring/Summer 2022

Countering Russian Subversion during Federal Elections in Canada in the Era of Social Media and Fake News

Julia M. Hodgins

To cite this article: Julia M. Hodgins, *Countering Russian Subversion during Federal Elections in Canada in the Era of Social Media and Fake News*, ITSS Verona Magazine, Vol. 1, no. 1, Spring/Summer 2022.

Keywords: Cyber Subversion, Countering, Democracy, Elections, Debunking

ITSS Verona website: https://www.itssverona.it/itss-magazine

LinkedIn: https://www.linkedin.com/company/itss-verona/

Instagram: https://instagram.com/itss_verona?igshid=YmMyMTA2M2Y=

Twitter: https://twitter.com/itssverona

Published online: June 18th, 2022

Executive Summary

Free and well-informed voting is a foundational democratic value; interfering with it is the utmost threat to democracy. The Russian cyber-subversion in the U.S. elections of 2016 had two components (Jamieson, 2020). First, an intrusion and exfiltration of information from the DNC's servers, later exposed in WikiLeaks. Second, a disinformation campaign performed by an army of troll farms, bots, and true Trump-voters over Twitter, Facebook, and news outlets; all together amplified content created to raise fear about Clinton's potential regime, and manipulated opinion which spread in *contagion* mode. Physical and cultural proximity between the cyber and media ecosystems in the U.S. and Canada, aided by intense cross-border traffic, facilitated the contagion spread of fake news about Clinton, exposing Canadians to the effects of disinformation; matter this policy brief aims to prevent (Boutilier, 2020). Although Russian meddling was clear to the U.S government, findings were unsuitable for legal prosecution. While its impact on the voting outcome eludes metrics, an enduring effect is the erosion of trust in democracy, institutions, and the reinvigoration of social fragmentation (Thornton & Miron, 2019).

This policy brief addresses the prevention of Russian interference in Canadian elections, arguing that the best offense is a resilient defence of our national cyber ecosystem, one where the state, the private sector, and civil society cooperatively dissuade intrusions and dismantle disinformation attacks. After defining the policy scope, the four main challenges to thwart this threat are discussed – regulation, obscureness, low-cost access, and uncritical audiences – concluding with policy recommendations to build societal resilience.

Scope

Every four years Canadians elect parliament and Prime Minister based on a blend of experience, feelings, and beliefs brewed with information from diverse news outlets, and discussions sometimes held within online venues; cyberspace entails risks that simultaneously threaten individuals and states (Reveron, 2013). Marcus Kolga suggests: “the ability of Canadians to make informed decisions and participate in civic discourse” as the referent object of foreign interference (Kolga, 2021, p1). Two overarching assumptions guide this analysis. First, democracy is a regulatory ideal, societies move towards or away from it based on their ability to hold healthy debates (Quintanilla, 2021). Second, cyberthreats to democracy are ongoing and increasingly more advanced and technologically sophisticated, hence deterring all threats is unlikely but limiting their benefit undermines motivations (Nye, 2017). Evidence suggests that Canada must articulate a ‘whole-of-society’ approach protecting the integrity of our electoral ecosystem: networks and public debate (Kolga, 2021).

Challenges to countering cyber-subversion

The first challenge is the difficulty to apply regulations. Canada consists - amongst others - of a territory, with political and administrative jurisdiction over the specific geography contained within boundaries. This territoriality is hardly transferable to the electromagnetic spectrum (Melzer, 2021). If a Russian soldier, intelligence agent, or Russia-sponsored actor conducts an attack in our territory, there will be legal and political consequences based on our laws and the international ones, unlike a cyber attack where there is no territoriality to defend but only electromagnetic networks. Also, Canadian law insufficiently addresses foreign cyber-involvement as it requires proven intent, limiting prosecution and sanctions (Statutes of

Canada, 2018); attribution issues hinder accountability. Locations where attackers connect to power, access the Internet, and place servers represent regulation opportunities whenever discovered (Nye, 2010). According to the Law of Neutrality in warfare, neutral states must prevent hostilities conducted from their territory by or sponsored third states , and should support in tracing Russia-sponsored intruders (Melzer, 2021).

Second challenge is cyberspace's obscureness, which underpinned the *hack-and-leak* Russian technique: phished emails that DNC's members clicked on facilitated access for data exfiltration (Thornton & Miron, 2019). Also, Russia concealed identities, surrogated operators, recruited civilian volunteers, disguised intrusions, and denied responsibility, escaping retaliation and prosecution (Jamieson, 2020). The information stolen ultimately undermined the DNC's and the West's reputation (Betz, 2017).

Conversely, obscureness could support deterrence. External attackers do not know networks' layout. Architects should design networks to successfully segment connectivity, thus denying access while remaining operable during cyberattacks (Jamieson, 2020). A combination of Active Defence, fortifying intrusion prevention and incident response, and deterrence by denial and by entanglement to develop interdependence, will deflate motivations for intruding, finally preventing persistent threats (Nye, 2010).

On a related note, social media platforms apply *government-like policies* (Bond, 2020) based on 'opaque' decision-making (Yablon, 2020), which are capable of detecting and de-throttling fake-news disregarding culprits' identity (Kolga, 2021). Whilst useful, this evident asymmetry between private actors and the state erodes public trust while indulges platforms' credibility, making Canadians more prone to Russian trolls' tactics (Jamieson, 2020).

Thirdly, low-cost access to cyberspace drives an ever-growing plethora of actors (Nye, 2010). Russia 'punched hard' the West by recruiting non-state actors at minimum investment. Canadian cyberspace keeps expanding nonetheless. Opposing it, however, will only hurt our country's functionality and undermine the benefits that IT advancement brings to individuals, businesses, communities and countries.

Fourthly, the challenge of uncritical audiences as the ultimate battlefield is their mental and conversational universes (Nye, 2010). The referent object boils down to allowing the public debate to remain genuine, emerging from Canadians' needs, values, and expectations. Information warfare skills have been a Russian asset since the Cold War (Nye, 2010; Kolga, 2021). In 2016, the Russian disinformation army selected, reframed, and amplified mendacious content that misled opinion, raised fear, and influenced voter decisions. While the 89 per cent percent of Canadian households accessing the Internet along with media outlets make them a *juicy* target, their agency could be aggregated into responding to such stimuli by scrutinizing statements and debunking fake news (*Communications Monitoring Report 2019*, 2021). Said response should be spread by community managers and citizens themselves in an opposing contagion, escalating from fact-checking into combating cyber disinformation in kind, proportionately, and efficiently. This response raises the quality of public debate and ensures it remains resilient over time, enduring technological innovations' challenges. A safe assumption for lack of evidence is to consider Canadians' informational literacy profiles being diverse. In this regard, experiences such as those of Taiwan (Smith, 2017), and of *Lie Detectors* transferring Media and Information Literacy (MIL) skills to school students are worthy of review and replication (www.LieDetectors.org, 2018).

Policy recommendations

Deterrence by denial. Invest in ongoing improvement of *Active Defence* protocols and standards, focusing on guarding the Canadian electoral community and communication networks. Educate citizens on hardening protection of their online media accounts consistently. Encourage intense anti-phishing education to electoral community employees and volunteers.

Protect the integrity of the Canadian electoral cyber ecosystem. Regulate designing networks to segment connectivity under diverse scenarios. Develop protocols to identify vulnerabilities and promote cyber hygiene practices to mitigate risks, i.e., hardening access to information; raising encryption and surveillance; controlling user credentials; screening exits; recording the use of applications, educating Canadians into awareness and implementation.

Early detection of threats. Share cyber intelligence within the Canadian intelligence community - both horizontally and vertically - to understand threats and sharpen countering intrusions skills, i.e., reducing discovery timelines, identifying signs of concern, managing incidents, reverse-engineering modus operandi. Assess the creation of AI algorithms to recognize abnormalities within the cyber-traffic of the electoral community.

Protect the integrity of public debate. Coordinate the development of a federal policy on media and information literacy (MIL) partnering with the cyber and the educational ecosystems, adapting successful experiences; integrate MIL content within the education system beginning at elementary, up to professional levels. Work with Canada Radio-Television and Communications Commission in reviewing professional standards to prevent and counter disinformation threats. Promote analytical exercises within community managers and citizens to develop skills for detecting trolls and impersonators; and, cyber-marathons to identify developers able to create

games and applications, capable of transferring skills to identify fake-news and inflammatory narratives; distribute those resources free for all devices amongst Canadian cyberspace networks. Partner with social media corporations and scholars to monitor circulating narratives based on uncorroborated information, users propagating suspicious accounts, and, replicate algorithms that de-throttle and demote such content in online venues lacking those. Create and massively advertise public mechanisms for rectification of wrong statements and declarations to deplore false content and authors.

Cyber-diplomacy. Craft a cooperation agreement with the European Union to share knowledge and lessons learned on MIL. Foster discussions about protecting elections from cyberattacks. Develop cooperation and commercial interdependence with Russia.

Cyber-coercion. Enforce the Law of Neutrality in cyber, should neutral states do not cooperate in tracing threats, a diplomatic sanction could be warranted. Review the application of warfare law to protect non-military targets.

Conclusion

Cyber subversion in elections is facilitated by the difficulty of regulating cyberspace, its obscureness, the low-cost of access, and uncritical audiences. An integrative approach to build resilience will greatly support Canada in deterring potential Russian intrusion and disinformation campaigns for the long term, in two main ways: deterring intrusion to networks, and fostering abilities to counter fake-news.

Reference list

Canada Radio-Television and Communications Commission. (2021, June 13).*"Communications Monitoring Report 2019*. https://crtc.gc.ca/pubs/cmr2019-en.pdf

Betz, D. (2017). *Cyberspace and The State: Toward a Strategy for Cyber-power*. Routledge.

Bond, S. (2020, September 24). Facebook, Twitter Remove More Russian-Backed Fake Accounts Ahead Of Election. *NPR*. https://www.npr.org/2020/09/24/916636508/facebook-twitter-remove-more-russian-backed-fake-accounts-ahead-of-election

Boutilier, A. (2020, November 23). Foreign meddling is a threat to Canadian elections, and politicians should be briefed on it now, former CSIS. *The Toronto Star*. https://www.thestar.com/politics/federal/2020/11/23/foreign-meddling-is-a-threat-to-canadian-elections-and-politicians-should-be-briefed-on-it-now-former-csis-boss-says.html

Government of Canada. Statutes of Canada, no. C-76 (2018). https://laws-lois.justice.gc.ca/PDF/2018_31.pdf

Healey, J. (2012, February 22). Beyond Attribution: Seeking National Responsibility in Cyberspace. *Atlantic Council.* https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/

Jamieson, K. (2020). *Cyberwar: How Russian Hackers and Trolls Helped Elect a President What We Don't, Can't, and Do... Know*. Oxford Univ Press.

Kolga, M. (2021, February). Taiwan Demonstrates How We Can Defend Canadian Democracy Against Information Warfare. *Canadian Global Affairs Institute*. https://www.cgai.ca/taiwan_demonstrates_how_we_can_defend_canadian_democracy_against_information_warfare

LieDetectors.org. (2018). European Commission's drive to tackle Fake News and Digital Disinformation needs fast action on education and independent funding guarantees. *www.LieDetectors.org*. https://lie-detectors.org/wp-content/uploads/2018/03/HLG-MIL-PRESS-RELEASE-European-Commission%E2%80%99s-drive-to-tackle-Fake-News-and-Digital-Disinformation-needs-fast-action-on-education-and-independent-funding-guarantees.pdf

Melzer, N. (2011). *Cyberwarfare and International Law.* UNIDIR. Unidir.org. https://unidir.org/publication/cyberwarfare-and-international-law

Nye, J. (2010). *Cyber Power*. Cambridge: Harvard Kennedy School.

Nye, J. (2017). “Deterrence and Dissuasion in Cyberspace.” *International Security* 41(3), 44-71. doi-org.libproxy.kcl.ac.uk/10.1162/ISEC_a_00266.

Quintanilla, P. (2021, Junio-Julio). Mafias, Estado y democracia. *Revista Ideele*, 298. https://www.revistaideele.com/2021/06/23/mafias-estado-y-democracia/

Reveron, D. S. (2012). *Cyberspace and national security*. Georgetown University Press.

Smith, N. (2017, April 7). Schoolkids in Taiwan Will Now Be Taught How to Identify Fake News. *Time*. http://time.com/4730440/taiwan-fake-news-education/

Thornton, R., & Miron, M. (2019). Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom. *Journal of Cyber Policy*, *4*(2), 257–274. https://doi.org/10.1080/23738871.2019.1640757

Yablon, R. (2020, March 5). Political Advertising, Digital Platforms, and the Democratic Deficiencies of Self-Regulation. *Legal Studies Research Paper Series*, Paper No. 1584 Papers.ssrn.com. https://ssrn.com/abstract=3549366