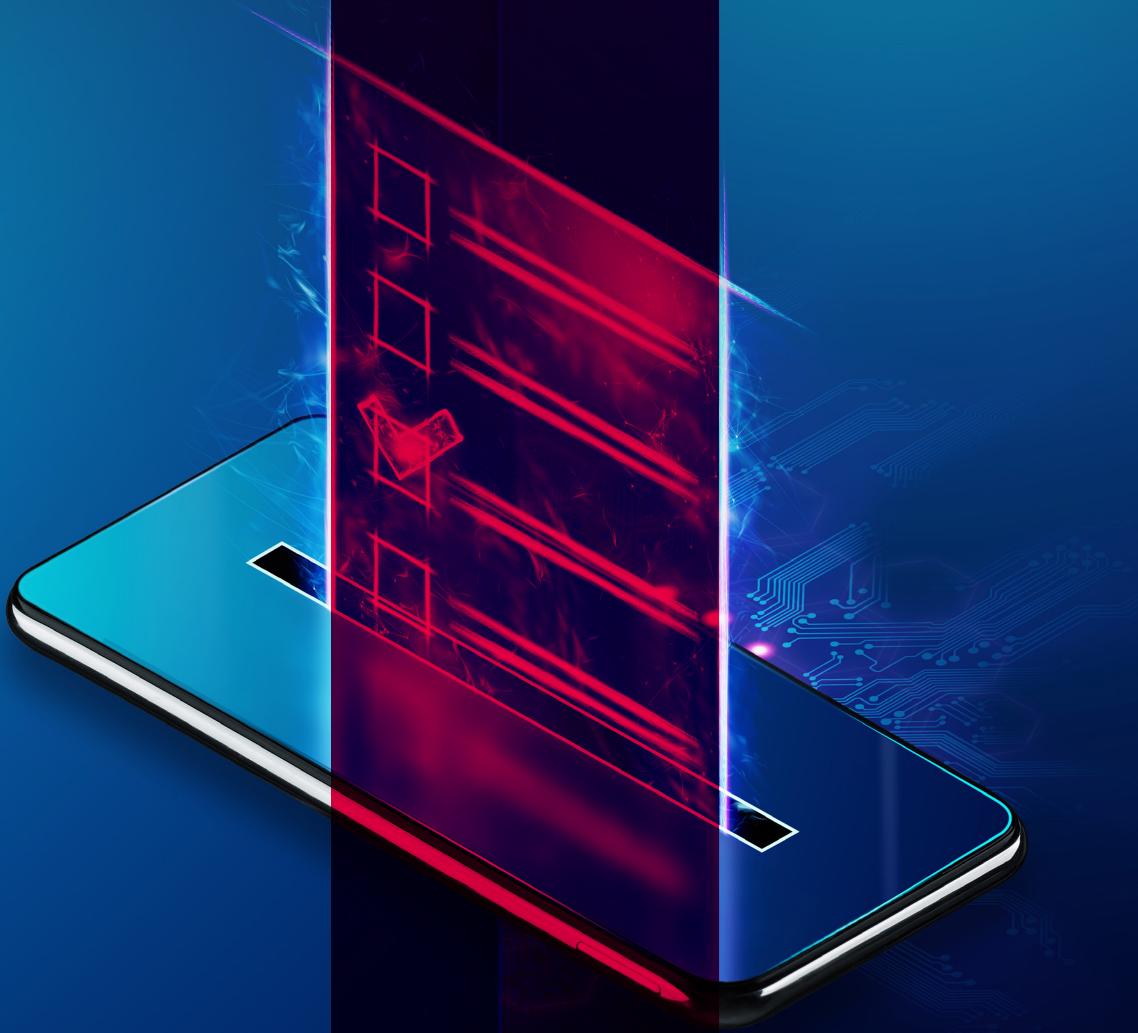
Centre for International Governance Innovation

SPECIAL REPORT

Next-Generation Technology and Electoral Democracy: Understanding the Changing Environment



Centre for International
Governance Innovation

SPECIAL REPORT

Next-Generation Technology and Electoral Democracy: Understanding the Changing Environment

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

KONRAD
ADENAUER
STIFTUNG

This special report was made possible thanks to the financial support of the Konrad-Adenauer-Stiftung (KAS) Canada.

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

For publications enquiries, please contact publications@cigionline.org.

Printed in Canada on Forest Stewardship Council® certified paper containing 100% post-consumer fibre.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Credits

Managing Director and General Counsel Aaron Shull
Manager, Government Affairs and Partnerships Liliana Araujo
Publications Editor Susan Bubak
Senior Publications Editor Jennifer Goyder
Graphic Designer Brooklynn Schwartz

Table of Contents

About the Project

Rapid transformation of the digital sphere has created new and ever more insidious threats to democracy and the electoral process — on a global scale. Growing evidence of foreign influence operations combined with mounting worries over corporate surveillance, the power of platform monopolies and the capabilities of the dark web have challenged government and society in unprecedented ways.

CIGI convened a transdisciplinary team of experts from fields such as computer science, law, public policy and digital communication to formulate a special report for key government and civil society stakeholders. The report uses illustrative case studies and also identifies, evaluates and prioritizes policy development and recommendations. It will serve as a foundational piece for facilitating future collaborative discussions aimed at horizontal policy collaboration and international cooperation to protect democracy.

Acronyms and Abbreviations

AI	artificial intelligence
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAPTCHAs	Completely Automated Public Turing tests to tell Computers and Humans Apart
COVID-19	coronavirus disease 2019
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
G7	Group of Seven
GAC	Global Affairs Canada
GGE	Group of Governmental Experts
IP	intellectual property
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NetzDG	Network Enforcement Act
NSICOP	National Security and Intelligence Committee of Parliamentarians
OEWG	Open-Ended Working Group
RCMP	Royal Canadian Mounted Police
RRM	Rapid Response Mechanism
SITE	Security and Intelligence Threats to Elections
Tor	The Onion Router

Introduction

Aaron Shull and Kailee Hilt

Introduction

Election interference and broader campaigns targeting democratic processes are facilitated by easy access to tools and capabilities embedded in social media and, more nefariously, hosted in the so-called dark web. Studies have indicated the expanding role played by social bots (automated, inauthentic accounts) in election campaigns, although their impact is difficult to measure. At the very least, they can serve to distort opinion, silence minority groups and artificially boost the views of fringe actors and groups.

Canada and Germany are like-minded global partners who champion common values and interests that are foundational to bolstering human rights, democracy and the rule of law, as well as international peace and security. With the significant uncertainty surrounding the advances in emerging technologies, coupled with the surge in disinformation and cyberthreats, there is an inherent need to strengthen our capacity to prevent the spread of malicious cyber activities by foreign actors. Together, Canada and Germany can help build global expertise and understanding on these issues by fostering best practices and measures that build trust and confidence between the two states and beyond.

This special report was the result of a research project conducted in partnership with the Konrad-Adenauer-Stiftung (KAS) Canada. It focuses on advancing policy-relevant thinking related to social media platforms, foreign interference, the (potential) impact of next-generation technology and their interplay with democratic institutions through a combined Canadian and German lens. The project brought together a diverse and interdisciplinary network of scholars and practitioners who are at the forefront of studying the effects of emerging technology on society and politics.

Given the rapid changes to the technological and geopolitical landscape, this project focused on several interrelated key research questions for exploration. These included, but were not limited to:

- → What are the existing and next-generation technologies and tools being deployed to inflict harm on our democracies and democratic institutions?
- → How can quantum cryptography be used to protect an election against hacking or accidental data corruption?
- → What are the various modalities for attributing a cyber operation to a state under international law?
- → What are Canada and Germany doing (or not doing) to protect against foreign interference within the domestic legislative landscape?
- → What are the strategies and lessons learned from social media platform transparency, authenticity and integrity measures that have been implemented to, ostensibly, combat the spread of mis- and disinformation during an election?
- → What is the role of intelligence in addressing foreign threats to democracy? How does the intelligence community, traditionally known for secrecy, engage the public on these threats?
- → What actionable recommendations can be made to policy makers to increase resilience of electoral processes and infrastructure moving forward?

Summary of Key Findings

The rise of advanced technologies such as artificial intelligence (AI) and automation powered by big data is amplifying the threats posed by malign actors with an intent to use cyber tools and capabilities to interfere with electoral systems and democratic processes on a global scale. Canada and Germany, like many Western democracies, are potential targets of adversarial state actors, domestic agitators, commercially motivated groups, or other non-state actors that might wish to interfere with or attempt to undermine our democratic processes and values. As threats continue to emerge and become more insidious, nations need to strengthen and innovate in their approach to defending against and mitigating the risks posed by foreign interference.

This special report explores the impact of current and next-generation technology on elections through a combined Canadian and German lens, while also providing recommendations for understanding and evolving response capabilities in this threat landscape.

This summary incorporates key findings from the seven expert contributions:

- Ulrike Klinger, “Computational Propaganda and the Future of Democratic Elections”;
- Samantha Bradshaw, “Evaluating Platform Responses to New Digital Threats Affecting Canadian Elections”;
- Eric Jardine, “The Dark Web and Democracy: Misinformation and the Use of Tor in Canada, Germany and the United States”;
- Florian Kerschbaum, “Security Considerations in Designing Electronic Voting”;
- Aaron Shull and Kailee Hilt, “International Law and Cyber Election Meddling: Unravelling the Grey Zone”;
- Michael Pal, “Evaluating Applicable Canadian and German Domestic Law to Address the Challenges of Foreign Interference”; and
- Wesley Wark, “Canadian National Security Approaches to Protecting Elections from Foreign Interference.”

As Klinger observes in her detailed contribution to this special report, it is important to understand that the social media environment was not designed for, and may not be conducive to, sincere political discourse; that the real concern needs to be focused not on the phenomenon of automated messaging, but rather on the processes of amplification; and that any regulation of social media platforms needs to proceed from a deeper understanding of how they work in the context of an election setting. Attaining that deeper understanding is currently inhibited by a lack of data access, the absence of standardized identification tools and weak contextual awareness.

In a Canadian context, Bradshaw’s case study identifies three strategies platforms adopted in the lead-up to the 2019 and 2021 federal elections: “inoculation” efforts against disinformation, such as hiring third-party fact-checkers, enhancing political knowledge and media literacy, or reducing the algorithmic visibility of misinformation; strategies that promoted the political participation of Canadians online; and fair campaign practices through improved advertising transparency, enhanced cyber hygiene and anti-harassment policies.

Despite these efforts, clear gaps remain, including algorithmic curation of dis- and misinformation and platform data access. Greater data access for researchers, especially with regard to content flows, metadata and targeting data about political advertising, and data about content moderation, would all be beneficial to ensuring that platform regulation, both formal and informal, can be effective. Given the rising importance of non-traditional media sources, new approaches to supporting digital journalism in Canada are also required. Large social media platforms could play an important role in making financial contributions to a diverse, localized and strong independent media ecosystem.

The dark web, as Jardine demonstrates in his contribution to this special report, offers a more clandestine setting for election interference. By its very nature, the dark web offers anonymity, avoids content moderation and provides a platform for launching disinformation efforts into open public debate. Studies suggest that the coronavirus disease 2019 (COVID-19) pandemic has resulted in an accelerated use of the dark web that portends future trends for contested election processes.

Any democratic electoral system must rely on securing its voting procedures. Increasing adoption of electronic voting systems, largely for the sake of convenience and in an effort to maintain or raise voting levels, introduces new vulnerabilities and challenges. There is the potential for human error and errors introduced into hardware and software. Voting tabulation and communication pose additional challenges for security. As Kerschbaum demonstrates in his case study, strong encryption systems and a layered information architecture will serve as important elements in hardening online electoral voting.

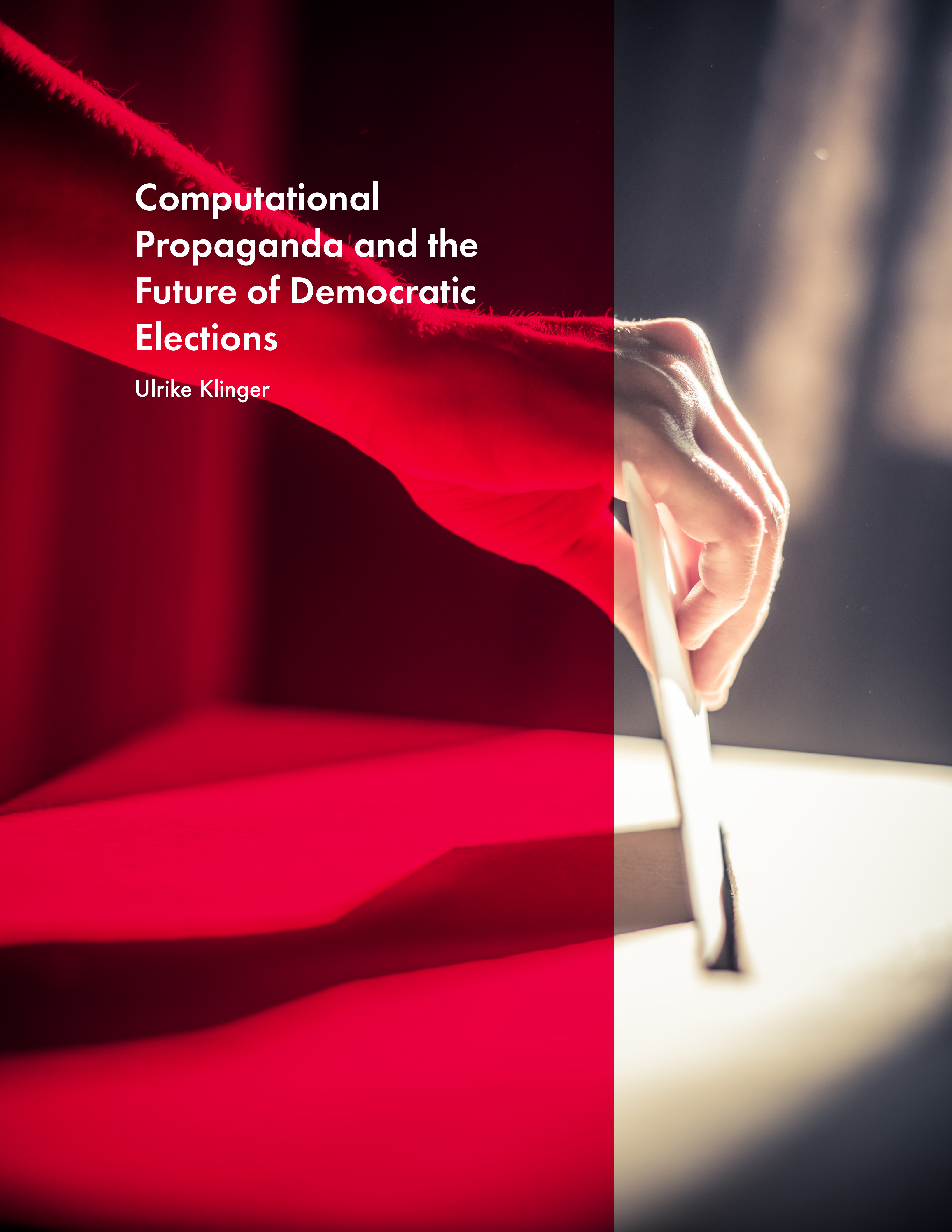
Efforts to mobilize international and domestic laws are clearly crucial to defending against election interference threats. Adversarial states can exploit current grey zones and ambiguities in international law. The dangers of such exploitation are compounded by the disrupted state of geopolitics. Efforts to construct some protective architecture, as the case study by Shull and Hilt illustrates, may include strengthened international law accords, multilateral deterrence and sanction efforts using such platforms as the Group of Seven (G7) Rapid Response Mechanism (RRM), and efforts to improve public understanding.

A comparison of Canadian and German regulatory and legal actions regarding foreign interference suggests the two countries have taken different paths. The Canadian path has involved efforts to tighten campaign finance laws, introduce modest regulation of social media platforms and prohibit the most obvious forms of disinformation. Germany has implemented a legal regime for mandatory takedown of illegal online content as well, and it has banned some political parties and limited their speech rights. Both paths confront questions of impacts of state action on free speech and expression online, as Pal indicates. These different models will likely be closely watched by other democratic regimes looking to balance effective action against foreign interference threats with the preservation of rights, especially regarding speech acts.

Distinct Canadian federal government responses to the threat posed by foreign interference in electoral processes are worthy of international study. These include the creation of a non-partisan early warning system to alert Canadians to signs of major election interference efforts and the publication of forward-looking strategic threat assessments. Canada, as the case study by Wark demonstrates, has also taken a lead through the G7's RRM and currently hosts the RRM secretariat. Given the prominent role played by communications intelligence organizations such as Canada's Communications Security Establishment (CSE) and Germany's Bundesamt für Sicherheit in der Informationstechnik (BSI), greater sharing of information and best practices outside the Five Eyes (a security alliance consisting of Australia, Canada, New Zealand, the United Kingdom and the United States) seems warranted.

Given the technological enabling of foreign interference in elections and democratic processes, democratic states need to find a suite of policies that can harden their processes without upending rights. As the case studies in this collection suggest, those policies need to be wide-ranging and involve technical, legal and regulatory, and informational efforts. A changing environment for political discourse represented by the advent of social media platforms and increasing aggressiveness by foreign state adversaries must be addressed. Ensuring that stable democracies with shared values, such as Canada and Germany, understand each other's approaches and can share best practices offers valuable ways to confront the current and future menace of foreign electoral interference.

Moving forward, this special report will be used to facilitate meaningful and lasting policy impact through targeted engagement with policy makers and an international network of experts. Knowledge translation and exchange will serve as an important avenue to discuss strategies for moving forward. The special report will emphasize areas where intervention is most needed, who will need to lead these initiatives, the resources necessary, the possible barriers to implementation, the methods of optimal communication, and the procedures that can be used to monitor progress and success.



Computational Propaganda and the Future of Democratic Elections

Ulrike Klinger

Key Findings

→ Computational propaganda may impact election campaigns in various ways, for example, by distorting the perceptions of the opinion climate, silencing minority groups and artificially amplifying fringe actors or opinions.

→ Identifying automated accounts (social bots) is a tedious and often frustrating activity due to three impactful limitations that researchers face: lack of data access, the absence of standardized identification tools and the ground-truth problem.

→ It is not the automation per se that can be a threat to democratic discourse but the artificial amplification of certain messages and authors. As the average users of social media do not post and comment very much, it does not need automation to be an outlier, a hyperactive user or a superspreader.

→ What happens on social media is largely non-transparent and unobservable for science and society, as platforms currently provide no or very limited access to their archives and data.

Introduction

Just a few weeks after the 2021 German federal election, an investigative research team of journalists found that about one-third of the radical populist party Alternative for Germany's most active commenters on Facebook were actually fake or inauthentic accounts (Baumgärtner et al. 2022). The existence of inauthentic and automated social media accounts comes as no surprise to researchers in the field (see, for example, Keller and Klinger 2018; Rheault and Musulan 2021). However, it illustrated again how common and rather easy it is to artificially inflate a party's or candidate's support base on social media and to create loud minorities.

Election campaigning is persuasive communication and thus necessarily always entails some form of opinion "manipulation." Despite its negative connotation, manipulation is a normal part of public discourse and not harmful per se. Democratic societies are plural and open; they thrive on the diversity of opinions and ideas, from contestation and conflict; and must also tolerate deviant voices and factually untrue content (for example, conspiracy theories). However, the rise and ubiquity of digital communication has made it fairly easy for state and non-state actors to engage in computational propaganda (i.e., "the assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion" [Woolley and Howard 2016]), which poses a potential threat to fair and equal elections and the basic functions of the public sphere as a marketplace of ideas.

Numerous studies from various countries employing a broad methodological toolset have shown that social bots (automated, inauthentic accounts) have been active in election campaigns in recent years (for example, Bastos and Mercea 2019; Keller and Klinger 2018; Boichak et al. 2021; Ferrara 2017). Not only have bots turned social media into a challenging environment for elections, but female candidates and candidates from minority groups also face hate campaigns, harassment and uncivil behaviour on social media that may discourage these groups from participating in electoral contests and silence diverse voices (Krook and Sanín 2020; Rheault, Rayment and Musulan 2019; Beltran et al. 2021; Bradshaw and Henle 2021). Computational propaganda may impact election campaigns in various ways, for example, by distorting the perceptions of the opinion climate, silencing minority groups and artificially amplifying fringe actors or opinions.

Social media plays an increasingly important role in opinion formation processes. In Germany, the internet has become the main news source for all age groups under 45, with social media as the most relevant news source online (Hölig and Hasebrink 2019, 11). For 22 percent of Germans, Facebook is a news source; for 23 percent of 18- to 24-year-old Germans, Instagram is a news source (ibid., 7).[1] The information citizens find on social media and through search engines is highly personalized, algorithmically curated and consists of free, non-paywalled content. Citizens encounter loud minorities, automated content, junk news and

[1] See www.digitalnewsreport.org/interactive/.

false information. But seeing is not believing, and opinion formation is a very complex process.

Defining Social Bots

Social bots are partially or fully automated Twitter accounts. Other platforms focus not so much on automation but on inauthentic or fake accounts. Most research on this topic centres on Twitter because data access is comparatively better than on other platforms. Automation is not problematic per se; many news organizations also use automated accounts. Twitter itself reports "malicious automation" in its transparency reports and deletes accounts that have been discovered and classified as maliciously manipulative. However, the numbers Twitter reports and the accounts deleted cannot be verified from the outside due to the lack of data access (Twitter does not provide access to data on deleted accounts). Without the opportunity to validate these numbers, one can only conclude that malicious manipulation by automated accounts exists to a considerable extent. While there are good reasons not to make this data publicly available in general (for example, it may enable malevolent actors to reverse-engineer and game the platform algorithms), independent researchers should be able to scrutinize the platform's self-reports and use this data as training data to develop better detection tools.

Not only identifying "bots" but also defining them is a difficult task, as this term has been used to describe a broad variety of automation. With the number of studies on this topic increasing, researchers are seeking more clarity regarding validity, definitions, the different types of bots and their activities. Based on a broad literature review, Stefan Stieglitz et al. (2017) conclude that, unlike other types of bots (such as chatbots), social bots are characterized by their high degree of human behaviour imitation and malicious intent. Robert Gorwa and Douglas Guilbeault (2018, 11) have created a comprehensive typology differentiating social bots from other automated programs, such as web crawlers and chatbots, noting that social media accounts that "exhibit a combination of automation and of human curation, often called 'cyborgs'" are the most challenging for researchers. Even though it has been shown that social bots are not (yet) as successful as humans in engaging other users in meaningful discussions, messages from bots seem to get retweeted as often as those from humans, indicating that Twitter users cannot easily distinguish between bots and humans (Ferrara 2018). In addition, there is a variety of bots that are not yet regarded as bots in this literature, such as automated accounts in games or mobile phone assistants (Grimme et al. 2017). As social bots are evolving alongside other technological innovation, such as machine learning and AI, one can expect to see new forms of automated communication and that it will become even more difficult to detect "malicious automation" in the future.

Automation and the Identification of Social Bots

Identifying automated accounts is a tedious and often frustrating activity due to three impactful limitations that researchers face: lack of data access, the absence of standardized identification tools and the ground-truth problem. Furthermore, studying social bots means tracing a moving target: data and tools age rapidly, making replication nearly impossible.

What happens on social media is largely untransparent and unobservable for science and society. While Twitter opened an academic track to access its archive via its application programming interface in early 2021, all other platforms currently provide no or very limited access to their archives and data. The data Twitter offers contains few metadata and hardly ever contains reliable geographic data. This limits the features one can analyze in searches for automated accounts. Facebook and other platforms use a distant or hostile approach toward research, further limiting or ruling out data access for researchers. The current situation means that independent research can only peek through the keyhole, but not adequately analyze discourse dynamics and information flows on social media platforms, let alone across different platforms.

When it comes to bot-detection tools, scholars can use dozens of different approaches. They can try to build their own detection instruments or use tools built by computer scientists as well as other easy-to-employ methods, ranging from single indicator methods, such as the number of published tweets per day, to multiple indicator methods based on machine learning, including hundreds of variables. The available tools are all based on different premises and definitions, and their results reflect these settings. Running several bot-detection methods on the same data set shows that each method identifies different accounts as bots with hardly any overlaps (Martini et al. 2021; Schuchard and Crooks 2021).

When using methods based on machine-learning and scoring systems, bot detection must define a threshold score that draws the line between automated and non-automated accounts. Consequently, the number of bots identified depends very much on this threshold. For instance, had the authors in their study on bots in the 2017 German election (Keller and Klinger 2018) set the threshold at 0.43, like Stefan Wojcik et al. (2018) from the Pew Research Center, they would have found that 37 percent of the followers of German political parties during the 2017 election campaigns were bots, instead of roughly 10 percent at a threshold of 0.75. The different tools and thresholds used in the existing studies mean that the authors cannot meaningfully compare their results.

Finally, the authors can compare detection tools against each other, but there is no way to validate them. The authors have no way of knowing how many bots are out there, and manual validation through digital forensics does not easily scale to large data sets. With the data and methods available to researchers, it is not possible to make exact statements about the precise number or the actual influence of social bots; rather, the existing studies are approximations. These studies show that automated Twitter accounts have been active in political discourses (such as before elections and referendums). However, to the author's knowledge, there is no empirical evidence that automated accounts have had a massive, decisive impact on the formation of opinion, let alone election outcomes so far. The authors' own study on the 2017 Bundestag elections showed that there were only a few active bots among the parties' followers, who also did not disseminate any political content (Keller and Klinger 2018). Thus, social bots remain a *potential* threat.

Beyond Automation: Superspreaders and Loud Minorities

While it is difficult to detect automated accounts as one form of computational propaganda, it may not even be necessary. After all, it is not the automation per se that can be a threat to democratic discourse but the artificial amplification of certain messages and authors — the "astroturfing" where one may expect grassroots mobilization and the gaming of algorithms through hyperactive interaction patterns. As the average users of social media do not post and comment very much, it does not need automation to be an outlier, a hyperactive user or a superspreader. Moreover, Soroush Vosoughi, Deb Roy and Sinan Aral (2018) showed that automated and non-automated accounts are on par in spreading disinformation.

Research has shown that hyperactive users — automated or non-automated — on social media platforms are shaping discourses with a high share of interactivity and by distributing opinions that clearly diverge from other users (Papakyriakopoulos, Serrano and Hegelich 2020). Thereby, they create loud minorities, possibly influencing the opinion climate by setting spiral-of-silence dynamics in motion (i.e., minority groups becoming louder and radical groups becoming more aggressive in their communication as they falsely perceive themselves to be a silent majority; see Scheufele and Moy 2000). Researchers applying agent-based modelling in networks concluded that in some settings, networks with only two to four percent bots are enough to turn the opinion climate; they can easily "sway public opinion — or the expression thereof" (Ross et al. 2019, 14). But this trend could also be achieved without automation. In the German-language #MeToo discourse on Twitter, 35 percent of all interactions (retweets, @mentions, replies) were accounted for by only 1.1 percent of the accounts involved, which were particularly active and primarily spread anti-feminist and racist narratives, thus hijacking the hashtag as a free rider (Martini 2020; Knüpfer, Hoffmann and Voskresenskii 2020). Similarly, the authors' analysis of a far-right campaign against the 2018 UN Global Compact for Migration in Germany showed that 0.28 percent of accounts posting on Twitter about this topic generated more than

20 percent of all retweets. These superspreaders are not all the same; they are not organizational or media accounts, seemingly individual users with varying follower reach. Presenting an extreme case of this pattern, a study by the Center for Countering Digital Hate (2021, 6–7) found that 65 percent of disinformation about COVID-19 vaccines (73 percent on Facebook, 17 percent on Twitter) can be traced to only 12 accounts — the "disinformation dozen." This amplification, automated or not, is certainly a problem for public discourse in democratic society and needs to be addressed by platform regulation. After all, the algorithmic systems behind most platforms play a supportive role in this amplification process. Facebook's algorithms, as one case in point, are built on the principle of user engagement. Information that attracts user engagement will be considered relevant by Facebook's algorithms, further increasing the visibility and reach of such artificially amplified messages.

Options for Governance

The internet, and social media in particular, enables anyone and everyone to communicate publicly worldwide and to reach a larger, even international, audience with content. Against this structural background, content that is not necessarily conducive to democracy or originated from inauthentic sources or networks, cannot be completely prevented or even banned. Anyone can place political advertisements on social media, start coordinated activist networks, or use automated Twitter accounts to disseminate or share content, with a small investment of resources. Those who want to spread lies or engage in "dark participation" (Quandt 2018) will always find ways to do so.

Social media does not exist to promote political dialogue, democratic participation or opinion formation. It is not a democracy machine. It exists to make money and is designed accordingly, reflecting platforms' business models. It transforms our lives into marketable data sets: our daily lives; our networks of friends and acquaintances; and the things we do, say or share are the resources for creating immense wealth (Zuboff 2019). This system can cause collateral damage for democracies. The key question is how can we minimize the negative effects for democratic societies.

Social bots are no longer unknown and obscure creatures but have entered the political agenda. For example, in December 2018, the European Commission (2018, 4) released its *Action Plan against Disinformation*, addressing social bots as a technique "to spread and amplify divisive content and debates on social media" that might be used to disseminate disinformation. In the same month, Ralph Brinkhaus, leader of the German conservative Christian Democratic Union parliamentary group, called for legislative action against social bots, including legal measures forcing platforms to label automated accounts as bots (dw.com 2018). The German Interstate Media Treaty (Medienstaatsvertrag) of 2020 explicitly introduces an obligation for social media platforms to flag automated content in article 18(3):

> Providers of telemedia in social networks are obliged to specify the fact of automation in the case of content or messages created automatically by means of a computer program, provided that the user account used for this purpose appears to have been made available by natural persons. It must be made legibly clear, with or before the content or the message, that it was automatically created and sent using a computer programme that controls the user account. "Creation" within the meaning of this provision does not only mean when content and messages are automatically generated immediately before they are sent, but also when prefabricated content or a pre-programmed message is used automatically with the transmission.[2]

While this regulation demonstrates the good intentions to safeguard public discourse and find a way to incentivize social media platforms to self-regulate, it also indicates the limited understanding of technology and computational methods among regulators. In fact, with the available data and tools, it would be impossible to make a valid and legally sound judgment about the degree of automation of an account. As regulation does

[2] See *Interstate Media Treaty (Medienstaatsvertrag)*, 28 April 2020, entered into force 7 November 2020, online: <www.die-medienanstalten.de/fileadmin/user_upload/Rechtsgrundlagen/Gesetze_Staatsvertraege/Interstate_Media_Treaty_en.pdf>.

not only entail setting rules but also enforcing the rules and sanctioning non-compliance, the question here is how to monitor the flagging of social bots as established in the treaty. As things currently stand, state regulators would just have to believe social media platforms and trust their flagging practices and reported numbers. A better way to counter computational propaganda would be to target amplification, not automation.

Targeting amplification rather than automation would mean moving beyond the question of whether accounts are social bots or not. This approach would start with platforms getting better at understanding bias in their algorithms. For instance, Twitter recently found in an internal study that tweets from the political right and right-leaning news outlets are amplified by Twitter's algorithms, but the company does not yet understand why (Chowdhury and Belli 2021; Huszár et al. 2022). Similarly, the Facebook Papers (internal documents revealed by whistleblower Frances Haugen) pointed to Facebook's algorithms as driving divisive content (Milmo 2021). Addressing this issue also means focusing on the behaviour rather than the characteristics of accounts, particularly outlier accounts and superspreaders, and their role in public discourses. While it is not a problem in itself that some users, perhaps activists, are posting at a much higher volume and frequency than other users, it is remarkable to see how extremely small numbers of users can drive discourse dynamics and networked campaigns. This phenomenon also points to the need for increased efforts in digital literacy training, not only for teenagers and students but also for older people and professional multipliers, such as journalists. We need more of what Bruce Bimber and Homero Gil de Zúñiga (2020) have termed "epistemic editing": truth-biased filtering of information before broadcasting it to a mainstream audience, publicly identifying false claims and providing information about the sources of truth claims — all classic functions of journalism. This means democratic societies need better gatekeeping to prevent amplified campaigns on social media platforms from finding their way into mainstream media and discourse by mistaking them for authentic, grassroots movements. In this current marketplace of ideas, some users are much louder than others, amplified by algorithms and their own hyperactive behaviour, and society needs to find new ways to attribute relevance and legitimacy in such dissonant public spheres (Pfetsch 2018).

To safeguard the future of democratic elections and to counter the negative collateral effects of social media platforms, we need a combined and comprehensive effort involving social media platforms, political actors, civil society — and researchers. To find effective ways of regulation, one needs to understand how the object of regulation works. To safeguard discourse dynamics and information flows on social media, we need to know more about them. One may find it ironic that research has not only moved on from studying social bots as a phenomenon in itself, but also started to actively use neutral bots to study bias in platform algorithms (Chen et al. 2021).

An important step forward would be to set up independent, constant and comparative monitoring of public (not private) election-related communication on social media that is well-funded and endowed with adequate data access. Currently, the monitoring of election campaigns is mostly event- and project-driven, highly fragmented and under-institutionalized. Platform regulation means incentivizing companies to counter amplification of harmful content (such as disinformation about vaccines) and cooperate in safeguarding election campaigns from external and internal computational propaganda.

Works Cited

Bastos, Marco T. and Dan Mercea. 2019. "The Brexit Botnet and User-Generated Hyperpartisan News." *Social Science Computer Review* 37 (1): 38–54. doi:10.1177/0894439317734157.

Baumgärtner, Maik, Roman Höfner, Ariane Fries and Ann-Katrin Müller. 2022. "Die AfD ist ein digitaler Scheinriese." Spiegel, January 21. www.spiegel.de/politik/deutschland/afd-in-sozialen-netzwerken-der-digitale-scheinriese-a-f6563fee-7e10-4891-9f99-f3c6a8d02a88.

Beltran, Javier, Aina Gallego, Alba Huidobro, Enrique Romero and Lluís Padró. 2021. "Male and female politicians on Twitter: A machine learning approach." *European Journal of Political Research* 60 (1): 239–51.

Bimber, Bruce and Homero Gil di Zúñiga. 2020. "The unedited public sphere." *New Media & Society* 22 (4): 700–15.

Boichak, Olga, Jeff Hemsley, Sam Jackson, Rebekah Tromble and Sikana Tanupabrungsun. 2021. "Not the Bots You Are Looking For: Patterns and Effects of Orchestrated Interventions in the U.S. and German Elections." *International Journal of Communication* 15: 814–39.

Bradshaw, Samantha and Amélie Henle. 2021. "The Gender Dimensions of Foreign Influence Operations." *International Journal of Communication* 15: 4596–618.

Center for Countering Digital Hate. 2021. "The Disinformation Dozen: Why Platforms Must Act on Twelve Leading Online Anti-vaxxers." https://252f2edd-1c8b-49f5-9bb2-cb57bb47e4ba.filesusr.com/ugd/f4d9b9_b7cedc0553604720b7137f8663366ee5.pdf.

Chen, Wen, Diogo Pacheco, Kai-cheng Yang and Filippo Menczer. 2021. "Neutral bots probe political bias on social media." *Nature Communications* 12: 1–10. www.nature.com/articles/s41467-021-25738-6.

Chowdhury, Rumman and Luca Belli. 2021. "Examining algorithmic amplification of political content on Twitter." *Twitter Blog*, October 21. https://blog.twitter.com/en_us/topics/company/2021/rml-politicalcontent.

dw.com. 2018. "Gemany mulls crackdown on social media bots." dw.com, December 16. www.dw.com/en/germany-mulls-crackdown-on-social-media-bots/a-46764545.

European Commission. 2018. *Action Plan against Disinformation.* Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. JOIN(2018) 36 final. https://eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf.

Ferrara, Emilio. 2017. "Disinformation and social bot operations in the run up to the 2017 French presidential election." *First Monday* 22 (8): 1–33. doi:10.5210/fm.v22i8.8005.

———. 2018. "Measuring Social Spam and the Effect of Bots on Information Diffusion in Social Media." In *Complex Spreading Phenomena in Social Systems: Influence and Contagion in Real-World Social Networks*, edited by Sune Lehmann and Yong-Yeol Ahn, 229–55. Cham, Switzerland: Springer.

Gorwa, Robert and Douglas Guilbeault. 2018. "Unpacking the Social Media Bot: A Typology to Guide Research and Policy." *Policy & Internet* 12 (2): 225–48. doi:10.1002/poi3.184.

Grimme, Christian, Mike Preuss, Lena Adam and Heike Trautmann. 2017. "Social Bots: Human-Like by Means of Human Control?" *Big Data* 5 (4): 279–93.

Hölig, Sascha and Uwe Hasebrink. 2019. *Reuters Institute Digital News Report 2019*. June. Hamburg, Germany: Verlag Hans-Bredow-Institut. https://hans-bredow-institut.de/uploads/media/default/cms/media/x52wfy2_AP47_RDNR19_Deutschland.pdf.

Huszár, Ferenc, Sofia Ira Ktena, Conor O'Brien, Luca Belli, Andrew Schlaikjer and Moritz Hardt. 2022. "Algorithmic amplification of politics on Twitter." *Proceedings of the National Academy of Sciences of the United States of America* 119 (1): 1–6. www.pnas.org/content/pnas/119/1/e2025334119.full.pdf.

Keller, Tobias R. and Ulrike Klinger. 2018. "Social Bots in Election Campaigns: Theoretical, Empirical, and Methodological Implications." *Political Communication* 36 (1): 171–89. doi:10.1080/10584609.2018.1526238.

Knüpfer, Curd, Matthias Hoffmann and Vadim Voskresenskii. 2020. "Hijacking *MeToo*: transnational dynamics and networked frame contestation on the far right in the case of the '120 decibels' campaign." *Information, Communication & Society* 1–19.

Krook, Mona Lena and Juliana Restrepo Sanín. 2020. "The Cost of Doing Politics? Analyzing Violence and Harassment against Female Politicians." *Perspectives on Politics* 18 (3): 740–55.

Martini, Franziska. 2020. "Wer ist #MeToo? Eine netzwerkanalytische Untersuchung (anti-) feministischen Protests auf Twitter." *Medien & Kommunikationswissenschaft* 68 (3): 255–72.

Martini, Franziska, Paul Samula, Tobias R. Keller and Ulrike Klinger. 2021. "Bot, or not? Comparing three methods for detecting social bots in five political discourses." *Big Data & Society* 8 (2): 1–13. doi:10.1177/20539517211033566.

Milmo, Dan. 2021. "Facebook revelations: what is in cache of internal documents?" *The Guardian*, October 25. www.theguardian.com/technology/2021/oct/25/facebook-revelations-from-misinformation-to-mental-health.

Papakyriakopoulos, Orestis, Juan Carlos Medina Serrano and Simon Hegelich. 2020. "Political communication on social media: A tale of hyperactive users and bias in recommender systems." *Online Social Networks and Media* 15: 1–15. www.sciencedirect.com/science/article/pii/S2468696419300886.

Pfetsch, Barbara. 2018. "Dissonant and Disconnected Public Spheres as Challenge for Political Communication Research." *Journal of the European Institute for Communication and Culture* 25 (1–2): *59–65*. doi:10.1080/13183222.2018.1423942.

Quandt, Thorsten. 2018. "Dark Participation." *Media and Communication* 6 (4): 36–48.

Rheault, Ludovic and Andreea Musulan. 2021. "Efficient detection of online communities and social bot activity during electoral campaigns." *Journal of Information Technology & Politics* 18 (4): 324–37.

Rheault, Ludovic, Erica Rayment and Andreea Musulan. 2019. "Politicians in the line of fire: Incivility and the treatment of women on social media." *Research & Politics* 6 (1): 1–7. doi:10.177/2053168018816228.

Ross, Björn, Laura Pilz, Benjamin Cabrera, Florian Brachten, German Neubaum and Stefan Stieglitz. 2019. "Are social bots a real threat? An agent-based model of the spiral of silence to analyse the impact of manipulative actors in social networks." *European Journal of Information Systems* 28 (4): 394–412. doi:10.1080/0960085X.2018.1560920.

Scheufele, Dietram A. and Patricia Moy. 2000. "Twenty-five years of the spiral of silence: A conceptual review and empirical outlook." *International Journal of Public Opinion Research* 12 (1): 3–28. doi:10.1093/ijpor/12.1.3.

Schuchard, Ross J. and Andrew T. Crooks. 2021. "Insights into elections: An ensemble bot detection coverage framework applied to the 2018 U.S. midterm elections." *PLoS One* 16 (1): 1–19

Stieglitz, Stefan, Florian Brachten, Björn Ross and Anna-Katharina Jung. 2017. "Do Social Bots Dream of Electric Sheep? A Categorisation of Social Media Bot Accounts." *Australasian Conference on Information Systems*. https://arxiv.org/abs/1710.04044.

Vosoughi, Soroush, Deb Roy and Sinan Aral. 2018. "The spread of true and false news online." *Science* 359 (6380): 1146–51. doi:10.1126/science.aap9559.

Wojcik, Stefan, Solomon Messing, Aaron Smith, Lee Rainie and Paul Hitlin. 2018. "Bots in the Twittersphere." Pew Research Center, April 9. www.pewresearch.org/internet/2018/04/09/bots-in-the-twittersphere/.

Woolley, Samuel C. and Philip N. Howard. 2016. "Political Communication, Computational Propaganda, and Autonomous Agents." *International Journal of Communication* 10: 4882–90. http://ijoc.org/index.php/ijoc/article/view/6298/1809.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY: PublicAffairs.

Evaluating Platform Responses to New Digital Threats Affecting Canadian Elections

Samantha Bradshaw

Key Findings

- Social media has raised several concerns for the integrity and security of elections in Canada and around the world. From foreign influence operations to the amplification of extremist points of view, social media has become a key threat vector for disrupting democracy.
- Platform self-regulation has become an increasingly prominent strategy used to combat these harms. In addition to incremental changes made to their terms of use and community guidelines, platforms adopted three types of country-specific policies in the lead-up to the 2019 and 2021 federal elections in Canada:
  - policies to inoculate users against disinformation, such as hiring third-party fact-checkers, enhancing political knowledge and media literacy, or reducing the algorithmic visibility of misinformation;
  - policies to encourage political participation, such as promoting civic engagement or combatting hate speech and suppressive content; and
  - policies to ensure fair political campaigning, such as improving advertising transparency and cyber hygiene and anti-harassment policies.
- Many of these private self-regulatory responses have been important for improving the integrity and security of the Canadian digital public sphere. But there are still some gaps, challenges and areas of improvement for private self-regulation, particularly around the algorithmic curation of misinformation, data access and transparency, and supporting digital journalism in Canada.

Introduction

Since 2016, technology companies have taken several private self-regulatory steps to combat disinformation and foreign influence operations (Taylor, Walsh and Bradshaw 2018). These strategies include:

- creating new policies against election-related misinformation;
- establishing relationships with third-party fact-checkers;
- labelling false or misleading content;
- using AI and machine-learning technologies to help identify harmful content;
- making algorithmic adjustments to demote certain kinds of content in news feeds or recommendation systems;
- investing in media literacy initiatives; and
- improving company transparency through reporting, the creation of ad archives and the publication of high-profile takedowns.

Social media companies have also launched country-specific initiatives to combat the increasing threats to democracy. These initiatives often involve working with local partners to address country-specific problems, such as violence against minority or marginalized communities. Unlike the global initiatives or changes platforms make to their policies and community guidelines, some country-specific initiatives can be temporarily established to support a particular election or high-profile political event.

Platform self-regulatory approaches aim to combat the wide range of problems facing the quality and health of the overall information ecosystem. However, these self-regulatory approaches are often criticized for lacking transparency in decision making or accountability if self-regulatory processes fail to address problems. In addition to self-regulatory responses, governments have also imposed or updated new laws to address issues including the spread of mis- and disinformation online, foreign interference, hate speech, or political advertising and spending (in Michael Pal's contribution to this special report, he provides an overview of some of these laws in the Canadian and German context).

This case study explores the private self-regulatory measures that platform companies took in conjunction with the Canadian government and civil society in the lead-up to the 2019 and 2021 federal elections. While Canadians use many social media platforms for news and politics, this report focuses on three of the largest in Canada in terms of use (Facebook, Twitter and Google/YouTube). The author draws on information from platform blogs and company announcements, which were released in the lead-up to the 2019 and 2021 federal elections in Canada to inform Canadian citizens, media and policy makers of the steps that each company was taking to improve the information ecosystem ahead of the vote.[3]

Evaluating Platform Self-Regulatory Responses to Digital Threats in Canadian Elections

Heading into the Canadian federal elections in 2019 and 2021, Facebook, Twitter and Google/YouTube worked with Canadian federal agencies, academics and civil society to implement policies and safeguards. More than 30 initiatives were established by the three platforms to address three main areas of concern: inoculating Canadians against disinformation; promoting political participation across Canadian society; and safeguarding political campaigning in Canada. Table 1 summarizes the platform initiatives.

Inoculating Users against Disinformation

One of the biggest challenges social media has raised for democracy is the spread of disinformation online. Canadian media and policy makers have been particularly concerned with how false, misleading or highly biased information might inhibit citizens' ability to formulate political opinions and therefore effectively participate in politics. Some of these concerns focused on foreign interference and the way that state actors might use social media to disrupt elections for geopolitical gain (CSE 2021). Others focused on social media itself and how the features of these surveillance-driven and attention-demanding technologies might prioritize rumour and sensation over news and information (Bernhard 2021). Platforms took several steps to address these concerns in Canada, including working with third-party fact-checkers to combat mis- and disinformation, enhancing political knowledge and strengthening media literacy and journalism, and reducing the algorithmic visibility of misinformation.

Combatting Mis- and Disinformation through Third-Party Fact-Checkers

One strategy, used primarily by Facebook, was to employ fact-checkers to help inoculate users against disinformation. During the 2019 federal election, Facebook partnered with third-party fact-checker Agence France-Presse to fact-check election-related information in both French and English.[4] In February 2020, Facebook also expanded its collaborations with third-party fact-checkers to include a partnership with Radio-Canada's Les Décrypteurs to fact-check information in the Canadian context.[5] Facebook was the only platform to implement partnerships with Canadian third-party fact-checkers; both Google and Twitter did not launch any Canadian-specific partnerships to fact-check information, but both companies have other global or localized fact-checking partnerships that could have been relevant for Canadian elections.

While fact-checking is important for promoting high-quality and accurate news and information about politics, there are several important questions about its efficacy, especially in a digital environment. Fact-checked information usually appears as an informational label under content shared on social media. However, research about labels demonstrates mixed results. Labels disputing the accuracy of content can reduce how often it gets shared (Mena 2020), but research has also

[3] Canadian-specific initiatives that fall outside of the election periods are not covered in this report, nor are incremental changes made to company policies on a global level.

[4] See https://facebookcanadianelectionintegrityinitiative.com.

[5] Ibid.

Table 1: Overview of Canadian-Specific Platform Policies to Combat Digital Challenges to Democracy

Policies	Facebook	Twitter	Google/YouTube
Inoculating Canadians against disinformation			
Third-party fact-checking	Partnership with Agence France-Presse to fact-check election-related information in French and English Partnership with Radio-Canada's Les Décrypteurs to fact-check political information in Canada		
Enhancing political knowledge, media literacy and journalism	Voter information notifications link to Elections Canada's website from News Feed Worked with MediaSmarts to disseminate bilingual advertising to help people make informed decisions about news Pages can no longer self-identify as "news"	Compiled a list of hashtags and candidates to follow for information about the federal election Notifications about the election were sent on a subscription basis to help people stay informed	Promoted links to relevant information on election day Livestreamed leaders' debates on YouTube Hosted knowledge panels for political candidates Launched Google News Showcase, a product and licensing program that provides space for newsrooms to curate content for readers across Google News and Discover Paid for paywalled content so Canadians can access more news Provided journalist training in digital skills Supported business and news entrepreneurs for journalism in Canada
Reducing the algorithmic visibility of misinformation	Reduced political content in Canadian News Feed		Elevated authoritative services for election news and information in Google Search and YouTube's breaking news and top news products

Policies	Facebook	Twitter	Google/YouTube
Promoting political participation across Canadian society			
Promoting civic engagement	Election day reminders were sent the night before and day of an election, with a button to find polling stations “I voted” story stickers and profile frames and augmented reality effects (designed in partnership with Apathy is Boring)	Worked with Elections Canada to launch a custom Twitter emoji for the election	Created a link to Google and YouTube homepages with information on how to vote
Combatting hate speech and harmful or suppressive content	Designated hate organizations and figures in Canada and banned them from having a presence on Facebook and Instagram Partnered with Global Network Against Hate Worked with the Centre for Israel and Jewish Affairs and Canadian Jewish Holocaust Survivors and Descendants to remove misleading or false information about the Holocaust Added Indigenous-specific hate terms to hate speech policies	Launched “hide replies” feature (tested in Canada but eventually rolled out to everyone)	

Policies	Facebook	Twitter	Google/YouTube
Safeguarding political campaigning in Canada			
Improving advertising transparency	Created an ad library, a searchable database that contains ads run on Facebook and Instagram related to politics and issues of national importance	Introduced political advertising certification and ad transparency centre	Did not accept election advertising
Cyber hygiene and anti-harassment policies	Launched Equal Voice partnership to protect woman leaders Provided resources for candidates running for office Created "Cyber Hygiene Guide" to support cybersecurity		

Source: Author.

demonstrated that the timing of corrections matters, and if a user has been pre-exposed to a disinformation narrative, the label might not have any effect on their beliefs about the accuracy of the content (Pennycook, Cannon and Rand 2018). The authors show that even a single exposure increases subsequent perceptions of accuracy, both within the same session and after a week. Moreover, this "illusory truth effect" for fake-news headlines occurs despite a low level of overall believability and even when the stories are labelled as contested by fact checkers or are inconsistent with the reader's political ideology. These results suggest that social media platforms help to incubate belief in blatantly false news stories and that tagging such stories as disputed is not an effective solution to this problem. It is interesting, however, that the authors also found that prior exposure does not impact entirely implausible statements (for example, "The Earth is a perfect square"). Thus, fact-checking can be an effective strategy for reducing the spread of misinformation, but because it does not scale well with the speed of social media, it is only a partial solution to combatting disinformation.

Enhancing Political Knowledge and Strengthening Media Literacy and Journalism

All three platforms took steps to enhance the political knowledge of Canadians. Facebook created voter information notifications that linked to Elections Canada's website from its News Feed feature.[6] Facebook also placed limits on pages, so that pages could no longer self-identify as "news."[7] Twitter compiled a list of hashtags and candidates to follow for information about the federal elections, and provided notifications about the election but on a subscription basis to help users stay informed (Austin 2019c; 2021). Google helped enhance political knowledge by promoting links to relevant information on election day, sharing resources on how and where to vote, creating knowledge panels for political candidates and livestreaming federal debates on YouTube (Google 2021).

Platforms also made several investments in media literacy initiatives in Canada. During the 2019 election, Facebook worked with MediaSmarts to spread bilingual advertisements to help people

[6] Ibid.

[7] Ibid.

make informed decisions about news.[8] Google also made investments in media literacy for Canadians. In 2017, Google announced a $500,000 grant to develop and deliver a digital media literacy program to help Canadian students identify misinformation online (Nanji 2017). The company also announced several initiatives to support Canadian journalism at the local and national levels, including a licensing program that helps newsrooms curate content for readers using Google News and Discover, covering paywall fees so that Canadians can access paywalled content for free (Geremia 2021a). Google also announced investments in programs to train journalists on digital skills for reporting (Geremia 2021b). Twitter did not announce any Canadian-specific investments in media literacy programs for citizens or journalists in the lead-up to the Canadian elections.

Investments in media literacy and journalism are a core component of long-term strategies to address disinformation. In particular, Google's efforts to remove pathways to news and information about Canadian politics in the lead-up to the election were part of an innovative policy that helped alleviate some of the pressures on newsrooms to market content on social media. The digital transformation of news has altered how local and national news outlets sustain their business models as ad revenues decrease and content strategies adapt to fit new online consumption patterns. Having access to local news matters for democracy: it can promote empathy to combat polarization, encourage voting and strengthen political knowledge about the community and the world. Thus, investments made in local journalism can help offset some of the negative consequences of digitization in news by providing Canadians free access to news without hurting the bottom line of local outlets producing and distributing content online.

Reducing the Algorithmic Visibility of Misinformation

Ahead of the 2019 election in Canada, Facebook and Google also introduced measures to limit the reach of misinformation via recommendation algorithms and in News Feeds. Facebook announced it would reduce the amount of political content in Canadian News Feeds[9] and Google announced it would elevate authoritative services for election news and information in Google Search and on YouTube (McKay 2019). Twitter did not launch any Canadian-specific initiatives to reduce the algorithmic visibility of mis- and disinformation on its platform.

While algorithmic changes are one of the most important strategies for combatting the organic spread of disinformation, there are several limitations to both Facebook's and Google's approaches. With regard to Facebook, defining what constitutes political information is a difficult question with no straightforward answer, especially as political issues can often overlap with important social issues in Canada. Civic advocacy, expert opinions and news events could all be considered "political content" that might no longer be easily discoverable by Canadians. Second, without a clear discussion about what constitutes political content, this policy serves to promote commercial interests over activism and public goods. Finally, without insight into the algorithmic curation of content, there is no way to evaluate what kinds of political content were demoted in News Feeds, and if these policies led to biases. Simply demoting political content with no clear definition of what political content is, and no way to audit or evaluate whether the algorithmic changes produced their intended consequences, leaves plenty of questions around the efficacy of this strategy.

Google's approach to algorithmic downgrading was slightly different from Facebook's approach. Rather than demoting political content, Google Search and YouTube promoted content from authoritative sources in their algorithms. While this approach could help prevent mis- and disinformation from being amplified by algorithms, there is still a lack of transparency about how, when and for whom algorithms recommend certain kinds of content, and if gaps or biases exist. For example, when it comes to Google Search, threat actors have been known to "game" these systems by exploiting "data voids," which are gaps in authoritative sources of information (Bradshaw and Howard 2019). Here, disinformation or conspiratorial websites use terms that professional and mainstream media do not use in their coverage, so that when users search for those terms, search engines will surface the conspiratorial content since authoritative sources do not exist.

[8] Ibid.

[9] Ibid.

Promoting Political Participation

In addition to inoculating users against disinformation, social media platforms took several steps to promote political participation and combat voter suppression. Social media has not only changed how citizens find news and formulate political opinions, but it can also shape how citizens behave in a democracy, including how they participate in online conversations, activism and assembly, or whether they will vote. Platforms adopted two kinds of policies to address these concerns: promoting civic engagement and combatting hate speech and harmful or suppressive content.

Promoting Civic Engagement

Facebook and Twitter implemented policies to promote civic engagement in the lead-up to the Canadian election. Twitter encouraged political participation by creating custom election emojis (Austin 2019a). Similarly, Facebook, in conjunction with Apathy is Boring, a Canadian non-partisan, youth-led organization that promotes civic engagement among Canadian youth, developed "I voted" stickers, profile frames and augmented reality effects to encourage voting.[10] Facebook also sent out election day reminders the night before and day of an election, with a button to find polling stations. Research has demonstrated that social media platforms play an important role in shaping voting behaviour, and continuing to implement features to promote political participation, particularly in partnership with civil society initiatives, are promising paths forward.

Combatting Hate Speech and Harmful or Suppressive Content

Facebook and Twitter both introduced initiatives to combat hate speech and harmful or suppressive content on their platforms. Facebook's measures included designations for hate organizations and the removal of organizations and groups in Canada spreading hate; collaborations with the Centre for Israel and Jewish Affairs and the Canadian Jewish Holocaust Survivors and Descendants to remove false, inaccurate or misleading information about the Holocaust; and consultations with Indigenous groups to add Indigenous-specific hate terms to their hate speech policies.[11] In July 2019, Twitter also implemented a policy to hide replies to tweets, so that users could limit the reach of hateful or abusive content on their timelines (The Canadian Press 2019).

Understanding the unique manifestations of hate speech within and about various Canadian communities is important for combatting it online. Platforms' measures that adopt an informed and localized approach to hate speech policies are important first steps, especially when they involve direct consultations with local communities to understand the breadth and nature of hateful content and its effect on people's lives and well-being. However, these issues are ongoing, and more collaborations and research should be done to study and combat hate speech, harmful content and voter suppression in Canada. Given the importance of these issues for safety and well-being, policies should also extend beyond election time.

Promoting Campaigning

Finally, platforms also introduced new policies to promote political campaigning. In the digital era, there are more opportunities for political candidates to identify new constituents, fundraise and communicate with voters. However, the laws and regulations that ensure fair elections and equal competition have not always kept pace with the new digital affordances of technology. Platforms have taken a number of steps to address some of these new challenges, including improving advertising transparency to adhere to Canada's Elections Modernization Act and safeguarding female candidates from online abuse and harassment.

Improving Advertising Transparency

All three platforms adopted new policies to address issues of ad transparency in the lead-up to the Canadian election, updating their platform policies and developing tools to adhere to Canada's election laws. In March 2019, Facebook created a registry for digital advertising called the Ad Library.[12] This searchable database, for both active and inactive advertisements, digitized advertisements on "social issues, elections or politics" targeting Canadian Facebook users across Facebook and Instagram

[10] Ibid.

[11] Ibid.

[12] Ibid.

and provided users with transparency information about the sponsor of the advertisement. This database was a newer version of the Ad Archive Facebook created for the United States in 2018. In 2019, Twitter implemented a political content certification process to advertise on its platform. Advertisements that were accepted for publication would be made viewable in Twitter's advertisement transparency, which also provided users with transparency information about the sponsor of the advertisement (Austin 2019b). Google took a different approach from Facebook and Twitter when it came to political advertisements: rather than creating a new tool to address the transparency requirements noted in Canadian law, Google blocked all political advertisements on its platforms until the end of the 2019 federal election.[13]

While both Facebook and Twitter created digital advertisement archives for the previous Canadian elections, more can still be done to address some unaddressed challenges and support elections with integrity. In particular, platforms should take further steps to improve the transparency of political advertising by disclosing the identity of advertisers and publishing more data about how and why individuals were targeted with an advertisement. While digital ad archives can help hold political advertisers accountable by creating an archive of all the advertisements bought and placed on social media, we have little detailed insight into why certain users were targeted other than broad demographic details. If platforms allow advertisers to micro-target users based on other datapoints (such as their hobbies, interests or political leaning), these datapoints should also be made transparent to users.

In contrast to Facebook and Twitter, Google completely pulled out of political advertising. While this approach can avoid some of the tricky transparency issues around how and why people are targeted with ads, it also has limitations. In particular, digital platforms have created opportunities for non-incumbent politicians to reach wider audiences, and studies have shown that digital advertising helps create a level playing field for candidates "down the ballot," who might not have the resources to buy expensive television and radio advertisement slots and print ads.

Cyber Hygiene and Anti-harassment Policies to Protect Female Candidates

Facebook adopted several policies to help prepare female politicians and candidates for (cyber) security concerns that often arise alongside the spread of mis- and disinformation. In 2017, Facebook created a "Cyber Hygiene Guide" and a crisis hotline for political candidates running for office in Canada (Facebook 2017). In April 2019, in collaboration with Equal Voice, a multi-partisan organization dedicated to empowering women at all levels of political office, Facebook also launched the #HerVoice safety guide to help protect women leaders and empower them to safely campaign on social media, as female politicians often face greater levels of hate and harassment online (Facebook 2019). Google and Twitter did not adopt any specific policies to help female Canadian politicians.

Numerous academic studies have found that female politicians experience greater levels of harassment online than their male counterparts. Harassment targeting women not only lasts for longer periods of time, but it also often uses gender stereotypes and sexualized tropes to suppress their participation online and undermine their legitimacy. Qualitative accounts of harassment against women have shown that it can have a negative, measurable impact on their online behaviours. Platform initiatives that consider the unique way women experience social media and work directly with women to support them, such as Facebook's #HerVoice guide, are an important step in helping empower female politicians to campaign in a safe environment. Since harassment can also be intersectional, these initiatives could be extended to other minority or marginalized individuals to address the specific needs and threats they might face.

Conclusion

Platforms adopted several policies to improve the security and integrity of the Canadian digital public sphere. Many of these private self-regulatory responses can have a positive effect on promoting safety during digital campaigns and protecting female candidates, improving media literacy, and working with local partners to help protect Canadians from hate speech, harassment and suppression

[13] See https://support.google.com/adspolicy/answer/9338582?hl=en.

messages online. But there are still many gaps and challenges facing private self-regulation, particularly around the algorithmic curation of misinformation, data access and transparency, and supporting digital journalism in Canada.

Two important questions remain: Are private self-regulatory responses going to be enough to address these ongoing challenges? Or will government regulators need to step in to compel a more adequate response by platform companies to mis- and disinformation online? There are indeed benefits and trade-offs to both approaches. Platforms have the tools to identify and remove harmful accounts quickly and at a global scale. However, these approaches often lack transparency or accountability for decisions, and users have very few options to appeal platform takedowns. Similarly, there is a lack of consistency around the world in terms of how much resources platform companies put into combatting information integrity issues, with certain stakeholders in the Global South remaining underrepresented or integrity teams insufficiently funded to deal with problems, especially beyond election cycles.

While government regulation can help improve transparency and accountability, regulation can also be slow, cumbersome and disconnected from the technology, especially in a digital environment where technology is constantly evolving and changing. At the same time, heavy-handed regulations that address issues about content could compel platforms to over-censor information, limiting the ability of social media technologies to promote fundamental human rights. There have already been many examples of authoritarian regimes using content regulations to suppress freedom of speech and freedom of the press in their own countries. However, it is clear that election and campaigning laws, or privacy laws, have not kept pace with innovations in technology and are clear areas where government regulators could do more to protect citizens and consumers.

Overall, both private self-regulation and government regulation and oversight will be needed to address the variety of issues at the nexus of information integrity and democratic well-being. As immediate first steps, platforms could adopt the following recommendations to build on their current initiatives to safeguard elections and the digital information ecosystem.

→ Implement partnerships in Canada to improve data access and transparency: Even though social media has become integral to the processes of democracy, we have very little insight into how platforms affect the political opinions and behaviours of Canadians. Although platforms have adopted several policies to help reduce the algorithmic spread of misinformation, make advertising more transparent, or reduce the spread of hate speech online, researchers do not have enough data to evaluate the effectiveness of these strategies and whether biases might exist in current platform practices. Platforms should establish partnerships with Canadian universities, civil society organizations and think tanks to make data available so that researchers can measure, evaluate and understand how social media is shaping democratic discourse in Canada. There are several kinds of data that would benefit researchers: the content (and metadata about the content) reaching a large number of Canadians should be made available for researchers and academics to evaluate the kinds of information and accounts being amplified by algorithms; metadata and targeting data about political advertisements should be made available to allow researchers and academics to understand, evaluate and address how citizens are micro-targeted with political advertisements; and data about content moderation practices in Canada, including aggregate statistics about the kind of content being removed on platforms, as well as an archive of removed content should be made available for public interest research.

→ Increase collaboration and partnerships with local media: Local news organizations continue to face immense financial pressure in the digital era due to declining advertising revenue. To alleviate some of these pressures, platforms made investments in journalism during the 2019 and 2021 federal elections, by covering the cost of paywalled content or by providing training for journalists on new digital skills. However, platforms could go further in their investments by reallocating a share of revenue to local news providers. These investments could continue to remove paywalls from national and local news services, not just during election periods. They should also focus on developing partnerships and making investments in French and Indigenous news programs in Canada to allow for more diverse and culturally representative sources of news.

This case study provided a summary of the key policies adopted by social media platforms in the lead-up to the 2019 and 2021 federal elections in Canada. While it does not cover all of the private self-regulatory initiatives, such as incremental changes to terms of service or community guidelines, this summary is designed to help policy makers learn from Canada's experience and navigate key high-level areas for future policy intervention both in Canada and abroad.

Works Cited

Austin, Michele. 2019a. "An update on Canadian political advertising." *Twitter Blog*, August 29. https://blog.twitter.com/en_ca/topics/company/2019/update_canadian_political_advertising_2019.

———. 2019b. "Inside the 43rd Canadian general election on Twitter." *Twitter Blog*, September 23. https://blog.twitter.com/en_ca/topics/insights/2019/canadian_election_on_Twitter_2019.

———. 2019c. "Providing clarity on political advertising in Canada." *Twitter Blog*, June 26. https://blog.twitter.com/en_ca/topics/company/2019/political_advertising_in_canada.

———. 2021. "Inside the 44th Canadian general election on Twitter." *Twitter Blog*, August 17. https://blog.twitter.com/en_ca/topics/events/2021/inside-the-44th-canadian-general-election-on-twitter.

Bernhard, Daniel. 2021. "Social media giants continue to harm democracy and it's evident during this election." *Toronto Star*, September 8. www.thestar.com/opinion/contributors/2021/09/08/social-media-giants-continue-to-harm-democracy-and-its-evident-during-this-election.html.

Bradshaw, Samantha and Philip N. Howard. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. Oxford, UK: The Computational Propaganda Project at the Oxford Internet Institute, University of Oxford. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf.

CSE. 2021. *Cyber Threats to Canada's Democratic Process: July 2021 Update*. Ottawa, ON: CSE. https://cyber.gc.ca/sites/default/files/2021-07/threat-to-democratic-process-2021-3-web-e.pdf.

Facebook. 2017. *Cyber Hygiene Guide: Politicians and Political Parties*. https://facebookcanadianelectionintegrityinitiative.com/files/Cyber-Hygiene-Report-en-ca.pdf.

———. 2019. "#HerVoice: Facebook Safety Tips for Women Leaders." https://d3n8a8pro7vhmx.cloudfront.net/equalvoice/pages/688/attachments/original/1556039255/HerVoice_final_en.pdf.

Geremia, Sabrina. 2021a. "We're expanding our support of news in Canada." *Google Canada Blog*, June 24. https://blog.google/intl/en-ca/company-news/outreach-initiatives/were-expanndig-our-support-of-news-in/.

———. 2021b. "Answering top questions about News Showcase in Canada." *Google Canada Blog*, June 24. https://blog.google/intl/en-ca/company-news/outreach-initiatives/answering-top-questions-about-news/.

Google. 2021. "How We're Supporting the 2021 Federal Election." *Google Canada Blog*, August 18. https://canada.googleblog.com/2021/08/how-were-supporting-2021-federal.html.

McKay, Colin. 2019. "Federal Elections 2019: Helping Canadians Make Informed Decisions." *Google Canada Blog*, September 23. https://blog.google/intl/en-ca/company-news/outreach-initiatives/federal-elections-2019-helping/.

Mena, Paul. 2020. "Cleaning Up Social Media: The Effect of Warning Labels on Likelihood of Sharing False News on Facebook." *Policy and Internet* 12 (1): 165–83. www.researchgate.net/publication/334740447_Cleaning_Up_Social_Media_The_Effect_of_Warning_Labels_on_Likelihood_of_Sharing_False_News_on_Facebook.

Nanji, Sabrina. 2017. "Google bankrolls Canadian school program targeting fake news." *Toronto Star*, September 19. www.thestar.com/news/gta/2017/09/19/google-bankrolls-canadian-school-program-targeting-fake-news.html.

Pennycook, Gordon, Tyrone D. Cannon and David G. Rand. 2018. "Prior exposure increases perceived accuracy of fake news." *Journal of Experimental Psychology* 147 (12): 1865–80. https://psycnet.apa.org/record/2018-46919-001.

Taylor, Emily, Stacie Walsh and Samantha Bradshaw. 2018. *Industry Responses to the Malicious Use of Social Media*. Riga, Latvia: NATO Strategic Communications Centre of Excellence.

The Canadian Press. 2019. "Twitter users in Canada will now be able to hide replies to tweets." *Financial Post*, July 11. https://financialpost.com/technology/personal-tech/twitter-users-in-canada-will-now-be-able-to-hide-their-replies-to-tweets.

The Dark Web and Democracy: Misinformation and the Use of Tor in Canada, Germany and the United States

Eric Jardine

Key Findings

- → Dark web content is resilient to moderation efforts and can percolate back into society.
- → During the considered portion of the COVID-19 pandemic (2020–2021), dark web sites more than doubled in number shortly after peak global search interest for "COVID" (as determined by Google Trends).
- → The daily number of dark web users in Canada, Germany and the United States was consistently above each country's respective 2019 average, showing a greater use of Tor during the COVID-19 period.
- → Democracy requires both common agreement on informational reference points and the ability to debate ideas; however, the dark web can be used by those with the intention of weaponizing information to destabilize democracy by undermining the political coherence of nations.
- → Despite the dark web's design as a resilient platform, remedial steps to manage the use of the dark web as an element in a weaponized information campaign do exist.

Introduction

Information can be weaponized and used to affect political, social, economic and, indeed, likely psychological outcomes. The use of information in this way requires stable platforms of production and viable mechanisms of transmission; collectively, the pairing of an *intention* to turn information into a weapon with ecosystem *capabilities* that produce stable transmission pathways could be thought of as a "weaponized information environment." This case study shows how the dark web can act as both a platform and a mechanism of transmission for weaponized information. Broadly, the dark web, which is an anonymous and decentralized portion of the global internet, is a highly resilient host for informational content, and The Onion Router (Tor) browser, used to access these sites, can provide users with an anonymized mechanism of informational transmission (Jardine 2019a). This case study first summarizes the functions of the dark web and then details its potential role in a weaponized information environment. It then explores data related to this technology in the context of the information environment surrounding the COVID-19 pandemic. The conclusion points to ways in which the dark web's role in a weaponized information environment might be blunted.

The Dark Web

The dark web is a class of technologies that makes people anonymous online (Gehl 2018; Jardine 2015). While a number of dark webs exist, such as I2P and Freenet, the primary dark web is run on a system known as Tor (Dingledine, Mathewson and Syverson 2004). Tor anonymizes a user's activity by relaying a query through a series of randomly assigned nodes that are part of Tor's global overlay network. This network sits on top of the regular internet and consists of between 6,000 and 6,500 volunteer devices that run Tor protocols and are distributed globally. These nodes act like waypoints on the journey of information through the Tor network. While Tor is vulnerable to some deanonymization techniques and can be effectively policed by large law enforcement agencies (Jardine 2021; Johnson et al. 2013), it is generally a robust anonymity-granting tool, meaning simply that a person's identity and actions cannot be easily linked together.

The Tor dark web also allows for fairly elaborate functionality, including both reader and publisher anonymity (Gehl 2018). When using the Tor browser, which is downloaded and installed on a device from the Tor Project webpage or launched as part of Tails, a user gains effective reader anonymity. Users of the Tor browser can employ the system much like Chrome or Safari to engage anonymously with surface web content, such as by visiting Reddit or CNN.com. They can also use the browser to access dark web sites, which end with the especial suffix ".onion." Globally, about

90 percent of Tor users employ the browser to engage with surface web content on an average day, although more users in repressive regimes tend to employ Tor for this sort of privacy and censorship circumvention purpose than those in politically free regimes where use tends to disproportionately cluster on dark web sites (Jardine 2018b; Jardine, Lindner and Owenson 2020).

Publisher anonymity on Tor is exemplified by the ability to host .onion sites, which are effectively anonymously administered dark web sites running regular web protocols (for example, HTML) (Gehl 2018). The use of regular web protocols implies that dark web sites look and feel, absent perhaps some functions of JavaScript, a lot like regular websites that users would routinely access on the surface web. This similarity makes dark web .onion sites a useful and comparatively resilient platform for a variety of socially harmful content, including drug cryptomarkets (Martin 2014) and child abuse content sites (Owen and Savage 2015). Especially as major internet platforms have begun to more deliberately moderate surface web content, the dark web has also become an increasingly common location for the hosting of objectionable informational content, ranging from extremist content (for example, the Daily Stormer moved to the dark web after it was moderated out of existence by surface web platforms) to, increasingly, health dis- and misinformation-related sites (Jardine 2019a; Topor and Shuker 2020).

The Dark Web as a Capacity Element in a Weaponized Information Environment

The dark web's potential role in a weaponized information environment is two-fold. First, the dark web is a resilient techno-social reservoir for misleading information (Jardine 2019a). Producers of weaponized information can choose the dark web as a location to host content, free from much of the centralized control that characterizes the surface web. This resilience, however, is bought at the expense of reach, since accessing the Tor dark web can be an informationally intensive process that requires downloading specific tools (for example, the Tor browser) and accumulating knowledge about site addresses, social norms and procedures for engaging with dark web content in a secure way (Chen, Jardine and Liu 2021; Jardine 2021).

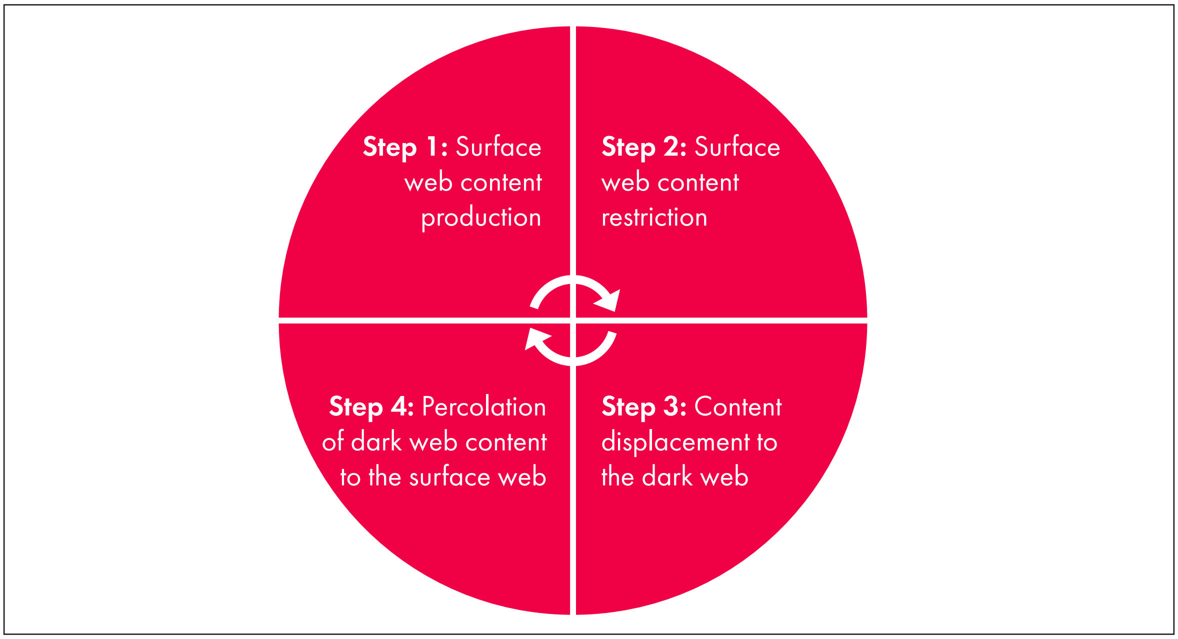
Secondly, the Tor browser is also a highly effective privacy tool and censorship-circumvention instrument (Jardine 2018a; 2018b). Motivated users can, therefore, opt to use Tor in place of their regular web browser to access content that is either hosted directly on a .onion dark web site or housed on the regular surface web, but do so in an anonymous way. People could access content on the Tor dark web and then carry the memetic ideas back to the surface web and daily life, providing a means of weaponized information diffusion (Jardine 2019a).

The dark web as platform (via .onion sites) or mechanism of transmission (via the Tor browser) for weaponized information generally highlights the capacity role this class of technology can play within a weaponized information environment. Abstracting from the discrete functions of the dark web also allows for a wider view of the technology within the dynamic context of a moderated surface web information environment. As detailed elsewhere (Jardine 2019a), content moderation efforts by major internet platforms are likely to generate a cycle of displacement, rehoming and percolation from the dark web to the surface web. Detailed in Figure 1, this dynamic process suggests that the dark web is not a world apart from the information environment of the surface web but is instead fully enmeshed in one system of information.

COVID-19 as an Example

The 2020–2021 COVID-19 pandemic period is a good example of the role the dark web can play in a weaponized information environment. During the pandemic, major tech platforms undertook large and concerted efforts to moderate health-related mis- and disinformation. Platforms such as Facebook, Twitter and YouTube banned accounts, minimized the display of posts and demonetized content based on their relationship to standard

Figure 1: The Surface-to-Dark-Web Content Moderation Cycle


Step 1: Surface web content production
Step 2: Surface web content restriction
Step 3: Content displacement to the dark web
Step 4: Percolation of dark web content to the surface web

Source: Jardine (2019a).

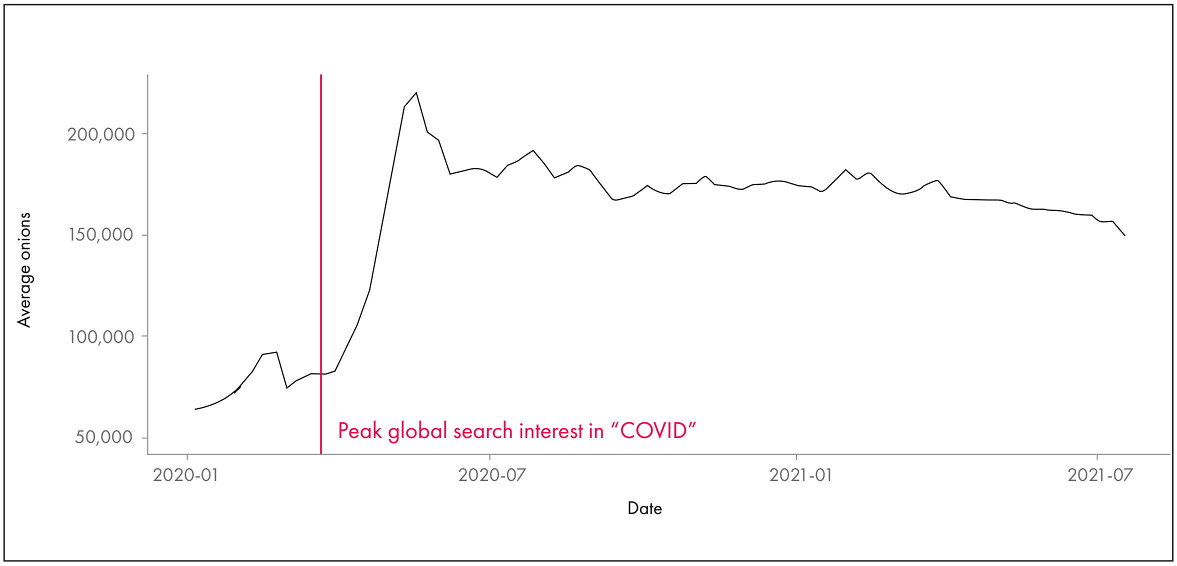
health guidance. In such a censored environment, the dark web might play two roles, as specified above. First, the Tor dark web might readily become a tool of resilient information storage (i.e., home to hosted content). Second, people might also seek to use the Tor browser more in an effort to circumvent perceived censorship by governments and big tech to reach the "truth" (Jardine 2018b).

These possible functions also suggest two simple empirical tests. First, if Tor dark web sites acted as resilient homes for potential mis- and disinformation during the COVID-19 pandemic, then the number of dark web sites should have increased noticeably from their pre-pandemic levels. Second, and in similar fashion, if the Tor browser can act as a privacy tool and censorship-circumvention instrument that could be employed to access secretive knowledge that runs counter to, say, official health guidance from the Centers for Disease Control and Prevention or the World Health Organization, then we would expect Tor client connections (which are distinct, non-unique Tor users on a given day) to be higher than what was normal before the pandemic started. Data to assess both claims exists, with dark web site counts available at a global scale and Tor client numbers available at the country level.

In line with expectations, both of these simple predictions about the potential role of Tor, broadly considered, within a temporally specific weaponized information environment are plausibly correct. Figure 2 plots the average number of Tor dark web sites per week from the start of 2020 until August 14, 2021, which basically spans the start of the global pandemic until the time of writing.

The vertical red line falls during the week of March 22, 2020, when Google Trends data suggests that the query "COVID" hit its highest level of population-normalized global search volume (incidentally, the highest volume of search for the term was from Canada). Almost immediately after this point of peak global interest in COVID-19, the weekly average number of .onion sites (dark web sites) surged from around 75,000 in operation per week (which is roughly in line with pre-pandemic levels) to more than 200,000 and has remained above 150,000 ever since. Certainly, not all of these new sites would have been related to COVID-19 health-related misinformation. Some, for example, were sites that peddled COVID-19-related health interventions (Bracci et al. 2021a; 2021b) and stolen Zoom credentials (Chawla 2020). Many other dark web sites, however, did explicitly work to host and purvey dis- and misinformation (Topor and Shuker 2020).

Figure 2: Weekly Tor Dark Web Sites and Peak Global Interest in "COVID"



Sources: See https://metrics.torproject.org/userstats-relay-country.html; https://metrics.torproject.org/hidserv-dir-onions-seen.html.

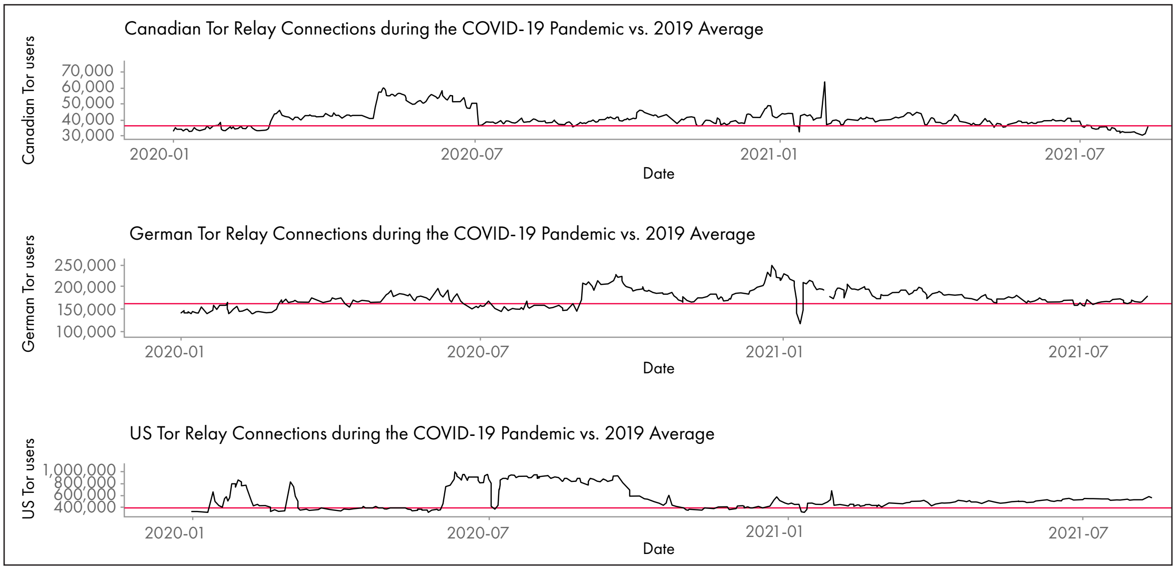
Usage of the Tor browser was also significantly higher than normal during the pandemic period, providing a demand-side view of patterns of informational consumption and substantiating the function of the Tor browser as a potential mechanism of information diffusion (Jardine 2019b). As detailed in Figure 3, Canada, Germany and the United States all exhibit significant periods of above-average Tor client connection rates relative to their respective 2019 usage rates (as depicted by the horizontal red lines). Additionally, Tor use globally has generally plateaued around 2–2.5 million daily client connections, so it is unlikely that these periods of greater usage (compared to the 2019 average) are a function of a naturally expanding user base (Hampson and Jardine 2016). Instead, the best explanation is likely that the information environment surrounding COVID-19 pushed people toward the Tor browser as a tool to access information that is either on the Tor dark web or censored within a particular jurisdiction but available generally on the surface web.

Implications for Democracy

Democracy is a tricky thing. It requires both some degree of common ideational agreement and the ability to actively debate ideas. In a democracy, people need to agree upon minimal normative sets. For example, participants in a democracy need to agree that the loser of an election acquiesces to being governed by the winner, even though the contenders almost by definition disagree about how things ought to be done. Common informational reference points (such as everyone has watched the same news or is conversive about the same cultural moments) can likewise facilitate group cohesion and promote social trust. At the same time, active efforts to police ideas, stifle dissent and muzzle contrary viewpoints, if taken too far, will themselves eventually imply that democracy is gone.

The dark web as a class of technologies presents a true policy dilemma for democracies with regard to its informational function. On the one hand, as pointed out above, the dark web can act as both a platform and transmission mechanism for information that might promote radical ideologies or sow the seeds of confusion about important

Figure 3: Canadian, German and US Tor Relay Connections during the COVID-19 Pandemic versus 2019 Average



Sources: https://metrics.torproject.org/userstats-relay-country.html; https://metrics.torproject.org/hidserv-dir-onions-seen.html.

Note: Red lines show 2019 Tor client average.

public issues (for example, health misinformation). In the broadest of terms, the dark web can weaken democracy by providing the capacity to potentially reduce social coherence and undermine trust to those who wish to weaponize information.

At the same time, public discourse can often be simply wrong (morally, factually or otherwise). In such a setting, viewpoints and opinions can become actively policed by the state, intermediaries or society writ large. Here, the existence of a class of technologies that can facilitate the stable hosting of ideas and their transmission into society can make all the difference between the persistence of democracy and the descent into totalitarianism. Indeed, it is not technically feasible to design an anonymity-granting technology that allows for the robust protection of rights but does not similarly protect those who would use the technology for illicit purposes — as the builders of Tor were well aware (Gehl 2018). In this sense, the dark web can both pose a challenge to democracy and act as a last bulwark against authoritarian tendencies in society.

Within the current historical moment, the informational roles that the dark web is plausibly playing in liberal democratic regimes suggest a few implications for politics and society. First, the dark web is acting as a host for extreme political points of view (Jardine 2019a). Operating thus as a stable platform for potentially radicalizing information effectively implies that political ideas that might be antithetical to democracy persist and remain reachable by sufficiently motivated individuals. Likewise, as pointed out above, steps undertaken to impose friction on the spread of this information (through content removal, demonetization and so forth) on surface web networks likely work to a degree but will not work as well for dark web content due to the decentralized structure of the system. The simple existence of ideas, of course, does not ensure that they are going to be agreed with, internalized or acted upon. In this sense, the dark web might mean that information that is antithetical to democracy is likely to be both persistent and easily accessible to more people, but in a setting where receptivity to these ideas is very low, it will hardly matter.

Another implication of the dark web for democracy can be seen through an analogy to the human immune system. The human body reacts to foreign bodies within it (for example, viral infection, a splinter in the toe and so forth) by mobilizing antibodies to seek out and destroy the pathogen. When this process gets too extreme, the human body ends up with an autoimmune disorder that effectively results in the body attacking itself. In extreme instances, autoimmune disorders can prove fatal. In this example, the dark web (or the content it hosts) could be thought of as a splinter or viral infection within a democracy. Sometimes, in such a setting, a democracy will need to react to what is available on the dark web, even by trying to compromise the integrity of the dark web itself in order to police the content (Chertoff and Jardine 2021). But overdoing the reaction to the dark web can be worse than the disease. Navigating the balance is the zone of politics.

Another implication, which extends somewhat from the internet as a whole, is that the information environment of the dark web is truly global. The Tor dark web, as an overlay network, leverages both the regular infrastructure of the internet and a series of volunteer nodes to obfuscate the identity of participants. This design structure and its resultant obfuscation of the identity of participants have one clear effect. As pointed out above, both consumption and production of content are done anonymously. Implicit in this anonymity is, especially on the production side, the idea that the producers of content could be based anywhere and might pretend otherwise. For example, while Russian troll farms often engage with regular surface web platforms where the reach of the content is wider, there is no reason to assume that similar actors are not producing content on dark web sites as well. While the reach of this information would be less due to a smaller user base, its resilience would be higher (Jardine 2019a). From the perspective of a malicious foreign actor attempting to destabilize democracies via information channels, targeting both easily moderated surface web sites with large user bases and resilient dark web sites with fewer users presents a potentially optimum mixed strategy — sort of like investing in both high-risk assets and more stable bonds.

The final implication is that specific democratic processes can be imperilled in a setting of mistrust induced by mis- and disinformation. Linking, say, electoral outcomes specifically to mis- and disinformation is challenging and hinges on the rate of exposure to untrue ideas, the degree to which these ideas are internalized, and the extent to which internalized ideas convert into actions that would not have otherwise been undertaken. This process would unfold like a funnel, with many more people seeing weaponized information than internalizing these messages and even fewer still acting in a way that they might otherwise not have done. Nevertheless, both at the level of discrete actions (voting within a specific election) and broader sentiment (levels of trust in democratic processes and institutions), even a few people who work fully through this funnel might begin to change the trajectory of history, especially since a highly motivated minority of people within a population at large can often compel significant social change (Avishai 2020).

Remedial Steps

Contending with the dark web as a stable socio-technical platform for production and a mechanism of transmission for mis- and disinformation is challenging. By design, Tor is built to be decentralized (Dingledine et al. 2004). By dint of organizational structure, decentralized networked structures are simply harder to contend with than centralized systems. By implication, efforts to contend with the dark web within any given jurisdiction are liable to be partial at best. Additionally, the Tor Project, which manages the protocol base and is an incorporated not-for-profit in the United States, is reactive to efforts to break Tor, patching flaws in the code that might reduce the privacy protections that the system provides to users.

And, to be clear, these functional design and organizational characteristics are what make Tor such a useful privacy tool and censorship circumvention system in repressive regimes (Jardine 2018b), but they also stymie effective single jurisdiction efforts to contend with the dark web as either a platform for mis- and disinformation or the Tor browser as a mechanism of information diffusion within liberal democracies.

Despite these real limitations to what can effectively be done to mitigate the role of the dark web in a weaponized information environment, a few policies, as outlined more fully elsewhere (Jardine 2019a), suggest themselves. These policies, as befit an internet governed in a multi-stakeholder way (Bradshaw et al. 2015; Raymond and DeNardis 2015), involve the concerted actions of both governments and private organizations.

The following are policies to contend with the dark web as a platform for mis- and disinformation:

→ Within the bounds of national law, governments can target sites that curate links to dark web sites, thereby reducing the ease with which users can find dark web content. For example, the takedown of DeepDotWeb disrupted, however temporarily, the ability of users to find dark web drug markets (Jardine 2021).

→ Governments can also enact rules to ensure that web-hosting services might, nominally, be responsible for the content of the .onion dark web sites they host, thereby ensuring that hosted content is, at a minimum, not in violation of existing law. For example, the Playpen child abuse site was hosted on Centrilogic servers in Le Noir, North Carolina (Chertoff and Jardine 2021).

→ Web hosts can also assume responsibility absent rules from government, as was nominally done by Daniel's Hosting, which hosted about 5–10 percent (roughly 7,500) of the available .onion sites at the time (Cimpanu 2020). "Daniel's" formal rules for using his services read:

  Rules

  - No child pornography!
  - No terroristic propaganda!
  - No illegal content according to German law!
  - No malware! (e.g. botnets)
  - No phishing, scams or spam!
  - No mining without explicit user permission! (e.g. using coinhive)
  - No shops, markets or any other sites dedicated to making money! (This is a FREE hosting!)
  - No proxy scripts! (You are already using TOR and this will just burden the network)
  - No IP [intellectual property] logger or similar de-anonymizer sites!
  - I preserve the right to delete any site for violating these rules and adding new rules at any time.
  - Should you not honor these rules, I will (have to) work together with Law Enforcement![14]

The following are policies to contend with Tor as a mechanism of information diffusion:

→ Content delivery networks can place CAPTCHAs (Completely Automated Public Turing tests to tell Computers and Humans Apart) on traffic coming from known Tor exit nodes in an effort to increase the costs of using Tor to access surface web sites, thereby limiting the use of the Tor browser as a mechanism of information diffusion. For example, Cloudflare imposed CAPTCHAs on exit node traffic in 2016, as they indicated at the time that 94 percent of the site requests from Tor that they were observing were "per se malicious" (Jardine 2019a), although the Tor Project contests this claim.

→ Sites that host user-generated content (for example, Facebook, Reddit, YouTube and so forth) could implement a real-name account procedure. Such a procedure would not need to be immediately reflected in usernames but would ensure that the identity of content producers is nominally linked to what is being produced in a way that would render use of the Tor browser as a mechanism of information diffusion (at least outgoing) somewhat less effective.

In sum, the dark web is both a resilient socio-technical home for mis- and disinformation and, via the Tor browser, a mechanism of information diffusion in an otherwise moderated information environment. Steps can be taken by governments and private sector actors, but any efforts made need to contend with the legitimate use of this technology in more repressive regimes where access to information is scarce (Jardine 2015).

[14] See http://87.120.8.194.

Works Cited

Avishai, Bernard. 2020. "The Pandemic Isn't a Black Swan but a Portent of a More Fragile Global System." *The New Yorker*, April 21. www.newyorker.com/news/daily-comment/the-pandemic-isnt-a-black-swan-but-a-portent-of-a-more-fragile-global-system.

Bracci, Alberto, Matthieu Nadini, Maxwell Aliapoulios, Damon McCoy, Ian Gray, Alexander Teytelboym, Angela Gallo and Andrea Baronchelli. 2021a. "Dark Web Marketplaces and COVID-19: After the vaccines." SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3783216.

———. 2021b. "Dark Web Marketplaces and COVID-19: before the vaccine." *EPJ Data Science* 10 (6): 1–26. https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-021-00259-w.

Bradshaw, Samantha, Laura DeNardis, Fen Osler Hampson, Eric Jardine and Mark Raymond. 2015. *The Emergence of Contention in Global Internet Governance*. Global Commission on Internet Governance Paper Series No. 17. Waterloo, ON: CIGI and Chatham House. www.cigionline.org/publications/emergence-contention-global-internet-governance/.

Chawla, Ajay. 2020. "Coronavirus (COVID-19) — 'Zoom' Application Boon or Bane." SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3606716.

Chertoff, Michael and Eric Jardine. 2021. *Policing the Dark Web: Legal Challenges in the 2015 Playpen Case*. CIGI Paper No. 259. Waterloo, ON: CIGI. www.cigionline.org/publications/policing-the-dark-web/.

Chen, Zhicong, Eric Jardine and Xiaofan Liu. 2021. "Examining the Information Pathways Leading to the Darknet: A Cross-National Analysis." 71st Annual International Communication Association Conference.

Cimpanu, Catalin. 2020. "Dark web hosting provider hacked again — 7,600 sites down." ZDNet, March 25. www.zdnet.com/article/dark-web-hosting-provider-hacked-again-7600-sites-down/.

Dingledine, Roger, Nick Mathewson and Paul Syverson. 2004. "Tor: The Second-Generation Onion Router." *Proceedings of the 13th USENIX Security Symposium*. www.usenix.org/legacy/publications/library/proceedings/sec04/tech/full_papers/dingledine/dingledine.pdf.

Gehl, Robert W. 2018. *Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P*. Cambridge, MA: MIT Press.

Hampson, Fen Osler and Eric Jardine. 2016. *Look Who's Watching: Surveillance, Treachery and Trust Online*. 1st ed. Waterloo, ON: CIGI.

Jardine, Eric. 2015. *The Dark Web Dilemma: Tor, Anonymity and Online Policing*. Global Commission on Internet Governance Paper Series, No. 21. Waterloo, ON: CIGI and Chatham House. www.cigionline.org/sites/default/files/no.21.pdf.

———. 2018a. "Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies." *New Media & Society* 20 (8): 2824–43. doi:10.1177/1461444817733134.

———. 2018b. "Tor, what is it good for? Political repression and the use of online anonymity-granting technologies." *New Media & Society* 20 (2): 435–52. doi:10.1177/1461444816639976.

———. 2019a. "Online content moderation and the Dark Web: Policy responses to radicalizing hate speech and malicious content on the Darknet." *First Monday* 24 (12). doi:10.5210/fm.v24i12.10266.

———. 2019b. "The trouble with (supply-side) counts: the potential and limitations of counting sites, vendors or products as a metric for threat trends on the Dark Web." *Intelligence and National Security* 34 (1): 95–111. doi:10.1080/02684527.2018.1528752.

———. 2021. "Policing the Cybercrime Script of Darknet Drug Markets: Methods of Effective Law Enforcement Intervention." *American Journal of Criminal Justice* 46: 980–1005. https://link.springer.com/article/10.1007/s12103-021-09656-3.

Jardine, Eric, Andrew M. Lindner and Gareth Owenson. 2020. "The potential harms of the Tor anonymity network cluster disproportionately in free countries." *Proceedings of the National Academy of Sciences* 117 (50): 31716–21. doi:10.1073/pnas.2011893117.

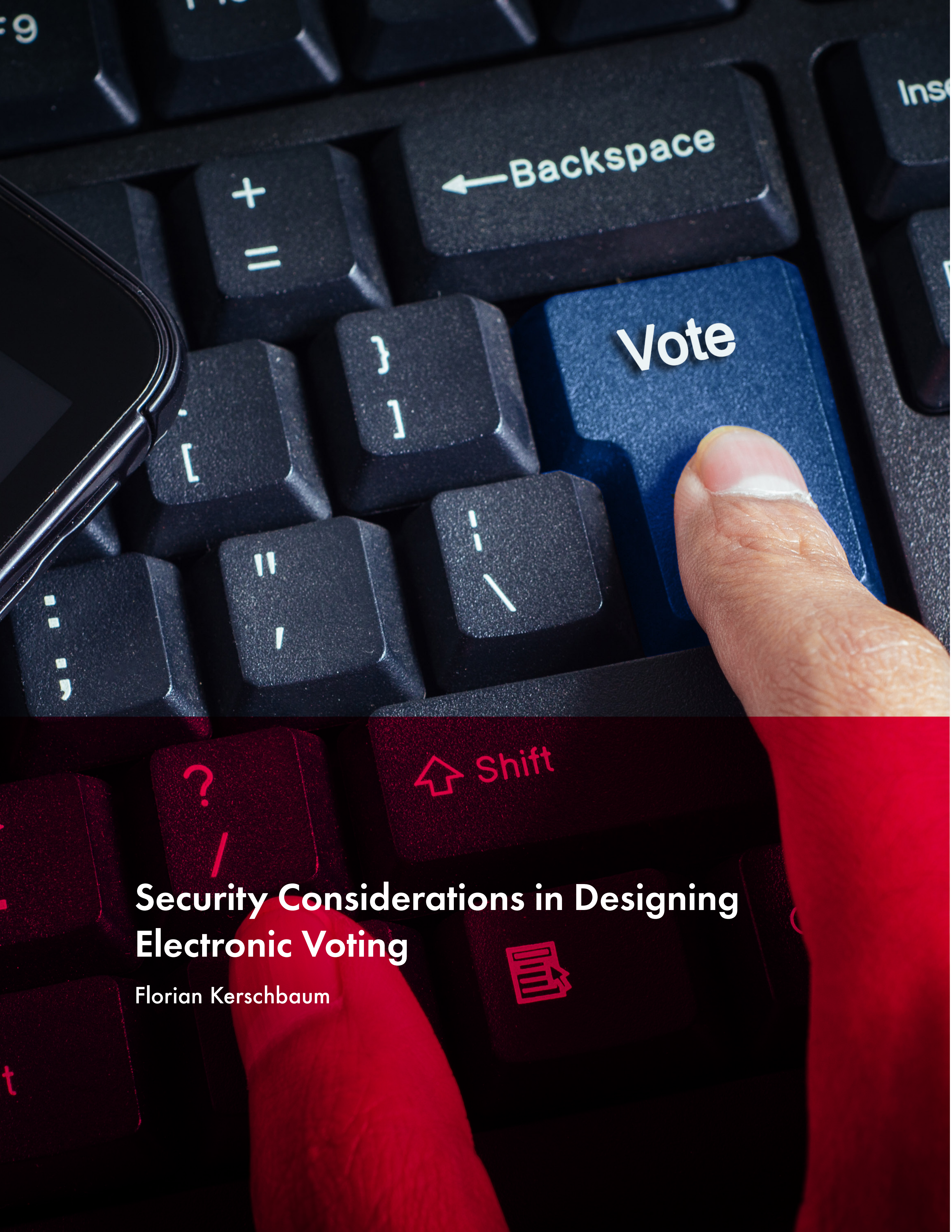
Johnson, Aaron, Chris Wacek, Rob Jansen, Micah Sherr and Paul Syverson. 2013. "Users get routed: traffic correlation on tor by realistic adversaries." *Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security*. doi:10.1145/2508859.2516651.

Martin, James. 2014. "Lost on the Silk Road: Online drug distribution and the 'cryptomarket.'" *Criminology & Criminal Justice* 14 (3): 351–67. doi:10.1177/1748895813505234.

Owen, Gareth and Nick Savage. 2015. *The Tor Dark Net*. Global Commission on Internet Governance Paper Series, No. 20. Waterloo, ON: CIGI and Chatham House. www.cigionline.org/publications/tor-dark-net/.

Raymond, Mark and Laura DeNardis. 2015. "Multistakeholderism: anatomy of an inchoate global institution." *International Theory* 7 (3): 572–616. www.cambridge.org/core/journals/international-theory/article/multistakeholderism-anatomy-of-an-inchoate-global-institution/B69E6361B5965C98CFD400F75AA8DC53.

Topor, Lev and Pnina Shuker. 2020. "Coronavirus Conspiracies and Dis/Misinformation on the Dark Web." *e-International Relations* 1–7. www.e-ir.info/2020/10/09/coronavirus-conspiracies-and-dis-misinformation-on-the-dark-web/.



Security Considerations in Designing Electronic Voting

Florian Kerschbaum

Key Findings

Based on the principles for designing secure election systems, it is important to:

- pay attention to the system's security aspects introduced by the user, configuration or software;
- examine the distributed nature of such an electronic voting system, including the need for available communication channels; and
- use cryptography to provide a secure core in a well-designed, layered architecture that is difficult to penetrate.

Introduction

Electronically supported voting can come in many forms. Most fundamentally, we need to distinguish between remote voting using personal devices or computers and voting at polling stations with voting machines. Remote voting using personal devices or computers is technically and organizationally very complicated. A voter's personal device or computer may not necessarily be trusted because many contain malware or may even have been physically tampered with. Remote voting also takes place in an uncontrolled physical environment, often the voter's home, and there is no option for voting staff to observe and intervene in manipulation attempts, including coercion. As a result, the design and implementation of a trustworthy remote election system is technically and organizationally very challenging.

Voting at polling stations with electronic voting machines excludes those previously mentioned drawbacks. A dedicated voting machine can include trusted hardware, trusted operating systems and mechanisms for tamper resistance or evidence-gathering not commonly found in personal devices or computers. Electronic voting machines can be designed carefully and securely for a single purpose. Accounting for the additional cost of securing an electronic election is easy and can be included in the public election budget.

Nevertheless, even electronic voting machines are not without technical security risks. A 100 percent secure computer system does not exist (Spafford, quoted in Dewdney 1989), and it is important to carefully balance the risks and benefits for democracy's most important process — an election.

Cybersecurity Threats to Electronic Voting

Before discussing potential countermeasures to secure an electronic election, the author will address the cybersecurity threat vectors affecting electronic voting. These include manipulation by the voter, manipulation by the tallier and (technical) manipulation by third parties.

Manipulation by the voter can include casting multiple or invalid votes that are counted in the wrong manner. In some elections, there is also an obligation to vote, which could be violated by not casting a vote. Invalid votes can be the result of a cyberattack by the voter, which can be trivially performed at the user interface or involve complex manipulation of the voting system, including its cryptography. In the simplest voting procedure, a vote can be trivially seen as a vector of many zeros and a one, where the position of the one indicates the candidate voted for. In a well-designed security system, this vote should be kept as secret as possible and not be revealed to any observer, at least not with the voter's identity attached. In a remote voting system, this process implies encrypting the vote. Herein arises the challenge: How can the tallier verify that the vote is valid and not, for example, all zeros and one entry in 100 million? Cryptography can address these challenges (Goldwasser, Micali and Rackoff 1989), but due to the distributed nature of the voting system, the necessary cryptographic mechanism just became much more complicated.

Manipulation by the tallier is defined as any deviation from the correct tallying of all casted votes. Josef Stalin once said, "It doesn't matter who votes, but who counts the votes" (Yasmann 2008). Hence, trust in this task is of the utmost importance for trust to be maintained in the democratic process. The tallier should not be able to count any uncast vote, double count any cast vote or omit counting any cast vote. An advantage of any electronic voting system is that if these complicated security objectives are fulfilled, there is no calculation error and the count is accurate. Manual counting of votes is highly error-prone, and this error can be eliminated by electronic voting.

The technical mechanism to prevent manipulation by the tallier is verifiability. This can include verifiability by a third party where all votes are available (in secret, encrypted form), or verifiability by each voter who can verify that their vote was included in the tally. Maintaining the secrecy of votes while ensuring verifiability is a cryptographic challenge but solvable. The author distinguishes between the technically correct verifiability, which can involve complicated cryptographic procedures (Goldwasser, Micali and Rackoff 1989) and may only be accessible to the experts, and the layman's verifiability where the verification process is accessible to all voters. Given the complexity of electronic voting systems, it seems obvious that a layman can no longer grasp the full extent of all technical and non-technical trust assumptions made in the design of the system. However, complicated cryptographic voting systems can include simple verification procedures that each voter can follow. These procedures would still make assumptions verifiable only to an expert but would enhance the voting process.

It is important to understand the impact of electronic voting on voters' trust in the system. A system that is not accessible and comprehensible may erode trust. However, a simple verification procedure as described may enhance trust despite the system being difficult to analyze. The German Supreme Court (Bundesverfassungsgericht) ruled in 2009 that elections need to be accessible and verifiable by everyone, even those without technical expertise. While this decision rules out a purely electronic vote, it is not clear whether this implies abandoning electronic voting altogether due to its technical complexity, given the above design options, or whether the described procedures can address the need for layman's verifiability, for example, by maintaining a paper copy of each vote. However, plans to introduce electronic voting in Germany were abandoned after this decision, and federal and state elections in Germany are entirely paper based.

Manipulation by third parties is already a major concern in current elections. Note that the current attack vector of manipulating public opinion via social media cannot be addressed by electronic voting, either remotely or by using voting machines. A public that is well informed by the press (or social media) remains an important cornerstone of any democracy. However, electronic voting introduces additional attack vectors for manipulation by third parties (Springall et al. 2014; Wolchok et al. 2010). The prevalence of cybercrime (ransomware and so forth) and the seeming inability even of highly resourceful companies to protect themselves erodes trust in computer systems and, consequently, electronic voting. Such manipulation can include violating the integrity of the voting system, including hardware or software, communication or the communication infrastructure, or the voter's safety.

The Threat of Availability

The author will elaborate on system (hardware and software) security later in this case study but will first highlight the threat of availability. While manipulation of communication messages can be easily detected and mitigated, the availability of a communication channel can be easily violated (Freiling, Holz and Wicherski 2005). The most common communication channel for any electronic voting system is the internet, which is accessible to everyone, including foreign nation-state actors. Denial-of-service attacks that undermine the availability of internet services are still often perpetrated against internet providers. It is relatively easy to create traffic exceeding a network's capacity or use vulnerabilities in the protocols or software to shut down key components of a network. This tactic can undermine an electronic voting system's availability and prevent validly cast votes from being counted. This is particularly worrisome, since many elections are time-restricted and the countermeasures to these cybersecurity threats are mostly reactive. A reactive countermeasure is employed in response to the occurrence of the threat, not proactively preventing the threat. Reactive security is cheaper and more effective against the particular threat, since it can analyze the threat, but this implies a time lag until systems become available again. Any large-scale electronic election should account for this threat by either having organizational measures in place, such as a potential extension of the election period, or alternative means of communication.

Another form of manipulation by third parties constitutes coercion of voters. Voting at polling stations includes physical precautions against such coercion: there is no evidence of the vote cast. In a remote election, this is impossible to achieve because physical measures are not possible. A person can always be present, watching a voter cast their vote. However, even then, possible electronic countermeasures may exist (Clark and Hengartner 2011). A voter may be given a panic password that allows them to cast a vote that is not counted, and the real vote may be cast another time. It will be challenging to educate voters about changed voting procedures and security measures in remote voting, but the advantages of remote voting, such as accessibility and voter convenience, will eventually surpass the deployment challenges. There are past successes that show that high-stakes secure, remote electronic systems can be built. For example, electronic banking is now widely accepted by the public and considered safe. The transition to electronic banking also required changes in user behaviour, such as getting used to secure authentication mechanisms and becoming aware of physical threats.

Cryptographic Mechanisims to Protect Electronic Voting

The previous paragraphs already contain many references to cryptographic mechanisms and how they can be used to implement secure electronic voting. It is important to understand how these mechanisms are designed and evaluated to judge whether they are necessary or sufficient to secure electronic voting. Cryptographic mechanisms are designed as mathematical operations in an abstract system (Anderson 2020). This system simplifies assumptions about the environment, the computing infrastructure and the adversary's capabilities. Such assumptions include the lack of a user, storage or communication interface with the physical world. Often, hardware manipulations are excluded, and the system is reduced to its most abstract mathematical form. Furthermore, cryptography makes assumptions about the computational power of an adversary, which may be challenged in the (distant) future by quantum computers, or the mathematical structure of a particular problem, which has already been very often challenged in the past. However, given these assumptions, cryptography provides the highest form of assurance: a mathematical proof of security. This proof of security is what instills trust in the use of cryptography as a means to protect electronic voting. Given that none of the assumptions are violated, the integrity of the electronic elections is guaranteed by the laws of mathematics.

Types of Errors

However, cybersecurity in real systems rarely fails due to a violation of this design process. There are three main ways that current computer systems are most commonly attacked: user error, configuration error or software error. User error is prevalent and best summarized as "don't click on that link" (in that email). However, in a well-designed electronic voting system, user error should at most lead to an invalid vote, and good interface design should ensure that this remains a rare occurrence (Bernhard et al. 2020). User error should be manageable in the design of electronic voting systems using the principles for security and user interfaces that have been developed. However, user error could be interpreted widely, for example, following advice from strangers on social media and, as such, not addressable by electronic means.

Configuration error is more difficult to manage. At the very least, any electronic voting system needs configurations for the ballot and the communication parties. An invalid ballot, for example, one that excludes a valid candidate or includes an invalid candidate, may affect many voters and the integrity of the election. However, in an electronic voting system, the ballot is nothing but a stream of bytes. As a countermeasure to manipulation, four-eyes principles (i.e., requiring at least two voting officials to approve a configuration) should be built into the entire election process. A single voting official should not be able to manipulate a ballot intentionally or unintentionally. Configuration error can also be addressed by educating the voting staff, automatic and manual testing of the system, and employing design principles for usability.

Software errors are often difficult to detect and almost impossible to prevent. Software is developed by humans who necessarily make mistakes. These mistakes can have dire consequences that can be abused to violate the integrity of the entire system. Imagine a vulnerability in a tallying server that can be exploited by a malformed input, then used to manipulate the system and lead to any election result the attacker desires. Many of the recent malware and ransomware attacks have used small but unknown vulnerabilities in the software, for example, the operating system.

Addressing software vulnerabilities is complicated and subject to current research. Fundamentally, there are three approaches to enhance software security: better software development tool support up to formal verification of the code; organizational processes such as ensuring a secure supply chain (i.e., trustworthy software vendors, open-source software and so forth) and following development principles using these tools, including proper testing; and, finally, resilient system design that incorporates modes of failure and ensures continued operation despite failing components. All these measures reduce the occurrence of software errors but are also very costly. Software developed by the National Aeronautics and Space Administration (NASA) space program is said to fulfill the highest standards of software quality (i.e., almost no software errors), but the development cost is also 10 times that of commercial software (Basili et al. 2002). Still, software errors have occurred in the NASA space program and cost millions of dollars (Sauser, Reilly and Shenhar 2009). Hence, it is crucially important to manage the software development process for electronic voting software to balance risks and costs.

The previous paragraphs may have given a bleak picture of cybersecurity in electronic voting systems, presumably diminishing the role cryptography can play. However, cryptography also enables a design that uses its advantages but does not neglect the challenges. The author envisions using cryptography embedded in electronic voting systems, such as voting machines, that can provide a secure core that, in a layered architecture, is the most difficult for an attacker to penetrate. Such a cryptographic core has the potential to greatly enhance the security of electronic voting systems and prevent certain attacks by malware on voting machines. It must, however, be designed with the correct requirements and balance between costs and risks to create a usable and trustworthy system.

Quantum Computers

The threat of quantum computers to the security of a cryptographic electronic voting system should also be addressed. As already mentioned, the assumptions of any cryptographic system can suddenly be broken, including cryptographic assumptions about the difficulty of solving a particular mathematical problem. Broken assumptions of the past include the security of cryptographic primitives such as MD5 or SHA-1, which were widely used. In response, cryptographic systems should be designed with what is known as crypto agility (i.e., the ability to replace any cryptographic parameter or algorithm). This is a complicated process but necessary for long-lived systems. The feasibility of building a quantum computer that breaks contemporary public-key cryptography should also be noted. Before quantum computers existed, Peter Shor designed the algorithm to break public-key cryptography using a hypothetical quantum computer in 1994. In 1998, the first quantum computer was built. It was soon hypothesized that quantum computers would emerge that could break contemporary public-key cryptography within 15 years. This prompted Ron Rivest, a co-inventor of public-key cryptography, at his keynote at the Financial Cryptography conference in 2001, to make the prediction that in 15 years, no such quantum computer would exist. Fifteen years later, in 2016, when the hypothesis that in 15 years, a quantum computer would break public-key cryptography was still promoted unchanged, Rivest's co-inventor Adi Shamir revisited this prediction in his keynote at the Financial Cryptography conference and made his own prediction that in another 15 years, no quantum computer would exist that could break public-key cryptography.

While some physicists continue to uphold the belief in the emergence of such a quantum computer within 15 years, others began to question whether it is even feasible to build such a quantum computer (Dyakonov 2018). The German BSI, an institution similar to the Canadian Centre for Cyber Security, released an analysis of the feasibility of building such a quantum computer (Wilhelm et al. 2020). This analysis states that, given a national investment comparable to the Apollo space mission or Manhattan Project, it would be feasible to build such a quantum computer, but it also states that it cannot specify the timeframe for such a project given the necessary technological breakthroughs. The report also states that such a quantum computer would be the size of a soccer field and take several hundred days to break a single public key, which is not much faster than traditional supercomputers. While this analysis certainly advocates to delay the use of quantum-safe algorithms, we can try to extrapolate the time given the current level of investment. In 1998, the first quantum computer had two qubits. The largest quantum computer so far, built in 2019, had 49 qubits. To reach the expected one million qubits necessary to break contemporary public-key cryptography will take at least another 60 years given steady exponential growth as in the early days of classical computing. Given all these analyses, it seems safe to assume that the use of quantum-safe cryptography is not necessary in the foreseeable future. Designing a crypto-agile system should fully suffice to accommodate future quantum computers, and it is much more likely that a component will need to be replaced due to the failure of a cryptographic assumption unrelated to quantum computers.

Conclusion

On the one hand, electronic voting systems provide many opportunities, such as higher voter participation due to ease of use (a voting machine can, for example, adjust the screen to accommodate people with vision challenges or provide feedback); reduction of tallying errors (electronic voting can tally error-free); prevention of manipulation attempts (such as discarding ballots or counting non-existent votes); and cheaper and faster execution of elections (due to simplified organizational procedures). On the other hand, electronic voting requires an initial investment to develop the systems (securely) and may raise trust and accessibility issues for people not accustomed to using computers (due to challenges in building mental models to understand the process). In this case study, the author surveyed the technical security risks and challenges. Public discussion often focuses on these risks and emphasizes a distrust in the process. However, given the unstoppable digitization of our lives, electronic voting should be unstoppable as well, and we should focus on finding the right design, processes and mechanisms to implement it safely for future generations.

Works Cited

Anderson, Ross J. 2020. *Security Engineering: A Guide to Building Dependable Distributed Systems.* Indianapolis, IN: Wiley.

Basili, Victor R., Frank E. McGarry, Rose Pajerski and Marvin V. Zelkowitz. 2002. "Lessons learned from 25 years of process improvement: the rise and fall of the NASA software engineering laboratory." *Proceedings of the 24th International Conference on Software Engineering,* May: 69–79.

Bernhard, Matthew, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang and J. Alex Halderman. 2020. "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" *IEEE Symposium on Security and Privacy.*

Clark, Jeremy and Urs Hengartner. 2011. "Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance." *International Conference on Financial Cryptography and Data Security.*

Dewdney, A. K. 1989. "Computer Recreations: Of Worms, Viruses and Core War." *Scientific American* 260 (3): 110–13.

Freiling, Felix C., Thorsten Holz and Georg Wicherski. 2005. "Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks." *European Symposium on Research in Computer Security*: 319–35.

Goldwasser, Shafi, Silvio Micali and Charles Rackoff. 1989. "The Knowledge Complexity of Interactive Proof Systems." *Society for Industrial and Applied Mathematics Journal on Computing* 18 (1): 186–208.

Sauser, Brian J., Richard R. Reilly and Aaron J. Shenhar. 2009. "Why projects fail? How contingency theory can provide new insights — A comparative analysis of NASA's Mars Climate Orbiter loss." *International Journal of Project Management* 27 (7): 665–79.

Springall, Drew, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine and J. Alex Halderman. 2014. “Security Analysis of the Estonian Internet Voting System.” *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. doi:10.1145/2660267.2660315.

Wilhelm, Frank K., Rainer Steinwandt, Brandon Langenberg, Per J. Liebermann, Anette Messinger, Peter K. Schuhmacher and Aditi Misra-Spieldenner. 2020. *Status of quantum computer development.* Bonn, Germany: Federal Office for Information Security. www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Studie-V_1_2.pdf.

Wolchok, Scott, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati and Rop Gonggrijp. 2010. “Security analysis of India’s electronic voting machines.” *Proceedings of the 17th ACM Conference on Computer and Communications Security*: 1–14.

Yasmann, Victor. 2008. “Russia Again Demonstrates Its Past Is Unpredictable.” Radio Free Europe, October 2. www.rferl.org/a/Russia_Again_Demonstrates_Its_Past_Is_Unpredictable/1293374.html.

International Law and Cyber Election Meddling: Unravelling the Grey Zone

Aaron Shull and Kailee Hilt

Key Findings

→ There are no universally understood rules that apply in cyberspace. This ambiguity has allowed adversarial states to exploit the "grey zone" of international law.

→ The "unforeseen" consequences of a state's aggressive cyber tactics, combined with its potential denial of any role or involvement in a cyberattack, have enabled a global ecosystem of distrust.

→ The time has come for the global community to clarify the rules and the subsequent repercussions for foreign electoral interference as a mechanism to foster long-term strategic stability. Existing structures such as the G7 RRM could be leveraged to identify nefarious state actors and swiftly impose a collective punishment.

→ Innovative thinking is needed to ensure that nations such as Canada and Germany can play a leadership role in crafting the governance architecture, whether it be through international discussions defining norms, technical standards or acceptable behaviour in cyberspace.

Introduction

The growing phenomenon of foreign election interference has shaken democracies around the world. From technical attacks on data to targeted influence operations, foreign actors, criminals and domestic groups have pushed boundaries by using bold tactics to sow confusion, fray civic threads and intensify existing societal polarization. While foreign efforts to meddle in elections are hardly new, barriers to entry are low. This has created an operating environment where the scope, scale and sophistication of these efforts are unprecedented. It has now become possible to undertake credible efforts to destabilize targeted states without resorting to conventional warfare.

Concerns over election interference through cyber means have featured prominently over the past several years. Perhaps the most politicized incident was the 2016 US presidential election where Russia pulled off one of the most audacious political scandals in history, marking the beginning of an ongoing assault to disrupt and influence in a sweeping and systematic fashion.[15]

To put this into perspective, in 2016, actors working on behalf of the Russian government hacked the email accounts of the Democratic National Committee and publicly released stolen files and emails, damaging the Hillary Clinton campaign (Rappeport 2016). Beyond this, Kremlin-linked miscreants rapidly spread misinformation using various social media avenues, promoting controversy and divisiveness (Weiss 2018). Efforts centred on acute social issues, ranging from gun rights, terrorism, abortion, immigration and race relations — often exploiting discord that frequently coincided with Donald Trump's rhetoric.[16] Trolls also posed as US citizens and US-based activists as part of their efforts to promote favoured candidates.[17] In addition, recent revelations made by the US Treasury Department indicated that a business associate of campaign officials for Donald Trump leaked polling data and campaign strategy to Russian intelligence services, potentially offering additional demographic targets for Russia's bots and propaganda (Mazzetti and Schmidt 2021).

These efforts were all taking place while the inner workings of the data-mining firm Cambridge Analytica initiated its psychological warfare tactics to predict and potentially influence choices at the ballot box by harvesting millions of Facebook profiles, in one of the tech giant's biggest data scandals to date (Rosenberg, Confessore and Cadwalladr 2018).

The US case makes clear that the digital sphere has become the new battleground, with adversaries intent on crippling the machinery of democratic institutions, and no democratic state is immune. Whether it is a sophisticated hack-and-leak operation to undermine a candidate's campaign or spreading misinformation that prioritizes extreme views, there are growing examples of great powers deploying partisan intervention

[15] See Muller (2019).

[16] See https://intelligence.house.gov/social-media-content/default.aspx.

[17] Ibid.

tactics as a foreign policy tool. Austria, Estonia, France, Germany, Hungary, Italy, Moldova, Montenegro, the Netherlands, Poland, Sweden, Ukraine and the United Kingdom are just some of the states that have had these tactics deployed against the integrity of their elections.[18]

Centring on Germany, Russia (for example) was found to have hacked into the German parliament's computer systems in 2015 (Bennhold 2020), and three years later, it breached the German government's main data network (Eddy 2018). Recently, the European Union's foreign policy chief Josep Borrell Fontelles accused the Russian hacking group Ghostwriter of allegedly interfering in the fall 2021 German parliamentary election by trying to gain access to private email accounts of parliament members using phishing emails (Miller 2021).

Of course, Russia is not the only adversarial state actor that has sought to augment disorder. North Korea, for instance, was implicated in the WannaCry ransomware attack that locked the computers of government agencies and businesses worldwide (Blankstein 2021), while Iran has a history of executing cyberattacks on critical infrastructure with high-profile operations against targets (Center for Strategic & International Studies 2021). There is also no question that China is the most technologically sophisticated country in launching influence campaigns that reach beyond elections, with senior security officials pointing to their efforts to steal IP and trade secrets in a calculated and sophisticated fashion (CSE 2021a).

Given the nature of today's geopolitical environment, attacks on the democratic process in countries around the world will almost certainly expand, posing a serious threat to Canadian and German strategic interests, prosperity and national security. With foreign states (or their proxies) adopting deceptive, clandestine or coercive tactics to advance their regimes, countries such as Canada and Germany cannot be passive and must seek a proactive course to protect the fragile underbelly of liberalism: democratic institutions. Underestimating the menace of electoral interventions jeopardizes the fundamentals of democratic order and responsible government. A much larger public conversation is needed to protect common interests, or else both nations will run the risk of being unprepared for what could be next.

International Law and Cyberspace: A Brief Discussion

A glimpse at the current rule structure demonstrates that there are no universally understood rules that apply in cyberspace. Actors stretch to interpret existing frameworks, such as the UN Charter and international humanitarian law, as applicable to technologies and actions that could not have been contemplated at the time that the law was written. This ambiguity has allowed adversarial states to exploit the grey zone of international law.

In this grey zone, actions are "deliberately designed to remain below the threshold of conventional military conflict and open interstate war" (Corn 2019). While these actions may fall short of war, there is no doubt that they are malevolent and destabilizing. Consequently, "not only do certain features of cyber-activities make international legal regulation very difficult, but major actors also have divergent strategic interests that will pull their preferred doctrinal interpretations and aspirations in different directions, impeding formations of a stable international consensus" (Waxman 2011, 425–26).

The UN Charter limits states' ability to use force. Article 2(4) stipulates that all member states "shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."[19] Any activity above this threshold would only be lawful under a very few prescribed exceptions. The first refers to actions authorized by the UN Security Council under chapter VII of the charter, which is not relevant here. The second is pursuant to article 51, which provides that "nothing in the present Charter

[18] *Cockrum v Donald J. Trump for President, Inc*, 365 F Supp (3d) 652 (ED Va 2019).

[19] *Charter of the United Nations*, 26 June 1945, Can TS 1945 No 7, art 2(4).

shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations."[20]

Nonetheless, the current legal interpretation and scope of the application of the "use of force" reflects a narrow approach and excludes all actions that are inherently non-violent. Typically, cyber-based interference and disinformation campaigns do not cause physical damage, even though they certainly have the power to destroy the legitimacy of an institution without the need for physical force. Prevailing legal interpretation, such as the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,*[21] one of the most widely recognized attempts to establish a framework on how to categorize different cyberattacks in the context of international law, does not construe interference as an act of war. In this way, we have reached a perverse time in legal history, where an adversarial state might destroy the ability of a democratic state to govern itself with legitimacy, which could undermine the fabric of its society and destabilize its national identity, but it does not constitute one of the highest crimes under international law: the illegal use of force.

Problems in applying the use of force framework to cyber operations have shifted the focus of election interference to violations of state sovereignty and the principle of non-intervention — both foundational principles of international law. At its most basic level, the principle of non-interference, for instance, provides that "no state has the right to intervene in the internal or external affairs of another."[22]

There are two broadly supported UN General Assembly resolutions that have some bearing on the scope of this principle. The first is the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty (Declaration on Intervention). The second is the Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations (Friendly Relations Declaration).[23] While strikingly similar, the relevant operative paragraph of the Friendly Relations Declaration is slightly more robust, as there is an explicit prohibition on any form of interference with the political, economic and cultural elements of another state (Shull 2013). It says: "no State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic, and cultural elements, are in violation of international law."[24]

These broad statements have also been endorsed by the International Court of Justice, which buttressed these rules in *Nicaragua v. United States of America* by affirming that the principle of non-intervention is part of customary international law[25] and that "a prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social, and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones."[26]

However, the notion of sovereign prerogative does have limits. "The question is where to locate the limit — which domains or activities should be off-limits because they fall within a State's *domaine réservé*[27] and which domains are subject to foreign action."[28]

[20] Ibid., art 51.

[21] The *Tallin Manual* 2.0 serves as an "expression of opinions of a group of independent experts acting solely in their personal capacity [and] does not represent the views of the NATO CCD COE, its Sponsoring Nations, or NATO. It is also not meant to reflect doctrine. Nor does it reflect the position of any organization or State represented by observers." See Schmidt (2017, 23).

[22] *Montevideo Convention on the Rights and Duties of States,* 26 December 1933, 49 Stat 3097, TS No 881, 165 LNTS 19 art 8 (entered into force 26 December 1934).

[23] *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations,* GA Res 2625 (XXV), UNGA, 25th Sess, UN Doc A/RES/2625(XXV) (1970).

[24] Ibid.

[25] "Customary international law consists of rules that are not found in a treaty but are nevertheless widely acknowledged to be binding for states despite being unwritten." See Schmidt (2020).

[26] See *Nicaragua v United States of America,* [1986] ICJ 14 at para 205, online: <https://casebook.icrc.org/case-study/icj-nicaragua-v-united-states>.

[27] This refers to a state's "exclusive power to regulate its internal affairs without outside interference." See Ohlin (2017, 1587).

[28] Ibid., 1588.

This analysis then rests on the presence or absence of coercion. Typically, acts that do not involve coercion lie outside the reach of the prohibition on intervention. The *Tallin Manual 2.0* concludes that the non-intervention principle might apply when "using cyber-operations to remotely alter electronic ballots and thereby manipulate an election" (Schmidt 2017, 313). However, in the case of the 2016 US presidential election, there was no evidence that Russian hackers changed the votes; instead, "they launched social media influence operations and released embarrassing hacked information from the Hilary Clinton campaign" (Marks 2021). In other words, election interference that does not manipulate the election process directly but seeks to influence voters' behaviour freely through information used to micro-target, may not — somewhat absurdly — constitute coercion under international law.

Some legal scholars have contended that there needs to be an added layer to connect the violation of the principle of non-intervention to the principle of self-determination. The essence of self-determination is articulated in article 21(3) of the Universal Declaration of Human Rights, which states "the will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures."[29] This is further matched by article 1 of the International Covenant on Civil and Political Rights that affirms that all peoples have the right of self-determination, and by virtue of that right, they freely determine their political status, and is further supported by article 25(b), which obligates states to ensure that the will of the electors is "free." This combination largely equates to the right of individuals to freely choose one's own political and economic regime, which is actualized through the electoral process when exercised without coercion. Equally, "external interference not only inverses this process by undermining its integrity and freedom but also impinges on the expression of authority and will by the government that emerges. It thus transpires that by aligning the principles of non-intervention and self-determination, the normative and operational scope of non-intervention shifts to the people and to the process of forming authority and will" (Tsagourias 2019).

However, the right of self-determination has remained fallow within the context of international law since the legal discourse generally shifts to state sovereignty.

The lack of shared norms on how to interpret the rules surrounding sovereignty has emphasized that not all aspects transfer equally well into the cyber environment. The UN Group of Governmental Experts (GGE) concluded in its 2015 consensus report that "state sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory."[30] However, even if it can be determined that a violation of state sovereignty has occurred, as with any cyberattack, there is the issue of attribution: "To get around this challenge, many actors simply define influence operations instigated from a sovereign territory separate from the targeted state as 'foreign' and condemn such operations by appealing to the principle of due diligence, the duty of a state 'not to allow knowingly its territory to be used for acts contrary to the rights of other States'" (Ördén and Pamment 2021, 3–4).

Plainly, the application of international law does not clearly address the issue of election interference within the cyber sphere. Foreign interference, such as espionage and covert operations, has, in turn, become an expected aspect of geopolitics. This ambiguity in the law will continue to breed international instability. Even though there have been significant efforts to advance the collective understanding of the applicability of pre-cyber-era international law to cyber operations, it does raise a pointed question: Why attempt to apply laws that were designed before computers existed? Why not update the international governance structure to account for contemporary technological realities? In the meantime, as emerging technologies and new tactics of cyber disruption continue, so too will the definitional questions and deliberations on how to respond.

[29] *Universal Declaration of Human Rights,* GA Res 217A (III), UNGAOR, 3rd Sess, Supp No 13, UN Doc A/810 (1948) 71, online: <www.un.org/en/about-us/universal-declaration-of-human-rights>.

[30] See <https://unidir.org/sites/default/files/2019-10/GGE-Recommendations-International-Law.pdf>.

A Selection of Cyber Norm Processes

The United Nations has released substantial recommendations on advancing responsible state behaviour in cyberspace in the context of international security. There are two competing initiatives: the first is the US-sponsored GGE; the other is the Russia-sponsored Open-Ended Working Group (OEWG). Both processes have focused on cybersecurity norms, such as those designed to protect critical infrastructure and supply chains. Encouragingly, the core commitments in the final GGE report mirrored those recognized by the parallel OEWG released in March 2021. They accepted that international law applies online and that the norms of responsible state behaviour agreed upon in the 2015 GGE report need to be upheld.[31] Thus, "norms and existing international law sit alongside each other. Norms do not seek to limit or prohibit action that is otherwise consistent with international law. They reflect the expectations of the international community and set standards for responsible State behaviour. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development."[32]

The call for protection against foreign election interference has been flagged by many state and non-state parties for consideration by both processes. Norm 13(f) specifically outlines that "a State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public." It then goes on to define sectors considered to be critical infrastructure and therefore off-limits to attack, which includes electoral processes.[33] The OEWG final report addressed the issue of "the protection of the public core of the internet — albeit in modified language — in both the threat section and the norms section and flagged the vulnerability of the infrastructure underlying political and electoral processes as a threat" (Broeders 2021, 21).

While norms are extremely useful, they are, unfortunately, not binding. There are misunderstood features of how norms actually work, which makes it possible to stigmatize actions that fall outside expectations, as with, for example, "rogue states" (Raymond 2020). The OEWG and other actors have observed that even though the norms have been adopted by the entire UN membership, lack of awareness hampers solidification of commitments, stressing that accountability and compliance in today's geopolitical environment continue to be a challenge.

The issue with the GGE and the OEWG is that they both rely on consensus, meaning if one country objects, agreement cannot be met. For the past several years, both groups have been working separately on the same governance issues with small tangible progress. As the GGE has now concluded, France and Egypt, along with more than 40 other states, are pushing for a "Programme of Action" (Digwatch 2020a) that would aim to end the "dual track discussions." Its goal would be to urge countries to implement the cyber principles they agreed to in 2015. It would also provide an avenue to potentially eliminate redundancy or duplication, as well as the added cost of having two bodies essentially addressing the same issues. But it is unclear whether this will move forward, as Russia has already secured a new OEWG for the years 2021–2025 (Digwatch 2020b).

There is also a separate UN body referred to as the open-ended Cybercrime Ad Hoc Committee that was established in 2019. This ad hoc committee is tasked with drafting a new cybercrime convention by 2023. To do so, it seeks to elaborate on a "comprehensive international convention on countering the use of information and communications technologies for criminal purposes."[34] Within this effort, Russia has proposed the creation of a global cybercrime treaty. However, Canada and other nations believe states should continue to use existing tools, such as the 2004 Budapest Convention,

[31] See *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UNGA, 70th Sess, UN Doc A/70/174, online: <https://undocs.org/en/A/70/174>.

[32] See *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UNGA, 76th Sess, UN Doc A/76/135 (2021), online: <https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf>.

[33] Ibid.

[34] See https://dig.watch/processes/cybercrime-ad-hoc-committee.

that set out common procedures for law enforcement cooperation in cybercrime cases.

The 2004 Budapest Convention "aligns member countries' laws covering acts that are considered computer crimes, and the powers that can be used to secure electronic evidence of serious crimes. This makes it easier for countries to cooperate on criminal investigations on cybercrime and wider crimes involving electronic evidence" (New Zealand Government 2020, 2). It is the only binding international instrument on the issue of cybersecurity that has been ratified by 65 countries.

Moreover, the fact that a government that faces widespread criticism for turning a blind eye to cybercriminals operating within its own borders is pushing a global cybercrime treaty is menacing. In recent years, Russia has significantly expanded its laws and regulations, fostering online surveillance of its citizens and filtering access to content from the outside world (Human Rights Watch 2020). Not surprisingly, the divisive vote on the global cybercrime treaty has exposed disagreements that focus on understanding what constitutes cybercrime, how law enforcement would be granted access to data in cross-border investigations and the role of governments in regulating the internet (Brown 2021).

Of course, several of these questions, in turn, raise significant implications for human rights, especially within the realm of privacy, due process, and freedom of expression and association. In essence, the stark disagreements regarding Russia's proposed treaty have revealed themselves long before states have even begun to discuss substance, suggesting a complicated path ahead for this agenda.

Aside from the United Nations, there have also been several initiatives that seek to establish voluntary principles around responsible state behaviour online. The Paris Call for Trust and Security in Cyberspace, for instance, is an effort that 79 other states and nearly a thousand civil society organizations and companies support.[35] This broad call for trust is an attempt to get states to agree to a set of international rules for cyberspace. It does, however, fall short of a detailed treaty. Rather, it is a high-level, non-binding document that calls for states to "promote the widespread acceptance and implementation of international norms of responsible behaviour as well as confidence-building measures."[36] It includes a series of principles such as defending elections from cyberattacks, protecting IP from theft and condemning the use of hacking tools by non-state actors.[37]

While the Paris Call urges states to strengthen capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities,[38] it avoids directly condemning these activities on a legal or normative basis. This is unlike the Global Commission on the Stability of Cyberspace that proposed a norm for the protection of election infrastructure, which openly condemns election interference beyond referring to these activities as simply "malign" and "malicious."

Explicitly, the Global Commission's 2019 report on *Advancing Cyberstability* stated that "governments must commit to refraining from engaging in cyber operations against the technical electoral infrastructure of another state. In recommending this norm, the Commission merely affirms that election interference is intolerable whether it is considered to be a violation of international law or not" (Global Commission on the Stability of Cyberspace 2019, Appendix B). This is further supported by suggesting stronger international cooperation in an effort to prevent, mitigate and respond to cyber intrusions against electoral infrastructure.

It is also worth noting that in June 2018, the G7 RRM[39] was announced at the Charlevoix G7 Summit[40] in response to foreign actors seeking to undermine a state's democratic societies and

[35] See https://pariscall.international/en/.

[36] See www.canada.ca/en/democratic-institutions/news/2020/05/frequently-asked-questions—paris-call-trust-and-security-in-cyberspace.html.

[37] Interestingly, the European Union joined the Paris Call following the latest Paris Peace Forum in September 2021. This was announced within the context of the European Union's initiatives relating to cyber resilience, AI and platform responsibility. In addition, the United States also joined, which came on top of efforts to hold countries accountable for harbouring online criminals, a long-awaited revamp of North Atlantic Treaty Organization (NATO) cybersecurity policy and an anti-ransomware alliance formed in October 2021.

[38] See Paris Call, principle 3, https://pariscall.international/en/principles.

[39] See www.canada.ca/en/democratic-institutions/news/2019/01/g7-rapid-response-mechanism.html.

[40] See www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2018-06-09-defending_democracy-defense_democratie.aspx?lang=eng.

institutions, electoral processes, sovereignty and security. A coordination unit was set up within Global Affairs Canada (GAC), serving as a permanent secretariat to the RRM by enabling information sharing and threat analysis and identifying opportunities for coordinated responses to diverse and evolving threats.[41]

Fostering cyber diplomacy requires more than the involvement of state actors, as industry and civil society also have a crucial role in strengthening capacity for a peaceful and more secure cyberspace. A recent example of this is the Oxford Process on International Law Protections in Cyberspace, a laudable effort organized by the Oxford Institute for Ethics, Law and Armed Conflict. It was established in partnership with Microsoft and brings together international legal experts from across the globe who are dedicated to identifying and clarifying the rules of international law applicable to cyber operations across a variety of contexts, one of which focuses on foreign electoral interference through digital means.[42]

Remarkably, even though there have been considerable efforts to advance this complicated area of policy, questions continue to flourish, mainly: How can states best tackle new and emerging security threats amid an environment of eroding international trust? Can normative constraints really limit state behaviour? If the norms negotiated to date are to be respected, what should the consequences be for breaking them, and how will those consequences be coordinated? Clearly, the digital sphere has become a central domain for international conflict requiring capacity-building efforts among states if stability is to be enhanced.

Conclusion

The ungoverned nature of cyberspace is presenting new barriers, widening old gaps and sowing mistrust like never before.

There are three concluding points to be made:

→ The international rules-based system in cyberspace is still in its infancy, despite multiple efforts under way in national, multinational, multi-stakeholder, academic and private sector fora. Even though there exists ambiguity in applying international law to cyberspace, and this can afford states a tactical advantage, the time has come for the global community to clarify the rules and the subsequent repercussions of disruption to enable long-term strategic stability. There needs to be concerted, coordinated efforts to punish states that impose ever more menacing cyber operations. Whether, for example, it be through an articulated framework or a model that mirrors a judicial sentencing guideline, imposing steep penalties is required to both deter and denounce conduct that strikes at the very heart of democracies: the legitimacy of the electoral process. Existing structures such as the G7 RRM could be leveraged to identify nefarious state actors and levy a collective punishment swiftly.

→ Innovative thinking is needed to ensure that nations such as Canada and Germany can play a leadership role in crafting the governance architecture. As Shelly Bruce, chief of Canada's CSE, noted in a public speech to the Centre for International Governance Innovation, "irresponsible cyber activity undermines the stability and predictability of cyberspace. Canada must be ready to respond. And at the same time, Canada must [continue to] actively participate in domestic and international discussions defining the norms, technical standards, and acceptable behavior in cyberspace" (CSE 2021b). Underestimating the threat of electoral interventions puts in jeopardy the fundamentals of democratic order and responsible government. It is important for Canada and Germany to protect common interests — or both nations will run the risk of being unprepared.

→ If the last decade has taught democracies around the world anything, it should be that no nation should be caught off guard when its election is the target of an interference campaign. The extreme degree of secrecy surrounding cyberweaponry and the subsequent threats posed by hostile states, criminals and others will only continue to deepen as emerging technology continues to proliferate. At the same time, most nations remain underprepared for what is likely to come.

[41] See www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/rrm-mrr.aspx?lang=eng.

[42] See www.elac.ox.ac.uk/the-oxford-statement-on-international-law-protections-against-foreign-electoral-interference.

Works Cited

Bennhold, Katrin. 2020. "Merkel Is 'Outraged' by Russian Hack but Struggling to Respond." *The New York Times*, May 13. www.nytimes.com/2020/05/13/world/europe/merkel-russia-cyberattack.html.

Blankstein, Andrew. 2021. "U.S. indicts three North Koreans in massive WannaCry, Sony hacks." NBC News, February 17. www.nbcnews.com/politics/justice-department/u-s-indicts-three-north-koreans-massive-wannacry-sony-hacks-n1258096.

Broeders, Dennis. 2021. "The (im)possibilities of addressing election interference and the public core of the internet in the UN GGE and OEWG: a mid-process assessment." *Journal of Cyber Policy* 6 (3): 277–97. doi:10.1080/23738871.2021.1916976.

Brown, Deborah. 2021. "Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights." Just Security, August 13. www.justsecurity.org/77756/cybercrime-is-dangerous-but-a-new-un-treaty-could-be-worse-for-rights/.

Center for Strategic & International Studies. 2021. "Significant Cyber Incidents Since 2006." https://csis-website-prod.s3.amazonaws.com/s3fs-public/211004_Significant_Cyber_Incidents.pdf?.

Corn, Gary P. 2019. "Navigating Gray-Zone Challenges in and through Cyberspace." In *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, edited by Winston S. Williams and Christopher M. Ford, 345–430. New York, NY: Oxford University Press.

CSE. 2021a. *Cyber Threats to Canada's Democratic Process: July 2021 Update*. Ottawa, ON: CSE. https://cyber.gc.ca/sites/default/files/2021-07/threat-to-democratic-process-2021-3-web-e.pdf.

———. 2021b. "Chief Shelly Bruce's speech for Centre for International Governance Innovation, May 18, 2021." CSE, May 18. https://cse-cst.gc.ca/en/information-and-resources/chief-shelly-bruces-speech-centre-international-governance-innovation-may.

Digwatch. 2020a. "France and partners propose a programme of action for advancing responsible state behaviour in cyberspace." Digwatch, October 8. https://dig.watch/updates/france-and-partners-propose-programme-action-advancing-responsible-state-behaviour.

———. 2020b. "Two UN resolutions on OEWG and GGE adopted." Digwatch, November 9. https://dig.watch/updates/two-un-resolutions-oewg-and-gge-adopted.

Eddy, Melissa. 2018. "Germany Says Hackers Infiltrated Main Government Network." *The New York Times*, March 1. www.nytimes.com/2018/03/01/world/europe/germany-hackers.html.

Global Commission on the Stability of Cyberspace. 2019. *Advancing Cyberstability Final Report*. November. https://cyberstability.org/report/#6-norms.

Human Rights Watch. 2020. "Russia: Growing Internet Isolation, Control, Censorship." Human Rights Watch, June 18. www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship.

Marks, Joseph. 2021. "The Cybersecurity 202: Legal scholars are working on the new rules for international hacking conflicts." *The Washington Post*, June 21. www.washingtonpost.com/politics/2021/06/21/cybersecurity-202-legal-scholars-are-working-new-rules-international-hacking-conflicts/.

Mazzetti, Mark and Michael S. Schmidt. 2021. "Biden Administration Says Russian Intelligence Obtained Trump Campaign Data." *The New York Times*, April 15. www.nytimes.com/2021/04/15/us/politics/russian-intelligence-trump-campaign.html.

Miller, Maggie. 2021. "EU 'denounces' Russian malicious cyber activity aimed at member states." *The Hill*, September 24. https://thehill.com/policy/cybersecurity/573867-eu-denounces-russian-malicious-cyber-activity-aimed-at-member-states.

Muller, Robert S. 2019. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. Vol. 1. Washington, DC: US Department of Justice. www.justice.gov/archives/sco/file/1373816/download.

New Zealand Government. 2020. "What is the Budapest Convention?" July 15. https://consultations.justice.govt.nz/policy/budapest-convention/user_uploads/1.-what-is-the-budapest-convention.pdf.

Ohlin, Jens David. 2017. "Did Russian Cyber Interference in the 2016 Election Violate International Law?" *Texas Law Review* 95: 1579–98.

Ördén, Hedvig and James Pamment. 2021. "What Is So Foreign About Foreign Influence Operations?" Carnegie Endowment for International Peace, Lines in the Sand Series No. 1. https://carnegieendowment.org/files/Orden_Pamment_ForeignInfluenceOps2.pdf.

Rappeport, Alan. 2016. "New Documents Released From Hack of Democratic Party." *The New York Times*, September 13. www.nytimes.com/2016/09/14/us/politics/dnc-hack.html.

Raymond, Mark. 2020. "Confronting the Ubiquity of Norms in Cyberspace and Cyber Governance." *Lawfare* (blog), March 12. www.lawfareblog.com/confronting-ubiquity-norms-cyberspace-and-cyber-governance.

Rosenberg, Matthew, Nicholas Confessore and Carole Cadwalladr. 2018. "How Trump Consultants Exploited the Facebook Data of Millions." *The New York Times*, March 17. www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

Schmidt, Michael N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge, UK: Cambridge University Press.

———. 2020. "Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace." *Texas National Security Review* (Summer): 32–47.

Shull, Aaron. 2013. "Cyber Espionage and International Law." GigaNet: Global Internet Governance Academic Network, Annual Symposium. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2809828.

Tsagourias, Nicholas. 2019. "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace." *EJIL:Talk!* (blog), August 26. www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/.

Waxman, Matthew C. 2011. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." *Yale Journal of International Law* 36: 421–59.

Weiss, Brennan. 2018. "A Russian troll factory had a $1.25 million monthly budget to interfere in the 2016 US election." *Business Insider*, February 16. www.businessinsider.com/russian-troll-farm-spent-millions-on-election-interference-2018-2.

Evaluating Applicable Canadian and German Domestic Law to Address the Challenges of Foreign Interference

Michael Pal

Key Findings

→ Canada and Germany have both updated their laws to deal with the challenges of foreign interference. The most controversial aspect of these reforms has been the impact on freedom of speech and expression online.

→ Both countries have imposed regulations on social media platforms. Canada has relatively strict regulation of foreign spending, third-party and interest groups, and political contributions in comparison to Germany.

→ The German Network Enforcement Act (NetzDG), which includes notice and takedown requirements for illegal content online, would raise difficult constitutional questions if a similar model were to be used in Canada.

→ The responses of both jurisdictions to foreign interference will be studied closely by other democracies.

Introduction

Foreign interference in elections is a long-standing problem plaguing democracies.[47] The Cold War saw plentiful examples of meddling by foreign states in elections.[48] The problem of foreign interference in elections has taken on a new urgency with the growth of the internet and the widespread use of social media, which facilitate global connections both beneficial and malign.[49] Both Canada and Germany have taken action in recent years to address foreign interference in its contemporary form in their domestic elections. The two countries have, however, taken different approaches.

The actions taken by each democracy have been structured and limited by their respective constitutions, which protect freedom of political speech. In Canada, the approach has been to prohibit the most obvious forms of disinformation regarding the conduct of elections, to tighten up campaign finance law to limit opportunities for financial involvement by foreign actors, and to introduce some modest regulation of the social media platforms that facilitate communication from foreign actors directly to Canadian voters. The German approach is mainly centred around the NetzDG law, which, most notably, implements a mandatory takedown regime for some illegal content distributed online.

Both the Canadian and German approaches to the problem of foreign interference are at best partial. They are first steps, rather than panaceas. Both countries are important examples for other democracies to draw on in the ever-evolving search for how best to address the contemporary manifestation of the old problem of foreign interference.

Canada

The Canadian Constitution

The Canadian Constitution establishes the country as a federal parliamentary democracy. Unlike the German Constitution, the Canadian Constitution specifies little about the operation of elections and political parties. The main constitutional provision relevant for the regulation of foreign interference in elections is section 2(b) of the Canadian Charter of Rights and Freedoms.[50] Section 2(b) protects freedom of expression, including political expression. It does so for "everyone," including foreign speakers, and also protects the freedom of listeners. The Supreme Court of Canada has interpreted section 2(b) very broadly so that it applies even to expression that has little value, such as deliberately told lies. Given this broad constitutional protection, election law in Canada has only attempted to address misinformation and disinformation at the margins.

[47] For the long history of election interference, see Levin (2020).

[48] Ibid., 152–67.

[49] See the three reports from CSE (2017; 2019; 2021).

[50] *Constitution Act, 1982*, s 35, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.

Regulation of Canadian Elections

Given the lack of specificity in the constitution regarding elections, most of the details of Canadian election law therefore fail to be determined by federal legislation. Canadian federal elections are tightly regulated by the Canada Elections Act. The main entities subject to the act are political parties, candidates and third parties, among others. Political parties, candidates, third parties and other regulated entities must register and report regularly to the non-partisan, independent electoral management body, Elections Canada.

It is important to note that, unlike Germany and some comparable jurisdictions such as the United States and Australia, Canada has a strict "egalitarian" model of campaign finance law (Feasby 1999). The Supreme Court of Canada has upheld relatively stringent limits on campaign spending during the election period as a reasonable and proportionate restriction on freedom of political expression.[51] Restrictions on contributions to political parties and their candidates are also tightly limited by the Canada Elections Act.[52]

It is in this context of reporting, disclosure and egalitarian campaign finance requirements that the current rules against foreign interference, mis- and disinformation have been introduced. They are mainly from the Elections Modernization Act of 2018,[53] although some restrictions predate that legislation.[54] Campaign malfeasance has been a perennial feature of Canadian elections, whether online or offline.

The Critical Election Incident Public Protocol is the mechanism by which foreign interference during an election campaign is reported to the public.[55] Given the highly sensitive nature of the decision to report interference, and the potential for it to shape the election campaign and outcomes, the protocol is an important element of the Canadian approach. Put in place for the 2019 election, the protocol is interpreted and administered by a panel of senior public servants.[56] The panel did not report any particular incidents in the 2019 or 2021 elections that rose to the threshold that it deemed necessary to trigger communication to the public.

Money in Politics

Foreign donations to political parties and candidates are explicitly prohibited by the Canada Elections Act.[57] The relatively strict limits on contributions to parties and candidates also indirectly help reduce the possibility of foreign donations. A clean domestic campaign finance system makes it easier for electoral authorities, other parties, researchers and the media to detect large sums of illicit money flowing into the coffers of a party.

Other important actors who have, in the past, been a venue for foreign influence in elections are third parties. Third parties are individuals or associations other than political parties, candidates and their affiliated entities. Individuals, interest groups, corporations and unions often act as third parties during elections for the purpose of conducting election advertising. The regulation of third parties is particularly relevant because many Canadian interest groups operate across the border with the United States, or on an international basis, and may accept contributions for foreign entities to fund advertising or other political activities. To the extent that their advertising campaigns are funded by foreign entities, that is a significant potential source of foreign involvement.

The total amount third parties can spend during the election campaign has been limited for a number of years (Feasby 1999) and was upheld as a constitutionally valid limit on freedom of political expression.[58] The spending limit is at a comparatively low amount and especially so in comparison to

[51] *Harper v Canada,* 2004 SCC 33. The spending limit applied to "third parties," which are interest groups or individuals.

[52] *Canada Elections Act,* SC 2000, c 9.

[53] *Elections Modernization Act*, SC 2018, c 31. For a summary of the legislation, see Pal (2018).

[54] Candidates, for example, have long been barred from falsely claiming during the election that an opposing candidate has dropped out: see *Canada Elections Act*, *supra* note 52, s 92.

[55] See www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol/cabinet.html. The protocol works in tandem with the Security and Intelligence Threats to Elections (SITE) Task Force involving the Royal Canadian Mounted Police (RCMP), the Global Affairs Canada G7 RRM, the Canadian Security Intelligence Service (CSIS) and the CSE. See www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html.

[56] The members are the clerk of the Privy Council, the national security and intelligence advisor to the prime minister, and the deputy ministers of justice, public safety and global affairs.

[57] *Canada Elections Act*, *supra* note 52, s 363(1).

[58] *Harper v Canada, supra* note 51.

systems such as Germany's where there is no spending limit imposed on interest groups.

The limits on third-party activity have been extended in recent years. A spending limit now applies in the "pre-writ" period of the months immediately prior to a fixed-date federal election (Pal 2017).[59] Perhaps most importantly, it has been since 2018 impermissible for domestic third parties to use foreign contributions for their core political activities, such as election advertising during the election period and the time just prior to it.[60] The Elections Modernization Act also expanded the types of activities of third parties that are regulated, from just advertising to also polling, get-out-the-vote and other partisan or political spending. All of these activities are subject to the ban on foreign contributions. Foreign third parties are also explicitly banned from carrying out regulated activities, including advertising and get-out-the-vote, during the pre-writ and election periods.[61]

Regulation of Social Media Platforms

The Elections Modernization Act introduced a new category of regulated entities for the purposes of elections: social media platforms. Television and radio broadcasters are primarily regulated by Canadian telecommunications law and, to a much smaller extent, by the Elections Act, with regard to elections. Under the Elections Act, parties and candidates are entitled to free broadcast time,[62] and broadcasters cannot discriminate for or against a party in selling advertising space.[63]

The Elections Modernization Act brought the largest social media platforms under a separate set of rules distinct from those of the traditional broadcasters.[64] Social media is characterized by a number of relevant features that distinguish it from broadcast or print media. These platforms facilitate micro-targeted advertising to individual users or small groups that the general public cannot see and therefore cannot scrutinize. It is also difficult for the audience or a regulator to know the source of an advertisement on a social media platform, in particular whether it is from a foreign or domestic source.

The Elections Modernization Act responded to fears of foreign interference in the form of paid, micro-targeted advertising on Facebook and other platforms that had arisen in the 2016 US election through a number of measures. To ensure transparency, social media platforms[65] must now, under Canadian law, maintain repositories of all paid election advertising.[66] These repositories can then be investigated and checked against mandatory reporting by political parties and third parties to ensure the rules are being followed and that there is no foreign involvement. As the measures apply only to paid advertising, they do not in any way address foreign mis- or disinformation spread in fora such as Facebook Groups, which is a significant gap.

Social media companies are also now explicitly banned from accepting money from foreign sources to place election advertisements on their platforms.[67] It is unclear how the platforms have interpreted this prohibition. For instance, we do not have direct evidence of whether platforms now undertake more stringent due diligence to ensure foreign advertisements cannot be placed on their platforms. It is important to note that these measures were deemed so onerous to comply with that some platforms, notably Google, declined to accept election advertising at all after the passage of the Elections Modernization Act (Pal 2020, 210).

Restrictions on Mis- and Disinformation

As with many other democracies around the world (Ringhand 2021), Canada has introduced election law that also contains some restrictions on mis- and disinformation. The Charter's protection for free political expression, including lies, however, restricts how far any government can go in addressing mis- and disinformation.

The Canada Elections Act now prohibits impersonation of candidates for office, with

[59] *Canada Elections Act, supra* note 52, s 2 (see definitions of "partisan advertising" and "pre-election period").

[60] Ibid., ss 349.02, 495.21.

[61] Ibid., ss 349.4(1), 351.1(1).

[62] Ibid., ss 335(1), 345(1).

[63] Ibid., s 348.

[64] Ibid., s 325.1.

[65] Only the largest platforms, based on users, are covered. See *Canada Elections Act, supra* note 52, s 325.1(1).

[66] *Canada Elections Act, supra* note 52, s 325.1(2)–(5).

[67] Ibid., s 349.02.

exceptions for satire.[68] It is also illegal to impersonate or purport to represent the chief electoral officer or an Elections Canada official. The prohibitions on impersonation would also likely apply to so-called deepfakes and other forms of manipulated and deceptive videos (Judge and Korhani, forthcoming 2022). These measures can be understood as limiting disinformation by foreign or domestic actors that harms the capacity of Canada to carry out a free and fair election.

There are some narrow measures aimed at "misinformation" rather than "disinformation," although their constitutionality is less certain. Section 91 of the Canada Elections Act is Canada's equivalent of an "anti-birther conspiracy" provision. The section prohibits dissemination of incorrect statements during an election about a candidate's place of birth, but also profession, criminal record or lack thereof, and some other factual matters (Dawood 2021). The provision was struck down as unconstitutional by an Ontario court,[69] although it appears likely to be reintroduced in a narrower form such that only intentionally spread lies about those factual details would be caught.

Germany

The Basic Law

Like Canada, Germany is a federal constitutional democracy. There are several pertinent differences in their legal and constitutional framework for regulating elections, including foreign interference. Germany's Constitution, the Basic Law,[70] creates a democracy with regular and free elections (article 20(1)). Article 5 protects freedom of speech, including political speech. Like the protection for political expression in the Canadian Charter, the Basic Law anticipates reasonable limits on free speech (article 5(2)).

Unlike Canadian constitutional law, the Basic Law directly addresses the presence of "unconstitutional political parties." The Basic Law famously deems some political parties as unsuitable to participate in electoral democracy, which is a response to the rise of the Nazi Party prior to the Second World War. German constitutional and election law therefore assumes that some parties will be prohibited. More recent rules against foreign involvement in elections therefore include restrictions on support by hostile foreign actors for banned German political parties.

German Elections and Campaign Finance

German federal electoral legislation regulates nearly all aspects of the democratic process. The main instruments are the Federal Elections Act,[71] Federal Electoral Regulations issued by the Ministry of the Interior pursuant to section 52 of the act and the Political Parties Act.[72] German election law emphasizes transparency, partial public funding of political parties due to their essential role in contemporary democracy, and a libertarian rather than egalitarian approach to money in politics. These features of German election law all have an impact on the regulation of foreign interference. Political parties are required to be transparent about their spending, contributions received and other aspects of their activities. They receive partial state funding based on a complex formula, taking into account their performance in the previous federal, state and European Parliament elections, as well as the amount of private donations they received. They do not face meaningful limits on contributions to the party or on spending.[73]

There is arguably a relationship between domestic campaign finance or political party law and foreign interference. To the extent that domestic contributions and spending are tightly regulated, it is easier to notice when money from foreign sources is flowing in to influence a domestic election. German law allows donations from foreigners under 1,000 euros and also permits citizens of the European Union to donate on the same terms as

[68] *Canada Elections Act, supra* note 52, s 481(1).

[69] For an argument against section 91 and similar prohibitions, see Karanicolas (2019).

[70] *Basic Law for the Federal Republic of Germany,* 23 May 1949, online: <www.gesetze-im-internet.de/englisch_gg/englisch_gg.pdf>.

[71] Federal Law Gazette I p. 1288 as promulgated on July 23, 1998, last amended by Article 2 of the Act of June 3, 2021.

[72] Federal Law Gazette I p. 149 as promulgated on January 31, 1994, last amended by Ninth Act Amending the Political Parties Act on December 22, 2004.

[73] *Political Parties Act*, Federal Law Gazette I p. 773 as published on 24 July 1967.

German citizens.[74] Some foreign involvement is therefore expected and permitted. Germany's laws require transparency, but the amount of money that can be contributed and spent is essentially unlimited, which dramatically scales up the risk.

NetzDG

Into this mix came the now famous NetzDG law first passed in 2017 (Gorwa 2021; He 2020).[75] The law has been amended since its introduction but maintains its basic components. It applies to the largest social media platforms, in particular Facebook and Twitter, rather than peer-to-peer messaging apps. The covered platforms must report on complaints regarding illegal content; take down clearly illegal content within 24 hours and, for more complicated instances, within seven days; inform users regarding their content moderation practices; and delete copies of material that has been taken down.

NetzDG applies only to the largest platforms and only to certain content. Content is subject to the takedown only if it violates specific provisions of the German Criminal Code.[76] As for offences of incitement, most of the forbidden content is not related to elections or only tangentially so. The provisions of NetzDG most relevant to elections involve prohibitions on the "dissemination" of "propaganda materials" or symbols of banned political parties.[77]

The law was controversial and scrutinized around the globe from development to implementation.[78] Critics of the law argued that within Germany, it unduly infringed freedom of speech and would incentivize platforms to take an overly broad interpretation of their obligations and take down more content than was strictly necessary (Gorwa 2021). Looking abroad, critics of NetzDG feared that authoritarian governments around the world would enact similar, but even more restrictive, measures and use the German example as cover.

While the alleged "chilling effects" of the law do not appear to have materialized, neither have more grandiose claims that it would clean up the German internet and prevent foreign interference.

Conclusion

While the growth of online communication has brought many benefits, the harsh reality of the likelihood of foreign interference through the internet has compelled democracies to take action. Fears of foreign interference affecting the result of a domestic election spurred on by the controversies surrounding the 2016 US election cycle have generated a host of responses. Canada and Germany have taken different approaches to this problem.

Canada has a relatively strict regulatory approach to the key players in electoral politics. It has firmly limited the role of foreign money in politics. Partially due to the structure provided by the Charter of Rights and Freedoms, however, Canada has taken only tentative steps toward regulating social media platforms.

Germany has a less stringent set of electoral laws than Canada overall in terms of its regulation of donors, interest groups and so on. Yet, due to its history, Germany has taken a stricter regulatory approach to harmful speech post-Second World War. The early version of the postwar German model involved banning certain extreme political parties and criminalizing some forms of hate speech. With NetzDG, the updated model includes the banning of political parties, criminal sanctions for harmful speech, and notice and takedown requirements for large online platforms used to spread illegal content.

The attempts by both Canada and Germany to respond to the challenge of foreign interference in elections are likely to be, at best, partial successes. They should be seen as first steps on a longer journey. New platforms emerge regularly with different internal rules. User behaviour changes. In this constantly shifting communications environment, new methods and opportunities for interference in elections abound. Shifting global allegiances between states also muddy any attempt to clearly identify which state actors are potential threats.

[74] Ibid., s 25.

[75] *Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act),* 12 July 2017, (entered into force 1 October 2017).

[76] Ibid., s 1.

[77] *German Criminal Code (Strafgesetzbuch)* [*StGB*], ss 86, 86a. There are also provisions related to data forgery that might potentially be relevant, as well to incitement of violence.

[78] For a comparison of NetzDG with the American model, see Moon (2019).

In sum, Canada and Germany, within their own domestic constitutional and legal frameworks, have sought to respond to a dynamic problem. Given their distinct approaches, their successes and failures in dealing with foreign interference are likely to be scrutinized closely by other democracies. Foreign interference in elections is a global problem, and there is now an ongoing search for solutions.

Works Cited

CSE. 2017. *Cyber Threats to Canada's Democratic Process.* Ottawa, ON: CSE. https://cyber.gc.ca/sites/default/files/publications/cse-cyber-threat-assessment-e.pdf.

———. 2019. *2019 Update: Cyber Threats to Canada's Democratic Process.* Ottawa, ON: CSE. https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf.

———. 2021. *Cyber Threats to Canada's Democratic Process: July 2021 Update.* Ottawa, ON: CSE. https://cyber.gc.ca/sites/default/files/2021-07/threat-to-democratic-process-2021-3-web-e.pdf.

Dawood, Yasmin. 2021. "Combatting Foreign Election Interference: Canada's Electoral Ecosystem Approach to Disinformation and Cyber Threats." *Election Law Journal* 20 (1): 10–31.

Feasby, Colin. 1999. "Libman v. Quebec (A.G.) and the Administration of the Process of Democracy Under the Charter: The Emerging Egalitarian Model." *McGill Law Journal* 44 (1): 1339–44.

Gorwa, Robert. 2021. "Elections, institutions, and the regulatory politics of platform governance: The case of the German NetzDG." *Telecommunications Policy* 45 (6): 1–26.

He, Danya. 2020. "Governing Hate Content Online: How the *Rechtsstaat* Shaped the Policy Discourse on the NetzDG in Germany." *International Journal of Communication* 14: 3746–68.

Judge, Elizabeth and Amir Korhani. Forthcoming 2022. "Deepfakes, Disinformation, and Elections: A Moderate Proposal for a Digital Right of Reply for Election-Related Digital Replicas." In *Cyber-Threats to Canadian Democracy*, edited by Holly Ann Garnett and Michael Pal. Montreal, QC: McGill-Queen's University Press.

Karanicolas, Michael. 2019. "Subverting Democracy to Save Democracy: Canada's Extra-Constitutional Approaches to Battling 'Fake News.'" *Canadian Journal of Law and Technology* 17 (2): 200–25.

Levin, Dov H. 2020. *Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions.* New York, NY: Oxford University Press.

Moon, Laura E. 2019. "A New Role for Social Network Providers: NetzDG and the Communications Decency Act." *Transnational Law & Contemporary Problems* 29 (1): 611–33.

Pal, Michael. 2017. "Is the Permanent Campaign the End of the Egalitarian Model for Elections?" In *The Canadian Constitution in Transition,* edited by Richard Albert, Paul Daly and Vanessa MacDonnell, 338–64. Toronto, ON: University of Toronto Press.

———. 2018. "Evaluating Bill C-76: The Elections Modernization Act." *Journal of Parliamentary and Political Law* 13: 171.

———. 2020. "Social Media and Democracy: Challenges for Election Law and Administration in Canada." *Election Law Journal: Rules, Politics, and Policy* 19 (2): 200–13.

Ringhand, Lori A. 2021. "Foreign Election Interference: Comparative Approaches to a Global Challenge." *Election Law Journal: Rules, Politics, and Policy* 20 (1): 1–9.

DEM DEUTSCHEN VOLKE

Canadian National Security Approaches to Protecting Elections from Foreign Interference

Wesley Wark

Key Findings

→ While Canadian federal elections have not, to date, been affected to any serious degree by foreign interference operations, the Canadian government has nevertheless taken major steps since 2016 to understand the foreign election interference threat and to ready its electoral ecosystem to respond.

→ A number of Canadian initiatives are worthy of consideration by Germany and other democracies. These initiatives include the creation of the Critical Election Incident Public Protocol and the public issuance of a series of strategic threat assessments by CSE.

→ Canada has expanded its multilateral capacity to share intelligence and best practices on foreign electoral interference through the G7 RRM and the secretariat hosted by GAC. Strong cooperation between Canada and Germany on understanding and responding to foreign electoral interference can be maintained through the RRM. Linkages between CSE and the German BSI, which share similar cybersecurity mandates, would allow for greater bilateral cooperation.[79]

→ Canada continues to examine the best way forward to ensure that social media platforms are responsible partners in the electoral ecosystem. Exchanges between Canada and Germany on social media regulation and best practices would be valuable for both countries.

History: Canada Awakens to New Threats of Foreign Election Interference

Canadian governmental concern with heightened foreign interference in elections, using non-traditional methods such as cyber, was initially prompted by the experience of close allied partners in 2016, in particular, brazen Russian interference operations targeting the US presidential election and various forms of external interference in the "Brexit" referendum in the United Kingdom.

The first step taken was to mandate CSE, Canada's cryptologic agency responsible for both foreign signals intelligence and cybersecurity matters, to study the threat and report publicly (Office of the Prime Minister 2017). The first CSE (2017) threat assessment, *Cyber Threats to Canada's Democratic Process*, was released in June 2017. Two subsequent threat assessment reports have been released on a biannual basis. The findings of these public threat assessments are discussed below.

The Canadian government also proceeded to create an action plan, "The Plan to Protect Canadian Democracy," which was announced at a press conference with three ministers in January 2019 (Gould, Sajjan and Goodale 2019). The action plan focused on four objectives:

→ enhancing citizen awareness;

→ improving readiness on the part of the "electoral ecosystem" to contend with foreign interference efforts;

→ generating expectations for social media platforms to take action to combat disinformation; and

→ combatting foreign interference, including building strong awareness of threats in cooperation with foreign partners.

Most of the action plan was domestically focused, but Canada pursued some new multilateral initiatives to enhance its capacity to defend the democratic process and combat foreign interference during elections.

[79] The German BSI (Federal Office for Information Security) is a counterpart agency to CSE and its component Canadian Centre for Cyber Security. The BSI maintains a website at www.bsi.bund.de/EN/Topics/topics_node.html. While the BSI posts technical cybersecurity bulletins, it does not produce public cyberthreat assessments.

Multilateral systems were already in place to share analysis of election interference threats. These included close security cooperation with the United States, the NATO alliance and, especially, the Five Eyes intelligence relationship, which links Canada's security and intelligence community with counterparts in Australia, New Zealand, the United Kingdom and the United States.

To expand these networks of information sharing, Canada also hosted a G7 summit in the summer of 2018, which led to agreement on the establishment of an RRM as an early warning system to deal with electoral and democratic threats (G7 2018). A coordination unit was established within GAC to produce analysis and reports on threats, including trends, to be shared across G7 countries. Membership in the RRM has since been extended to several non-G7 nations, including Australia, Lithuania, the Netherlands and New Zealand.[80]

While Germany is not a member of the Five Eyes, cooperation on understanding electoral threats is made possible through our shared membership in NATO and the G7, as well as through close bilateral relations.

The Canadian action plan included the creation of new and novel mechanisms to respond to foreign electoral interference. Principal of these was the Critical Election Incident Public Protocol. According to James Judd (2020, 21), a retired senior official and former director of CSIS, who was mandated to produce a report on the functioning of the protocol following the 2019 general election: "The Protocol appears to have been a uniquely Canadian invention. There does not appear to be any equivalent body elsewhere in the world."

The Critical Election Incident Public Protocol and the SITE Task Force

The creation of the Critical Election Incident Public Protocol and the SITE Task Force was announced as part of the government's "Plan to Protect Canadian Democracy" in January 2019. This new system was first tested in a federal election in the fall of 2019 and was in operation again during the most recent federal election, which ran from August 16, 2021, to election day on September 20, 2021.

To date, the system has not faced a crisis situation with regard to foreign interference in a Canadian election, but its purpose is clear. This Canadian innovation was stimulated by reflections on the US experience during the 2016 elections. As Judd (ibid., 13), the independent evaluator of the protocol, wrote in his assessment: "In essence the creation of the Protocol and its Panel was intended to avoid a situation such as occurred in the 2016 US elections. There was a significant degree of foreign interference in the election that was not made known to voters before the election occurred. It was not made public for fear that such a revelation might be construed as having been done for partisan reasons."

The Canadian protocol is designed to take politics and partisanship out of any public warnings of significant foreign election interference. It does so through a multi-stage process involving:

→ intelligence gathering and verification;

→ adjudication of election interference threats by a panel of senior civil servants;

→ briefings to any affected political party, if not prevented by any "overriding" national security reasons;

→ determination of the necessity of a public announcement;

→ notification of the prime minister, other major party leaders and Elections Canada; and

→ issuance of a statement by the relevant security agency head.

[80] See www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/rrm-mrr.aspx?lang=eng.

The key elements of the protocol are its foundation in verifiable intelligence, the decision-making role of a panel of senior civil servants and a high threshold for determining the need for a public announcement.

The intelligence element is provided by the SITE Task Force, represented by four core national security agencies: CSE, CSIS, GAC and the RCMP.[81]

Intelligence is used to brief the panel of senior civil servants on election threats, supported by two secretariats within the Privy Council Office. The panel is comprised of:

→ the clerk of the Privy Council;

→ the national security and intelligence advisor to the prime minister;

→ the deputy minister of justice and deputy attorney general of Canada;

→ the deputy minister of foreign affairs; and

→ the deputy minister of public safety.

As the May 2020 report on the workings of the protocol noted, the senior official panel was engaged in extensive discussions on the nature of the "high threshold" required for any decision to make a public announcement (ibid., 18–19). The Cabinet directive that informs the protocol describes the threshold as involving three considerations:

→ the degree to which interference undermines a free and fair election;

→ the potential to undermine the credibility of the election; and

→ the degree of confidence officials have in the intelligence picture (ibid., Appendix 2, 26–29).

In essence, the protocol relies on the experience of the senior civil servants involved and their contextual judgment. The protocol requires wrestling with both a potentially large range of threat actors, as well as a diverse set of interference operations including cyberattacks on critical infrastructure relevant to the election ecosystem, cybertheft of data, disinformation campaigns mounted on social media and more traditional foreign interference actions. The independent report noted in particular the importance of paying heed to "the application of new technologies and operational methodologies" by perpetrators, as well as new defensive measures taken by potential target states from which lessons could be learned (ibid., 23).

Despite the protocol not being severely tested in the 2019 federal election, the independent report found that "on the whole the implementation of the Protocol has been successful" (Government of Canada 2020, 21). In making recommendations for the future, Judd argued that the protocol should be continued with its original structure, but that its time frame for operation should be extended to a pre-writ period so that it would be in operation constantly. Judd also recommended ongoing study of the action plan's engagement with social media platforms, which he noted was the most widely criticized element of the plan (ibid., 22–24).

The Judd report was also provided to the National Security and Intelligence Committee of Parliamentarians (NSICOP) for review in September 2020. NSICOP summarized its responses to the government in its 2020 annual report. It recommended some changes of approach including the inclusion on the protocol panel of "eminent Canadians" who, in the committee's view, might "carry more weight" than senior civil servants in the highly politicized context of a federal election. It also urged frequent engagement with political parties on the protocol's purpose. NSICOP also wanted further study of how exactly the protocol would inform Canadians of a serious incident of election interference, including attribution (NSICOP 2020, 4–5).

The attribution issue was not addressed in the original Cabinet directive and, of course, raises issues of national security confidentiality, as well as a role for political judgments about the potential impacts of attribution on foreign relations that could be beyond the "pay grade" of even senior civil servants.

The attribution challenge underscores the central role played by intelligence in the election protocol. Confidence in the intelligence picture is a key element of the working of the protocol and the determination of the seriousness of any election interference threat. Given the role that cyberthreat intelligence may play,

[81] See www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html.

it is important to understand the public cyberthreat assessments produced by CSE.

Cyberthreat Assessments

CSE has produced three public assessments dealing with cyberthreats to Canada's democratic process. The most recent was released in July 2021 in advance of the federal election.

These threat assessments represent a substantial effort to inform Canadians about the realities of foreign electoral interference. They have taken on the hard challenge of making predictive, but prudent, judgments. They face the difficult problem of warning, without being seen to cry wolf.

The first threat assessment was released on June 16, 2017 (CSE 2017). It noted an increasing trend line in cyberthreat activity over the past 10 years and predicted that it would continue to increase in quantity and sophistication in the future. It cited several reasons for this prediction, including easy access to cyber tools; the rapid growth of social media as a main form of news, displacing older mainstream media sources; the difficulty of deterring cyberactivity; and a "dynamic of success emboldening adversaries to repeat their activity, and to inspire copycat behaviour."[82] The assessment took a prudential stance on the question of the extent to which Canada was a likely future target, arguing that this would largely depend on how foreign adversaries perceive Canadian policies. Because of a paper-based voting system and other processing controls, CSE assessed that the election process itself was not a particularly vulnerable target, but that political parties and politicians, and the media, were.

The 2017 threat assessment did look ahead to the planned 2019 federal election and was prepared to predict that "almost certainly, multiple hacktivist groups will deploy cyber capabilities in an attempt to influence the democratic process in 2019" (ibid., 33). Such attempts were deemed, at most, to rise to medium sophistication levels (ibid.).

The 2019 publication of *Cyber Threats to Canada's Democratic Process*, released on April 5, 2019, acknowledged the creation of the public-facing Canadian Centre for Cyber Security. This update was released prior to the fall 2019 election, which resulted in a Liberal minority government.

The 2019 update again stressed the accelerating trend of election interference, indicating that in the previous year, "half of all advanced democracies holding national elections had their democratic process targeted by cyber threat activity" (CSE 2019, 5). CSE expected that trend to continue (ibid.).

CSE also judged it "very likely" that "Canadian voters will encounter some form of foreign cyber interference" related to the 2019 federal election (ibid., 21). This was in keeping with a view that cyberthreat activity was increasingly focused on voters. But it balanced this assessment with a statement that "foreign cyber interference of the scale of Russian activity against the 2016 United States presidential election" was "improbable at this time" (ibid.).

Examples of known cyber interference activities targeting Canada included manipulation of social media and efforts by foreign state-sponsored media to disparage Canadian politicians (ibid.). Whether the latter example truly fits into the frame of cyber election interference is questionable.

Efforts to spread false information on social media were Russian-based and included false stories about Canadian military operations in Ukraine, involving fake news about a failed Canadian military raid that allegedly killed 11 military personnel, and a false story about Canadian soldiers dying after their military vehicle hit a landmine in eastern Ukraine (ibid.).

Having placed their predictive thumb on an assessment of high likelihood (in CSE terms, in the range of more than 80 percent probability) of cyber interference during the 2019 federal election, CSE then had to recalibrate with its July 2021 update.

The most recent of the series of CSE public cyberthreat assessments found that the cyberthreat landscape had remained "relatively stable" since 2017 and no longer demonstrated a strong upward trend. The main target of such activity continued to be voters.

Commenting on the impact of COVID-19, CSE found that a move to remote working had enlarged the cyberattack surface, and that the pandemic provided significant opportunities for threat actors

[82] See https://cyber.gc.ca/en/guidance/executive-summary.

to engage in false political narratives that might decrease confidence in elections (CSE 2021, 3).

Despite the absence of known indicators of significant cyber interference in the 2019 federal election, CSE held to a prediction for Canadian impact that balanced concern about the high likelihood of “some form of foreign cyber interference” in a future election, against an assessment that Canada remained a “lower-priority target” for state-sponsored cyber actors (ibid., 33).

Since the closing of the most recent Canadian election writ period (voting day was September 20, 2021), there were no media reports of significant foreign cyber interference, nor was the Critical Election Incident Public Protocol activated to provide any public warning of serious interference.

The relative security of the Canadian electoral system, the fact that Canada appears to be a lower-priority target, a rising public and media consciousness about foreign cyber interference, and a more observant role by social media platforms may all have contributed to this, at least provisional, happy state of affairs.

CSE public threat assessments continue to inform and warn but have not yet generated any cry-wolf dynamic.

Conclusion

The Canadian system for responding to threats of foreign interference in elections is a recent creation, stimulated by the experience of Russian interference in the 2016 US presidential election.

It is based on a determination to provide public warnings of election interference, if necessary, predicated on the judgment of a panel of senior officials who are meant to act on strictly non-partisan grounds, supported by a verifiable intelligence picture.

The Canadian approach accepts that the “attack surface” for foreign interference in elections is large and may combine both traditional and new technologically driven elements.

By insisting on a “high threshold” for public warnings of election interference, the Canadian system is alert to the need to avoid engagement in the electoral process, short of a crisis situation.

Supporting the intent of the system, there is a recognition of the need for enhanced public awareness of the nature of cyberthreats to the electoral process. CSE has met this need through a series of public threat assessments released every two years since 2017.

The Canadian government also recognizes the universality of foreign interference threats to democratic elections, has set up a new G7 mechanism to monitor such threats, and will look to allies and partners for information and best practice exchanges. In keeping with this approach, applying a Canada-Germany bilateral lens to election interference would be beneficial for both countries. Germany has experienced more significant forms of foreign election interference than has Canada to date (Morris 2021; Sugue 2021; Stelzenmüller 2017).[83] Canada has had the “luxury” of learning from others and building an innovative response system prior to the onset of a crisis. Adoption of some elements of the Canadian system by Germany might be advantageous, as would close and ongoing engagement between the two countries in a study of trends in foreign democratic interference.

[83] See https://securingdemocracy.gmfus.org/2021-german-elections/.

Works Cited

CSE. 2017. *Cyber Threats to Canada's Democratic Process.* Ottawa, ON: CSE. https://publications.gc.ca/collections/collection_2017/cstc-csec/D96-2-2017-eng.pdf.

———. 2019. *2019 Update: Cyber Threats to Canada's Democratic Process.* Ottawa, ON: CSE. https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf.

———. 2021. *Cyber Threats to Canada's Democratic Process: July 2021 Update.* Ottawa, ON: CSE. https://cyber.gc.ca/sites/default/files/2021-07/threat-to-democratic-process-2021-3-web-e.pdf.

G7. 2018. "The Charlevoix G7 Summit Communique." June 9. www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2018-06-09-summit-communique-sommet.aspx?lang=eng.

Gould, Karina, Harjit S. Sajjan and Ralph Goodale. 2019. "The Government of Canada's Plan to Safeguard Canada's 2019 Election." Speech delivered at National Presse Theatre, Ottawa, ON, January 30. www.canada.ca/en/democratic-institutions/news/2019/03/speech-thegovernment-of-canadas-plan-to-safeguard-canadas-2019-election.html.

Government of Canada. 2020. *Report on the Assessment of the Critical Election Incident Public Protocol.* May. www.canada.ca/content/dam/di-id/documents/ceipp-eng.pdf.

Judd, James. 2020. *Report on the Assessment of the Critical Election Incident Public Protocol.* www.canada.ca/en/democratic-institutions/services/reports/report-assessment-critical-election-incident-public-protocol.html.

Morris, Loveday. 2021. "Germany complains to Moscow over pre-election phishing attacks on politicians." *The Washington Post,* September 6. www.washingtonpost.com/world/germany-russia-cyber-attack/2021/09/06/7b9ca734-0f28-11ec-baca-86b144fc8a2d_story.html.

NSICOP. 2020. *Annual Report 2020.* Ottawa, ON: NSICOP. www.nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/annual_report_2020_public_en.pdf.

Office of the Prime Minister. 2017. "Minister of Democratic Institutions Mandate Letter." Office of the Prime Minister, February 1. https://pm.gc.ca/en/mandate-letters/2017/02/01/archived-minister-democratic-institutions-mandate-letter.

Stelzenmüller, Constanze. 2017. "The impact of Russian interference on Germany's 2017 elections." Brookings, June 28. www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

Sugue, Merlin. 2021. "Schäuble warns of foreign interference in German election." Politico, June 26. www.politico.eu/article/schauble-warns-of-foreign-interference-in-german-elections/.

yber at
the

Experts

CIGI has convened a knowledge-sharing network that is multidisciplinary in nature. This network has served as a collaborative space to facilitate expert views, opinions and recommendations to formulate an impactful report for key government and civil society stakeholders.

The following list of experts is indicative of those who have contributed to the development of this report and the subsequent engagement events that will follow upon the release of this publication.

Samantha Bradshaw is a postdoctoral research fellow at Stanford University, where she works at the Internet Observatory and the Digital Civil Society Lab. Samantha is a leading expert on technology and democracy. Her dissertation research examined the producers and drivers of disinformation, and how technology (artificial intelligence, automation and big data analytics) enhance and constrain the spread of disinformation online. At the forefront of theoretical and methodological approaches for studying, analyzing and explicating the complex relationship between social media and democracy, Samantha's research has helped advance academic debate, public understanding and policy discussions around the impact of technology on political expression and privacy.

Kailee Hilt is a research associate at CIGI, where her primary responsibilities involve contributing to the planning and execution of research output. She also provides research support and analysis on issues related to emerging technology, data governance, cybersecurity and online gender-based violence.

Eric Jardine is a CIGI fellow and an assistant professor of political science at Virginia Tech. He researches the uses and abuses of the dark web, measuring trends in cybersecurity, how people adapt to changing risk perceptions when using new security technologies, and the politics surrounding anonymity-granting technologies and encryption. Eric was a contributor to *Governing Cyberspace during a Crisis in Trust*, an essay series on the economic potential — and vulnerability — of transformative technologies and cybersecurity.

Florian Kerschbaum is associate professor in the Cheriton School of Computer Science at the University of Waterloo and director of the Waterloo Cybersecurity and Privacy Institute. Florian's interests lie in data security and privacy in data management, machine learning and blockchains. He extended real-world systems with cryptographic security mechanisms to achieve (some) provable security guarantees. His work has been applied to products for databases, supply chain management and radio frequency identification tracking.

Ulrike Klinger is the chair for digital democracy at the European New School of Digital Studies in Frankfurt, Germany, and an associated researcher at the Weizenbaum Institute for the Networked Society in Berlin, Germany. Ulrike's research focuses on political and digital communication: the transformation of digital public spheres, the role of digital media in election campaigns and the impact of technologies on public communication (for example, algorithms, social bots).

Michael Pal is associate professor in the Faculty of Law at the University of Ottawa and director of the Public Law Group. Michael is an expert on the law of democracy, comparative constitutional law and election law. He is currently working on projects related to voter suppression, electoral management bodies, election administration in democratic transitions and democratic theory. In 2017, he served as a commissioner with the Far North Electoral Boundaries Commission for the Province of Ontario, whose recommendations to add two new seats and to create the province's first Indigenous-majority riding and second Francophone-majority riding were adopted by the Legislative Assembly of Ontario.

Aaron Shull is managing director and general counsel at CIGI, where he acts as a strategic liaison between CIGI's research initiatives and other departments while managing CIGI's legal affairs and advising senior management on a range of legal, operational and policy matters. He has substantive expertise in international law, global security and internet governance. Aaron coordinated two CIGI essay series: *Security, Intelligence and the Global Health Crisis* and *Modern Conflict and Artificial Intelligence*.

Wesley Wark is a CIGI senior fellow and adjunct professor at the University of Ottawa's Centre on Public Management and Policy. Wesley recently retired from the University of Toronto's Munk School of Global Affairs and Public Policy, where he had taught since 1988. He served two terms on the prime minister of Canada's Advisory Council on National Security (2005–2009) and on the Advisory Committee to the President of the Canada Border Services Agency (2006–2010). More recently, he provided advice to the minister of public safety on national security legislation and policy. He has appeared on numerous occasions before parliamentary committees and comments regularly for the media on national security issues. Wesley was also an editor for the 2020 CIGI digital essay series titled *Security, Intelligence and the Global Health Crisis*. He is a former editor of the journal *Intelligence and National Security* and now serves on the journal's advisory board.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org