BRIEFING PAPER No. 6

ATLANTIK-BRÜCKE
CANADA

Foreign Information Manipulation and Interference: Priorities for Canada and Germany

Dr. Jean-Christophe Boucher
Associate Professor
University of Calgary

TABLE OF CONTENTS

ABOUT THE AUTHOR

Jean-Christophe Boucher is an Associate Professor at the School of Public Policy and the Department of Political Science at the University of Calgary. His current work focuses on applied machine learning to understand how the digital world shapes society. He is a Fulbright Scholar and is currently responsible for projects funded by the Social Science and Humanities Research Council (SSHRC) to understand civil-military relations in Canada; Heritage Canada to study Chinese information manipulation.

He holds a BA in History from the University of Ottawa, an MA in Philosophy from the Université de Montréal and a Ph.D. in Political Science from Université Laval. He specializes in international relations, emphasizing foreign policy, international security, and data analytics.

EXECUTIVE SUMMARY

The threat of foreign information manipulation and interference (FIMI) poses a severe risk to the political and economic stability of democracies worldwide. As highlighted in the World Economic Forum's Global Risk Report, AI-driven misinformation campaigns have emerged as the biggest short-term challenge, necessitating a proactive and comprehensive response strategy. Despite recognizing FIMI as a national security threat and establishing initiatives like the G7 Rapid Response Mechanism (RRM), democratic nations have struggled to counter the sophisticated tactics employed by state and non-state actors effectively. The immense scale, coordination, and disruptive innovation characterizing these campaigns have overwhelmed existing reactive measures, leaving democracies in a perpetual state of catch-up.

This paper proposes conceptualizing FIMI as a "crime of opportunity" to develop a more proactive defence framework. Drawing from criminological theories, it suggests that FIMI entrepreneurs exploit perceived vulnerabilities in a target's information ecosystem when the expected benefits outweigh operational costs and the likelihood of sanctions. Reframing FIMI through this lens, defensive strategies can disrupt the perceived opportunity structure rather than solely reacting to consummated offences. Rather than perpetually reacting to consummated offences, democracies should pursue "opportunity reduction" strategies that introduce strategic frictions at multiple vectors, impeding FIMI forces' abilities to rationalize reliable infrastructure access, dissemination conduits, and audience exploitation. This proactive, pre-emptive paradigm shift is crucial for enhancing democratic resilience against the severe, existential threat FIMI poses to political stability and human rights worldwide.

Drawing from our opportunity framework, the paper identifies three crucial conditions that enable FIMI operations: motivated offenders, suitable targets, and a lack of capable guardians. First, the paper examines four prominent actors posing significant FIMI threats: Russia, China, Iran and its proxies, and the far-right. Each actor employs distinct tactics and narratives tailored to specific audiences, aiming to undermine democratic institutions, sow societal discord, and advance their respective geopolitical agendas.

Second, regarding suitable targets, recent research findings highlight socioeconomic factors, educational backgrounds, and regional influences that contribute to varying degrees of vulnerability to misinformation across the Canadian population. Third, the absence of well-resourced dedicated institutions, comprehensive regulations, robust state capacity for detection, and limited civil society capacity to respond has created a permissive environment conducive to FIMI activities. This gap in governance and enforcement has enabled foreign actors to exploit digital vulnerabilities with relative impunity.

To address these challenges, the paper recommends a three-pronged strategy:

- Enhancing detection and response capabilities through better resource allocation and technology adoption.
- Strengthening international collaborations to ensure a unified and robust response to transcendent FIMI threats.
- Implementing pre-bunking strategies to build societal resilience against misinformation before it can take hold, with a focus on counter-narratives targeting the most vulnerable populations.

By conceptualizing FIMI as a crime of opportunity and implementing a proactive, multifaceted approach involving enhanced regulatory frameworks, dedicated institutions, and international cooperation, democracies can bolster their defences against the pervasive influence of foreign information manipulation. Preserving the integrity of democratic processes hinges on effectively mitigating the risks posed by FIMI and safeguarding the public from the corrosive effects of misinformation and disinformation.

INTRODUCTION

This year’s World Economic Forum's Global Risk Report identified artificial intelligence-driven misinformation and disinformation as the biggest short-term threat, posing risks to the political and economic stability of democracies, especially as key elections approach. With Canada's most recent public inquiry into election meddling by nation-state actors such as India, China, and Russia (Canada, 2024) alongside the upcoming European Parliament elections, policymakers in democratic countries focus on strategies to counter foreign interference and safeguard elections. This paper explores the intersection of technology, democracy, and security to illuminate real-world implications and offer perspectives on navigating the challenges of foreign information manipulation and interference in a globalized digital world.

During the G7 summit held in Charlevoix, Canada, in 2018, member states recognized foreign information manipulation and interference (FIMI) as a national security threat and pledged to address this escalating concern. As such, they formed the G7-appropriately-termed Rapid Response Mechanism (RRM). The RRM was mandated to “strengthen coordination to prevent, thwart and respond to malign and evolving threats to G7 democracies.” Furthermore, the RRM would “share information and threat analysis related to various threats to democracy, and is an established mechanism to identify opportunities for coordinated response” (Canada, 2019).

Unfortunately, despite ample empirical evidence of foreign state and non-state actors actively manipulating the information landscape to shape attitudes and behaviours of Western audiences while undermining democratic institutions worldwide, our ability to counter such manipulation has been neither swift nor effective. Indeed, as the COVID-19 pandemic (INFODEMIC), Russian aggression in Ukraine, China's election meddling in Western countries, Hamas and Iranian social media and information campaigns following the October 7, 2023, terrorist attack, or far-right global offensive against liberal values, foreign state and non-state actors’ interference in the information environment has met little resistance.

Western states recognize that much more needs to be done. Just recently, the United States, the United Kingdom, and Canada felt the urgency to reiterate their commitment, noting that “foreign information manipulation is a national security threat that undermines democratic values, human rights, governmental processes, and political stability.” (United State, 2024).

In this brief policy note, I shall explore the specific challenges that democracies encounter when formulating strategic responses to foreign manipulation and interference in information. Despite signing the RRM declaration more than seven years ago, we must admit that democratic nations, notably Canada and Germany, are still primarily reactive and have generally failed to build a comprehensive mechanism to address FIMI. Jumping from one crisis to the next, democracies can barely catch their breath, caught in an endless whack-a-mole enterprise. How can we move from such a reactive posture to building a response mechanism to increase our resiliency toward FIMI? How can democratic societies effectively optimize resource allocation to address and deter foreign interference? The crux of the matter rests in the complexity of discerning the specific issues, approaches, audiences, and moments suitable for proactive debunking interventions to respond to FIMI. We suggest it is helpful to conceptualize foreign information manipulation and interference as a *crime of opportunity.* By reframing FIMI in this context, through the prism of a comprehensive policy response framework, we might better understand its opportunistic nature and design proactive rather than merely reactive strategies.

Intractable nature of FIMI

At the core of the immense challenge in countering foreign information manipulation and interference (FIMI) campaigns lies the prodigious scale and highly coordinated nature by which state and non-state-backed actors can deploy these efforts. Leveraging formidable resources, FIMI architects strategically seed complementary disinformation narratives across many platforms and online communities (Bradshaw and Howard 2019; Batzdorfer et al. 2022). This multi- platform dispersion pursuit enables invasive entrenchment into the discursive environments of target societies before defensive actions can be mobilized. Facilitating this permeation is the novel implementation of automated botnet armies and cyber troop infrastructures (Stukal et al. 2022; Stukal et al., 2017). Such innovation obfuscates the true provenance of FIMI operations while manufacturing artificial amplification to achieve narrative saturation at unprecedented velocity and volume. The resulting manufactured engagement injects distortions that corrode public discourses and erode the coherence of the truth (Wanless and Pamment 2019).

Moreover, foreign actors exploit ideological divisions across online communities and thus strategically tailor their disinformation campaigns to fit different demographic and interest-based audiences (Bastos and Farkas 2019; Starbird et al. 2019). Malign actors covertly pursue unified narrative proliferation and discursive dominance across platforms by targeting these disparate online communities. These attempts to manipulate public opinion transcend siloed national jurisdictions and conventional defence frameworks (Stricot 2022). Their scale and hyper-coordinated execution make developing a comprehensive response strategy extremely difficult. Response resources are immediately overextended, while FIMI forces rapidly modify vector selection to bypass countermeasures. Persistent tactical innovations continually outpace defensive adaptations, consigning stalwart agencies to perpetual reactive triage against evolving incursions into the modern information ecosystem.

The cyclical emergence and normalization of disruptive FIMI tactics and technologies deepen this defensive predicament. Malign actors continually develop novel rhetorical strategies, synthetic media manipulations, and evolving information warfare techniques to circumvent existing institutional

safeguards (Tucker et al. 2022; Szostek 2018). The creeping ubiquity of generative AI capabilities like deepfakes destabilizes traditional verification markers, fluidly manufacturing believable falsehoods (Chesney and Citron 2019). For example, during the last Slovakian election in 2023, a disinformation operation used a deepfake to inculpate Michal Šimečka, the leader of the Liberal Progressive Slovakia, in election manipulation. Because the deepfake was in audio format, it bypassed Meta's manipulated-media policy circumscribed to deepfake video only (Meaker, 2023). FIMI forces readily leverage these innovations before regulatory paradigms can be adequately established. Ingrained defence models are rapidly outdated and unable to respond to the scale, range, and technological evolution. This rapid obsolescence imposes severe strategic handicaps. Extant countermeasures are persistently gamed as FIMI entrepreneurs iteratively deploy cyber-enabled tactics like bot herding, narrative camouflaging, meme indoctrination, and hyper-personalized microtargeting (Krafft and Donovan 2020; Ribeiro et al. 2019). Threat detection and mitigation capabilities cannot scale seamlessly against these ceaseless permutations in generative media manipulations and computational propaganda arsenals.

Furthermore, the most pernicious FIMI strategies defy tidy categorization by blurring the boundaries between truth and fiction (Park et al. 2023). Malign actors increasingly seed legit fragments of factual information into larger disinformation payloads. This erosion of verifiable grounding truth exacerbates the psychological influence of visceral, emotionally charged narratives designed to incite extreme reactions. Collectively, this cyclical onslaught of disruptive innovations by FIMI forces imposes immense defensive resourcing and operational debt. Mitigation requires reactive response protocols and proactive threat modelling to pre-empt offensive vanguards. As FIMI tactics reshape battlefield geometries, successful defence mandates predictive adaptation - an immense strategic and financial burden for democratic institutions perpetually reconstituting safeguards.

The reactive stance of democracies towards foreign interference presents a formidable challenge. Frequently caught in a cycle of responding to incidents rather than preemptively addressing underlying vulnerabilities, democracies struggle to effectively combat the multifaceted threats posed by foreign state

and non-state actors. This reactive approach needs to be revised when relying on fact-checking mechanisms, which, while valuable, often fail to counter information manipulation and its effects on targeted audiences successfully. Moreover, the limited allocation of resources towards reactive measures further compounds the issue, leaving democratic societies ill-equipped to tackle the evolving landscape of information warfare. Without a shift towards proactive strategies prioritizing resilience-building and comprehensive defence mechanisms, democracies remain vulnerable to manipulation and interference from external actors seeking to undermine their integrity and stability. Thus, a pressing need exists for democracies to reevaluate their approaches, allocating resources towards pre-bunking measures to effectively confront the challenges of foreign interference.

This new approach will entail identifying vulnerabilities and implementing measures to bolster defences and mitigate risks effectively. Through such a structured framework, policymakers can enhance the resilience of democratic societies against the ever-evolving tactics employed by malign actors seeking to undermine their integrity. Moreover, by recognizing FIMI as a crime of opportunity, we acknowledge the need for continuous vigilance and adaptability in our response strategies, ensuring they remain robust and effective in safeguarding against external threats.

FIMI as a crime of opportunity

We propose a simple organizing principle to ensure state preparedness for FIMI. Given the immense scale, coordination, and disruptive innovation adversaries deploy in foreign information manipulation and interference (FIMI) campaigns, a radical shift towards more proactive defence paradigms is imperative. Borrowing from criminology, the solution may lie with a response mechanism inspired by the Routine Activity Theory (RAT). Initially proposed by Cohen and Felson in 1979, Routine Activity Theory suggests that three conditions are conducive to a criminal opportunity: a motivated offender, a suitable target, and the absence of capable guardians. Actors rationally weigh perceived costs, benefits, and opportunities when contemplating unlawful conduct (Cornish and Clarke 1986; Felson and Clarke 1998); in other words, they perform a calculation balancing motivations, potential payoffs, and mitigating risks in choosing to perpetrate offences.

While frequently applied to physical crimes like burglary or robbery, rational choice constructs are relevant for cyber-enabled threat modelling like FIMI (Guerra and Ingram 2022; Maimon et al. 2023). FIMI entrepreneurs exploit perceived vulnerabilities in a target's information ecosystem as a fundamentally opportunistic enterprise in which expected benefits outweigh operational costs and the likelihood of sanction (Fridman et al. 2019). Malign actors evaluate anticipated gains, potential consequences of being caught, probable penalties, and other potential options in the information domain (Leukfeldt and Kleemans 2019). Through this framing, defending institutions could implement strategies to disrupt FIMI forces' perceived opportunity structure rather than perpetually scaling reactive mitigations against consummated offences. Derived from routine activity theory, such “opportunity reduction” aims to increase the real and perceived risks and costs of FIMI operations while minimizing anticipated rewards (Cohen and Felson 1979; Wortley and Mazzerole 2011). By introducing strategic frictions at multiple vectors, defensive efforts can impede FIMI entrepreneurs' ability to rationalize targeting reliable infrastructure, content dissemination channels, and potential constituencies (Borrion 2013).

An essential dimension involves adding more friction in the planning and execution phases of FIMI operations from foreign actors. Democracies must increase the real and perceived costs associated with organizing activities like narrative prototyping, influencer recruitment, audience curation, infrastructure acquisition, and funding resource allocation. In short, we need to make FIMI less attractive and more resource-intensive for state and non-state actors.

On the one hand, we should focus on complexifying and hardening the environment mechanism to increase FIMI offenders' appraisal of risks and investments required to launch successful campaigns. For example, we should make defensive investments in environmental fortifications like regulation and platform content moderation to erode FIMI forces' assessments of reliable dissemination avenues and anticipated audience reception (Maimon et al., 2023; Leukfeldt and Kleemans, 2019). Effective “reward reduction” also involves raising FIMI actors' perceived probabilities of sanctions and material losses through proactively targeting illicit finance streams and combatting jurisdictional arbitrage (Wortley and Mazzerole 2011). In tandem, defensive strategies should target FIMI entrepreneurs' anticipated reward structures to nullify perceptions of benefits and incentives. Normalizing public resilience against manipulated narratives through education, media literacy, and verified information-sharing partnerships could reduce FIMI groups' assessments of achievable legitimacy acquisitions and discursive dominance objectives (Gorwa 2019). We are thus proposing a paradigm shift towards opportunity reduction, allowing democracies to wrest strategic initiative and force FIMI actors into defensive postures (Clarke and Eck 2003). Instead of treating FIMI as an inevitability, democratic interventions should proactively erode FIMI entrepreneurs' capacity to succeed.

Motivated offenders, foreign threats, and FIMI

Across the democratic world, various state and non-state actors attempt to shape the information space to advance their respective interests and objectives. These actors are highly motivated and invest significant resources—in the billions of

dollars range—to sway the attitudes and behaviours of our domestic audiences. In this paper, we will briefly focus our attention on four different actors who pose the most pressing challenge to democracies: Russia, China, Iran and its proxies, and the far right.

Russia

First, Russia has emerged as a strategic actor adeptly wielding influence operations to advance its objectives on multiple fronts. At the strategic level, Russia seeks to reshape the geopolitical landscape in the long term by confronting and undermining Western nations, particularly the United States and its allies. A core Russian aim is to sow division within the NATO alliance by inflaming tensions and mistrust among member states. Russia hopes to reassert its global dominance and Soviet-era sphere of influence by chipping away at this powerful military coalition.

At an operational level, Russia's information warfare targets Western liberal democracies themselves. By amplifying illiberal rhetoric, conspiracy theories, and polarizing narratives, Russia foments social unrest and deepens existing divides along racial, political, and socioeconomic lines. This calculated stoking of discord and mistrust aims to undermine public confidence in democratic institutions, electoral processes, and objective truth. Tactically, Russia also leverages the information space to support its military campaigns, such as the ongoing invasion of Ukraine, by saturating audiences with pro-Russian disinformation. Much of Russia’s strategic communication, although sometimes appearing chaotic, nevertheless has an underlying structure and consistently seeks to promote these three categories of objectives.

In conducting these objectives, Russia targets audiences across the ideological spectrum. Russia's insidious information operations have been particularly pernicious in infiltrating and exploiting mainstream media channels and leveraging the immense reach of social media platforms to target and engage Western audiences effectively. On the far right, Russia provides direct support and amplification to fringe influencers and groups peddling racism,

xenophobia, authoritarianism, and anti-democratic ideals. By injecting their narratives into mainstream discourse and activating existing societal grievances, they hope to accelerate a civilizational shift away from liberal democratic values. Conversely, Russia also sponsors far-left groups, particularly those espousing anti-capitalism, anti-globalization, and strident anti-Americanism. Despite their ideological gulf with the far-right, these groups share Russia's hostility toward the liberal world order. By fueling extremism at both ends, Russia sows societal chaos and paralyzes effective responses to its geopolitical revisionism. It is noteworthy that Russia exploits domestic fault lines in our democracies, thus showing a deep knowledge of audiences and shaping its information operations accordingly.

With a sophisticated blend of overt and covert tactics, Russian state actors have adeptly hijacked reputable news outlets through coordinated influence campaigns, planted Kremlin-aligned pundits and narratives, and flooded editorial spaces with pro-Russian disinformation. However, the potency of Russia's information warfare lies in its masterful harnessing of social media's unprecedented scale and specificity. By unleashing sweeping bot armies and troll farms across platforms like Telegram, Meta, Twitter/X, YouTube and more, Russian operatives deluge the modern information ecosystem with targeted disinformation tailored to individual users' existing beliefs, biases and vulnerabilities. These pernicious influence operations do not just broadcast falsehoods - they micro-target audiences with emotionally- resonant narratives designed to erode trust in democratic institutions. Russia's skillful manipulation of social media's connectivity and algorithmic content curation has allowed it to bypass and undermine traditional gatekeepers while directly shaping the online realities of millions. Its deft fusion of legitimate and artificial amplifiers creates an illusory mainstream consensus around Kremlin interests. This malign influence, optimized through data analytics and AI assistance, presents an existential hazard to the integrity of the open internet and our increasingly digitized social fabrics.

In Canada, early research in June 2022 showed that Russian propaganda had infiltrated the far-right and far-left online ecosystem, with significant Canadian influencers promoting the Russian narrative on the Ukraine war (Boucher et al. 2022).

In Germany specifically, there have been multiple allegations that far-right groups, and specifically the AfD, have become a tool of Russian information operations seeking to undermine Germany's support to Ukraine, thus conflating further the impact of far-right groups on the information space (Solomon, 2024).

China

China has emerged as a potent purveyor of foreign information manipulation aimed at reshaping the global order to suit its authoritarian interests. At the strategic level, China seeks to undermine the Western-led rules-based international system and the liberal norms that underpin it. Beijing's long-term vision is to position itself as the preeminent world power, replacing the U.S.-led order with one more amenable to its dictatorial governance model and territorial ambitions.

Operationally, China has been accused of covertly meddling in elections across the democratic world. By amplifying the messaging and covert funding of politicians, parties, and operatives, which are seen as sympathetic or less confrontational to Beijing's interests, China attempts to tilt the political playing field in its favour. On a tactical level, China employs comprehensive influence campaigns to gaslight global audiences on issues like its internment of Uyghurs in Xinjiang, its crackdown on democracy in Hong Kong, and its existential claims over Taiwan. Deploying orchestrated armies of bots and trolls, China floods the information space with its narratives while suppressing criticism and dissent.

A core pillar of China's foreign influence operations involves the covert mobilization or transnational repression of diaspora communities in Western nations. Under the guise of promoting cultural outreach, Beijing's United Front Work Department has established thousands of overseas Chinese diaspora groups that can be leveraged to amplify Chinese Communist Party messaging, suppress regime critics, influence policy debates, and gather intelligence. Many of these efforts target universities and student groups. By co-opting diaspora

elites and community leaders, China creates pervasive human sensor networks to subtly influence host societies in line with Beijing's strategic aims. Combining this exploitation of ethnic ties with comprehensive state control over digital platforms and information flows, China has constructed formidable machinery to manipulate the global information environment. In this context, it's notable that Chinese influence operations significantly emphasize leveraging the idiosyncratic information ecosystem within diasporic communities. These efforts predominantly target platforms tailored for these audiences, including but not limited to Chinese-language media outlets and messaging applications such as Weibo and WeChat.

Iran and its proxies

Iran's information operations have exhibited a strategic focus on engaging Iranian diasporic communities, particularly emphasizing their vulnerability to transnational repression tactics. Iran seeks to maintain influence over these communities through various channels, using platforms catering to their cultural and linguistic needs. By nurturing ties with diasporic populations, Iran aims to extend its reach beyond national borders, fostering loyalty and solidarity among expatriates while also exerting control over dissenting voices.

Furthermore, in the aftermath of the October 7th terrorist attack by Hamas in Israel, Iran has been proactive in sponsoring or amplifying information operations conducted by proxies such as Hamas and Hezbollah, which have significantly contributed to the proliferation of antisemitic rhetoric and sentiments. By supporting these militant groups, Iran not only bolsters its regional influence but also advances its broader geopolitical objectives, often at the expense of stability and security in the Middle East. Through financial support, training, and media amplification, Iran has played a pivotal role in shaping the discourse surrounding Israel and the Jewish community, fueling so-called “anti-Zionist” narratives and fostering a climate of hostility. This active involvement underscores Iran's willingness to exploit information warfare as a tool for advancing its ideological agenda and destabilizing its adversaries.

Far right

The proliferation of information manipulation orchestrated by foreign far-right entities poses a significant security threat to democratic nations. In countries like Canada and Germany, these groups have expanded their influence to the extent that they now represent formidable domestic political entities. With a well-established global network comprising political parties, financiers, and influential figures, far-right factions actively engage in moulding the information sphere to propagate populist, xenophobic, and illiberal ideologies. Their support extends beyond national borders, as foreign actors actively back domestic groups, blurring the distinction between domestic and international information ecosystems. This concerted effort undermines trust in democratic institutions by incessantly targeting governmental bodies, mainstream media outlets, the judicial system, and experts, thereby eroding the foundations of democracy. Additionally, their agenda aims to subvert democratic principles of pluralism and tolerance by promoting anti-immigrant, anti-LGBTQ, and misogynistic narratives. Moreover, the far right has cultivated an aggressive and toxic online environment where disinformation runs rampant and dissenting voices are systematically silenced.

In Canada, for example, the Freedom Convoy movement emerged as a manifestation of transnational populism, showcasing how the global far-right leveraged digital platforms to voice antigovernment and antidemocratic sentiments. Online discourse framed the movement as a battle for the preservation of a threatened political order, portraying participants, including truckers, anti-vaccine activists, and far-right adherents, as defenders against domestic and global tyranny. Influential figures like Ezra Levant, Jack Posobiec or Tucker Carlson acted as online ambassadors, disseminating dystopian far-right perspectives through platforms like Twitter/X. The movement's resonance extended beyond national borders, drawing support from diverse groups worldwide, including Brexit supporters, MAGA followers, white supremacists, conspiracy theorists, and anti-vaxxers, all converging in solidarity with the Canadian protest.

In Germany, the rise of the far-right movement and the normalization of its movement through the AfD have become central themes of foreign information manipulation. The AfD is part of a global far-right coalition keen on sharing resources, strategies, and narratives. Research has shown that the AfD has been keen on borrowing communication campaigns from Austrian white supremacist groups and has been effective in normalizing illiberal values and intolerance toward immigrants and members of the LGBTQ+ community (Klinger et al., 2023).

Suitable target and FIMI

For foreign malign states or non-states to perceive information manipulation and interference as worthwhile activities to advance their interests, there needs to be a target, a vulnerable audience. A considerable risk exists for mis/disinformation to polarize societies along sociodemographic and ideological fault lines, affecting social cohesion. While both allies and adversaries might employ coordinated targeted messaging for political gain, not all societal members are equally susceptible to nefarious messaging nor equally resilient to its influence. Identifying the factors that heighten individuals' susceptibility is crucial for understanding which segments of society are most vulnerable to influence operations. This allows for designing policies and strategies to improve societal resilience, especially for higher-risk populations with greater needs (Shi & Stevens, 2021).

However, this risk factor fluctuates across subpopulations with unequal vulnerability to mis/disinformation - indicating the issue is structural, not merely individual deficiency. Addressing misinformation and disinformation requires a comprehensive understanding of the sociodemographic factors contributing to vulnerability. Akin to epidemiology, susceptibility to misinformation and disinformation can be conceptualized as a risk factor - the likelihood of an individual becoming misinformed over a given period. All people are inherently at some risk, as our knowledge is inevitably bounded by incomplete information and cognitive biases. Research shows that most individuals are generally uninformed, have limited knowledge of most topics, and need help to evaluate source credibility (Lewandowsky et al., 2012). This makes people vulnerable to astroturfing efforts to sway opinion and deliberate

influence operations aiming to shape public preferences and behaviours (Cho et al. 2011). Once individuals believe misinformation, they have difficulty updating their attitudes and beliefs when presented with contradictory evidence (Chan et al., 2017; Ecker et al., 2022).

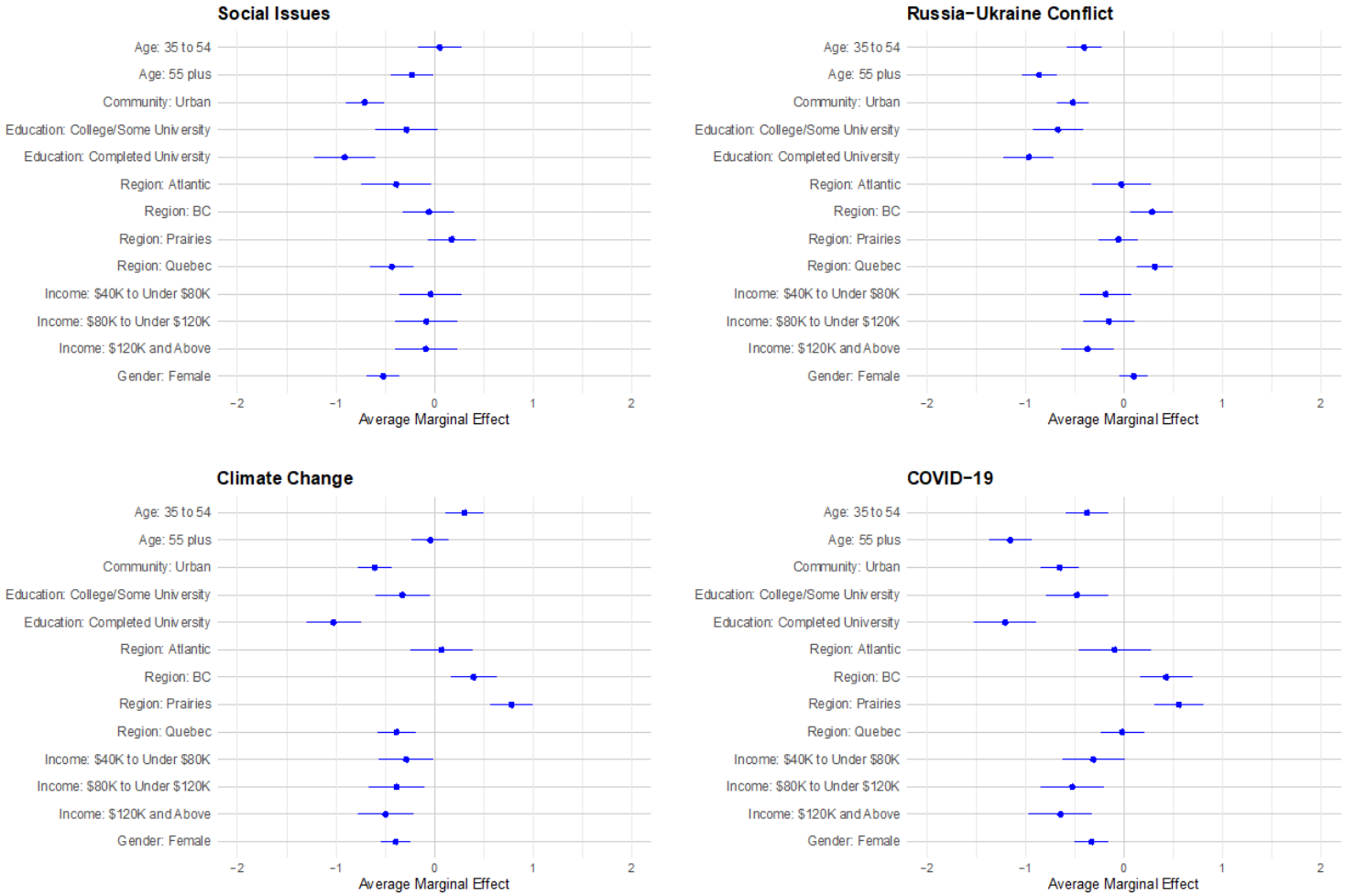
In 2022, our research team at the University of Calgary conducted a population-level survey in 2022 to look at Canadians' relative vulnerability to mis/disinformation, focusing on four topics: COVID-19, Climate change, the Russian- Ukrainian war, and social issues[1] (Boucher et al. forthcoming). To measure the extent to which an individual was misinformed, we designed a series of 15 statements. Respondents indicated the accuracy of a message on a scale from 0 (very inaccurate) to 10 (very accurate). First, and to our surprise, we found that answers to the 15 questions were highly correlated. This implies that vulnerability to misinformation is structural and might have little to do with an individual's knowledge of a particular issue. Technically, if a respondent had difficulty assessing the accuracy of the first misinformation statement – which was randomized for each respondent within and across topics when we conducted our survey – the odds were very high that they would also get the 14 following questions wrong. Our measures of uniformity indicate some internal consistency across all these statements. Put simply, if misinformation is a structural problem, or in other words, a vulnerability, the proactive correction of inaccurate information (fact-checking) may not be an effective strategy for combating misinformation and disinformation.

Overall, findings suggest that specific segments of the Canadian population may be more vulnerable to Russian disinformation campaigns due to socioeconomic factors, educational backgrounds, and regional influences. The Canadian public exhibits varying degrees of vulnerability to misinformation across different topics, including the Russian-Ukraine conflict. Our study found that income, education, community size, and gender were consistently associated with variations in susceptibility to misinformation. Lower-income individuals, those with lower education levels, residents of rural areas, and men were generally more vulnerable to misinformation.

[1] We asked four questions about COVID-19, Climate change, and the Russian-Ukraine war and three about social/legal issues.

Specifically, regarding the Russia-Ukraine conflict, the study revealed concerning findings about Canadians' vulnerability to Russian misinformation. A significant percentage (41.5%) of respondents expressed uncertainty about whether the U.S. was funding biological labs in Ukraine. This claim has been a fixture of Russian disinformation campaigns to justify their invasion. We also found that certain sociodemographic groups were more susceptible to misinformation about the Russia- Ukraine conflict. British Columbia and Quebec residents were slightly more vulnerable to misinformation on this topic than other regions. Additionally, individuals with lower household incomes (below $40,000) were more likely to be misinformed about the Russia-Ukraine conflict than higher-income groups. Furthermore, the study noted regional disparities in vulnerability to misinformation. Respondents from the Prairie provinces (Alberta, Saskatchewan, and Manitoba) were consistently more susceptible to misinformation across all topics, including the Russia-Ukraine conflict.

Figure 1: Average Marginal Effects – Misinformation by Topic and Socio-demographic Characteristics[2]



[2] Figure taken from Boucher et al. Forthcoming.

Based on the findings presented in the paragraphs, pre-bunking strategies to combat misinformation and disinformation should leverage the information about the sociodemographic factors contributing to vulnerability. The research suggests that susceptibility to misinformation is a structural issue, rather than an individual deficiency, and certain segments of the population are more vulnerable due to factors such as lower income, lower education levels, residing in rural areas, and gender (with men being more vulnerable). To effectively organize communication campaigns, pre-bunking strategies should prioritize and tailor their efforts to these higher-risk populations, considering their unique socioeconomic and regional characteristics. By strategically targeting and addressing the specific vulnerabilities of these groups, pre-bunking campaigns can enhance societal resilience and better protect against the influence of malign misinformation and disinformation operations.

Lose enforcement and FIMI

The final condition for FIMI operation is a relatively permissive enforcement environment. For all the actors examined above, little cost is associated with information manipulation and interference beyond ordinary diplomatic rebuttal. In our mind, four key elements have created this permissive environment:

1) lack of dedicated institutions;
2) lack of regulations;
3) lack of state capacity to detect FIMI;
4) lack of civil society capacity to respond to FIMI.

The absence of dedicated institutions for enforcing regulations creates a permissive environment that makes (FIMI) increasingly attractive for state and non- state actors. In many democratic systems, there's a notable gap in oversight due to the lack of specialized agencies or bodies specifically tasked with monitoring and addressing FIMI activities.

In Canada, for example, the responsibility for addressing foreign influence is dispersed among various departments, often operating independently. Through its Rapid Response Mechanism (RRM) team, Global Affairs Canada is tasked with monitoring and responding to foreign information manipulation and interference. However, this approach focuses primarily on external sources of manipulation, paying limited attention to domestic entities. Public Safety focuses on examining domestic groups, with a heightened focus on far-right extremism and addressing foreign interference through legal prosecution. Heritage Canada is mandated to sponsor programs to foster digital citizenship and media literacy, funding initiatives such as academic research and NGO programs to bolster societal resilience. Canada's intelligence agencies, including CSIS and CSE, possess internal capabilities for tracking foreign informational manipulation but often operate behind classified barriers and are perceived as reluctant to collaborate with other governmental entities. The Department of National Defence maintains some capacity for strategic communication and safeguarding the Canadian Armed Forces from foreign information operations during overseas deployments. Finally, the Privy Council of Canada oversees the coordination and streamlining of the government's response to FIMI. Consequently, much of the resources of the Government of Canada dedicated to FIMI are dispersed thin (10-15 personnel per team) across

Parliament Hill, and much of its time is devoted to briefing officials and coordinating activities.

Secondly, the absence of comprehensive regulation addressing FIMI represents a significant challenge in combating the growing threat posed by state and non-state actors leveraging digital platforms to manipulate public opinion and undermine democratic processes. Across various jurisdictions, including Canada and Germany, a gap exists in regulatory frameworks tailored to address the complex and evolving tactics employed in FIMI campaigns. Without clear guidelines and legal mechanisms to govern online information dissemination and counter foreign interference efforts, malign actors can exploit vulnerabilities in the information ecosystem with impunity. This lack of regulation enables the proliferation of disinformation and propaganda and undermines public trust in democratic institutions and electoral processes. To effectively confront the threat of FIMI, concerted efforts are needed to develop and implement robust regulatory frameworks that provide clarity, accountability, and enforceability in combating foreign influence operations and safeguarding the integrity of democratic societies. However, we must note that some progress has been made in Canada, where several internal policies and bills are in development. Furthermore, the European Union has made significant strides in building mechanisms and supranational entities to combat FIMI.

Thirdly, government agencies need more capabilities, exacerbating the challenges posed by FIMI. They need the necessary technological infrastructure, language proficiency, and domain expertise to combat propaganda effectively. The deficiency in state capacity for detecting FIMI presents a critical challenge in effectively addressing the multifaceted threats posed by foreign actors leveraging digital platforms for nefarious purposes. In Canada and Germany, as in many other nations, the rapidly evolving nature of FIMI tactics and the sheer volume of online content present formidable obstacles for detection by governmental authorities.

Moreover, the transnational nature of FIMI campaigns often requires cross-border cooperation and intelligence-sharing, adding another layer of complexity to detection efforts. As a result, state actors are usually unable to keep pace with the sophisticated tactics employed by malign actors, leaving democratic societies vulnerable to foreign interference in their information ecosystems. Significant investments in technology, training, and collaboration are necessary to address this challenge and enhance state capacity for detecting and countering FIMI, thereby safeguarding the integrity of democratic processes and information environments.

Finally, the lack of capacity in civil society to effectively respond to FIMI poses a significant obstacle in mitigating the impact of foreign interference on democratic societies. In both Canada and Germany, as in many other countries, civil society organizations often need more resources, expertise, and coordination to confront the sophisticated tactics employed by state and non-state actors in FIMI campaigns. Limited funding, organizational capacity, and technological know-how hamper efforts to monitor, analyze, and counteract disinformation and propaganda spread by foreign entities. Additionally, the decentralized nature of civil society responses further complicates coordination and collaboration among diverse stakeholders. Without robust support and investment in civil society initiatives to address FIMI, democratic societies remain vulnerable to manipulation and division, undermining public trust in institutions and democratic processes. Strengthening civil society's capacity to respond to FIMI requires increased funding, training, and coordination efforts to empower grassroots organizations and amplify their voices in combating foreign interference and safeguarding the integrity of democratic information ecosystems.

In hindsight, the pervasive issue of foreign information manipulation and interference (FIMI) in democratic societies stems from critical institutional and regulatory gaps, leading to fragmented responses and malign actors' exploitation of digital vulnerabilities. The dispersal of responsibilities across various departments, as illustrated in Canada, along with the absence of comprehensive regulatory frameworks, undermines efforts to tackle external and internal misinformation threats effectively. To enhance resilience against these threats, there is a pressing need for concerted actions, including

establishing dedicated institutions, formulating robust regulatory measures, and significant investments in technological upgrades, expert training, and cross-sector collaboration. These steps are essential to empower governmental agencies and civil society, enhance detection and response capabilities, and ultimately safeguard the integrity and trust of democratic processes.

CONCLUSION

The escalating challenges posed by foreign information manipulation and interference (FIMI) in democracies have been underscored by various international discussions and reports, highlighting the urgent need for a cohesive and proactive response strategy. Identifying AI-driven misinformation and disinformation as a significant risk to political and economic stability necessitates a robust framework that not only counters but anticipates FIMI activities. Despite efforts such as the G7's Rapid Response Mechanism, the reactive nature of current strategies has yet to prove sufficient in curbing the sophisticated and ever-evolving tactics employed by state and non-state actors. This points to a critical gap in our understanding and operational capabilities against such threats.

As democracies face these challenges, it becomes evident that a multifaceted approach involving enhanced regulatory frameworks, dedicated institutions, and international cooperation is required. The fragmentation of responsibilities and lack of stringent regulations across nations like Canada have made it easier for foreign actors to exploit vulnerabilities within digital information spaces. Creating more targeted and cohesive policies, alongside strengthening existing mechanisms, can provide a more resilient defence against the manipulations that threaten democratic integrity and stability. Moreover, engaging with civil society and improving public education on media literacy can play a pivotal role in bolstering societal defences against misinformation and disinformation.

Recommendations should focus on three strategic areas to effectively mitigate the risks associated with FIMI. First, enhancing the detection and response capabilities of democracies through better resource allocation and technology adoption is crucial. Second, international collaborations must be strengthened

to ensure a unified and robust response to FIMI threats, which often transcend national boundaries. Lastly, a significant shift towards pre-bunking strategies can help immunize the public against misinformation before it can have a detrimental impact. Our pre-bunking strategy should focus on building counter-narrative used by our most pressing adversaries in the information space (Russia, China, the far right, and to a lesser extent, Iran and their proxies) and concentrate our messaging on their target audience, which represents the population most vulnerable to foreign influence operations. Combined with a proactive and well-coordinated international effort, these strategies are vital in preserving the integrity of democratic processes and countering the pervasive influence of foreign information manipulation.

REFERENCES

Aday, Lu Ann. *At risk in America: The health and health care needs of vulnerable populations in the United States*. Vol. 13. John Wiley & Sons, 2002.

Bastos, Marco, and Johan Farkas. “Donald Trump is my President!”: The internet research agency propaganda machine.” *Social Media + Society* 5, no. 3 (2019): 2056305119865466.

Batzdorfer, Veronika, Holger Steinmetz, Marco Biella, and Meysam Alizadeh. "Conspiracy theories on Twitter: emerging motifs and temporal dynamics during the COVID-19 pandemic." *International journal of data science and analytics* 13, no. 4 (2022): 315-333.

Borrion, Hervé. 2013. “Quality Assurance in Crime Scripting.” *Crime Science* 2, no. 1: 1-12.

Boucher, Jean-Christophe, Erin Gibbs Van Brunschot, Garret Parry, Davina Shanti, and Jordan Arnold. Forthcoming. “Facts and Minds in a Digital Landscape: What Shapes Individuals’ Vulnerability to Misinformation?” in Bessma Momani and Shelly Ghai Bajaj (eds). *Misinformation in Canada.* Toronto: University of Toronto Press.

Boucher, J. C. (2022). Disinformation and Russia-Ukrainian War on Canadian Social Media. *The School of Public Policy Publications*, 15(1).

Bradshaw, Samantha, and Philip N. Howard. 2019. "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation." *Working Paper* 2019.3. Oxford, UK: Project on Computational Propaganda.

Bradshaw, Samantha, Hannah Bailey, and Philip N. Howard. *Industrialized disinformation: 2020 global inventory of organized social media manipulation.* Computational Propaganda Project at the Oxford Internet Institute, 2021

Chan, Man-pui Sally, Christopher R. Jones, Kathleen Hall Jamieson, and Dolores Albarracín. "Debunking: A meta-analysis of the psychological efficacy of messages countering misinformation." *Psychological Science 28*, no. 11 (2017): 1531-1546.

Chesney, Robert, and Danielle K. Citron. 2019. “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security.” *California Law Review* 107: 1753- 1820.

Cho, Charles H., Martin L. Martens, Hakkyun Kim, and Michelle Rodrigue. “Astroturfing global warming: It isn’t always greener on the other side of the fence.” *Journal of Business Ethics* 104 (2011): 571-587.

Cianci, Licia, and Davide Zecca. "Polluting the Political Discourse: What Remedies to Political Microtargeting and Disinformation in the European Constitutional Framework?." *European Journal of Comparative Law and Governance* 10, no. 1 (2023): 1-46.

Clarke, Ronald V., and John E. Eck. 2003. *Become a Problem-Solving Crime Analyst.* London: Jill Dando Institute of Crime Science.

Cohen, Lawrence E., and Marcus Felson. "Social change and crime rate trends: A routine activity approach (1979)." *In Classics in environmental criminology*, pp. 203-232. Routledge, 2010.

Cornish, Derek B., and Ronald V. Clarke. 1986. *The Reasoning Criminal: Rational Choice Perspectives on Offending.* New York: Springer-Verlag.

Ecker, Ullrich KH, Stephan Lewandowsky, and Joe Apai. “Terrorists brought down the plane!—No, actually it was a technical fault: Processing corrections of emotive information.” *Quarterly Journal of Experimental Psychology* 64, no. 2 (2011): 283-310.

Ekblom, Paul. 2010. *Crime Prevention, Security and Community Safety Using the 5Is Framework.* London: Springer.

Felson, Marcus, and Ronald V. Clarke. 1998. “Opportunity Makes the Thief.” *Police Research Series*, Paper 98, no. 1-36 (1998): 10.

Fridman, O., Kabernik, V., & Pearce, J. C. (Eds.). (2019). *Hybrid conflicts and information warfare: new labels, old politics*. Lynne Rienner Publishers, Incorporated.

Gorwa, Robert. 2019. "What is Platform Governance?" *Information, Communication & Society* 22, no. 6: 854-871.

Government of Canada. 2024. *Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions*. Accessed electronically on April 22, 2024.

https://foreigninterferencecommission.ca/#:~:text=On%20September%207%2C% 202023%20the,of%20Appeal%2C%20was%20appointed%20Commissioner.

Government of Canada. Global Affairs Canada. 2019. *Charlevoix commitment on defending democracy from foreign threats.* Document accessed electronically on March 8, 2024. https://www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2018-06-09-defending_democracy-defense_democratie.aspx?lang=eng.

Guerra, Chris, and Jason R. Ingram. 2022. "Assessing the relationship between lifestyle routine activities theory and online victimization using panel data." *Deviant Behavior* 43, no. 1: 44-60.

Klinger, U., Lance Bennett, W., Knüpfer, C. B., Martini, F., & Zhang, X. (2023). From the fringes into mainstream politics: Intermediary networks and movement-party coordination of a global anti-immigration campaign in Germany. *Information, Communication & Society*, 26(9), 1890-1907.

Krafft, P. M., & Donovan, J. (2020). "Disinformation by design: The use of evidence collages and platform filtering in a media manipulation campaign." *Political Communication*, 37(2), 194-214.

Leukfeldt, R., & Kleemans, E. E. (2019). "Cybercrime, money mules and situational crime prevention: Recruitment, motives and involvement mechanisms". *In Criminal networks and law enforcement* (pp. 75-89). Routledge.

Lewandowsky, Stephan, Ullrich KH Ecker, Colleen M. Seifert, Norbert Schwarz, and John Cook. "Misinformation and its correction: Continued influence and successful debiasing." *Psychological science in the public interest* 13, no. 3 (2012): 106-131.

Maimon, D., Howell, C. J., Perkins, R. C., Muniz, C. N., & Berenblum, T. (2023). A Routine Activities Approach to Evidence-Based Risk Assessment: Findings From Two Simulated Phishing Attacks. *Social Science Computer Review*, 41(1), 286-304.

Meaker, Morgan. 2023. "Slovakia's Election Deepfakes Show AI Is a Danger to Democracy." *Wired*, October 3, 2023. Accessed electronically on April 22, 2024. https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to- democracy/.

Park, Soyoung, Sharon Strover, Jaewon Choi, and MacKenzie Schnell. “Mind games: A temporal sentiment analysis of the political messages of the Internet Research Agency on Facebook and Twitter.” *New media & society* 25, no. 3 (2023): 463-484.

Ribeiro, Filipe N., Koustuv Saha, Mahmoudreza Babaei, Lucas Henrique, Johnnatan Messias, Fabricio Benevenuto, Oana Goga, Krishna P. Gummadi, and Elissa M. Redmiles. 2019. “On microtargeting socially divisive ads: A case study of russia- linked ad campaigns on facebook.” *In Proceedings of the conference on fairness, accountability, and transparency,* pp. 140-149. 2019.

Shi, Leiyu, and Gregory D. Stevens. *Vulnerable populations in the United States*. John Wiley & Sons, 2021.

Solomon, Erika. 2024. “Far Right’s Ties to Russia Sow Rising Alarm in Germany.” *New York Times*. April 15,2024. Accessed electronically on April 22, 2024: https://www.nytimes.com/2024/04/15/world/europe/germany-afd-russia.html?smid=nytcore-ios-share&referringSource=articleShare&ugrp=c&pvid=897A3763-795C-4CE3-B0A7- F519635F5D6F

Starbird, Kate, Ahmer Arif, and Tom Wilson. 2019. “Disinformation As Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations.” *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW: 1-26.

Stricot, Matthieu. 2022. “How Social Networks Manipulate Public Opinion.” *CNRS News*. https://news.cnrs.fr/articles/how-social-networks-manipulate-public-opinion.

Stukal, D., Sanovich, S., Bonneau, R., & Tucker, J. A. (2022). Why bother: how pro- government bots fight opposition in Russia. *American political science review*, 116(3), 843-857.

Stukal, Denis, Sergey Sanovich, Joshua A. Tucker, and Richard Bonneau. 2017. “Detecting Bots on Russian Political Twitter.” *Big Data* 7, no. 6: 375-390.

Szostek, Joanna. 2019 "Nothing is true? The credibility of news and conflicting narratives during “Information War” in Ukraine." *The international journal of press/politics* 23, no. 1 (2018): 116-135.

United States. U.S. Department of State. 2024. *Joint Statement from the United States, United Kingdom, Canada on Countering Foreign Information Manipulation.* Document accessed electronically on March 22, 2024. https://www.state.gov/joint-statement-from-the-united-states-united-kingdom- and-canada-on-countering-foreign-information-manipulation/.

Tucker, Joshua A., Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan. "Social media, political polarization, and political disinformation: A review of the scientific literature." *Political polarization, and political disinformation: a review of the scientific literature* (March 19, 2018) (2018).

Wanless, A., & Pamment, J. 2019. "How do you define a problem like influence?" *Journal of Information Warfare*, 18(3), 1-14.

Wortley, Richard, and Lorraine Mazerolle, eds. 2011. *Environmental Criminology and Crime Analysis*. Abingdon: Routledge.