Understanding and Responding to Disinformation Targeting Canadian Companies

June 1st, 2024

Contents

Executive Summary

The spread of falsehoods is as old as communications itself. Yet, what is unique to our age, with the advent of the Internet and social media, is the rapidly accelerating volume and velocity of the spread of false information, whether for tarnishing reputations, stoking ethnic tensions, influencing political campaigns, or casting doubt on scientific consensus and public health interventions during the COVID-19 pandemic. Online disinformation, increasingly recognized as a threat to democracy, social cohesion and economic security, is prompting government policy and legislative interventions. In Canada, the federal government has proposed and introduced several measures to address the spread of disinformation.

There is another important, and less discussed, target of online disinformation: Canadian companies. Online disinformation activity has been identified as a growing threat to companies, corporate brands and executives – and, more broadly, to Canada's economic security. Corporate disinformation can take the form of manipulated videos showing what appears to be faulty products, fake letters written to appear from executives making changes to corporate strategy, or other types of falsehoods to make headlines or undermine trust. Threat actors have used disinformation to negatively impact company share prices, public perceptions, and customer trust. Once online, corporate disinformation can be reposted and spread unwittingly, take on new forms, or be tied to larger conspiracy theories. New generative AI tools like ChatGPT, which can create text, images, and videos that are indistinguishable from real content, are making it easier to spread false narratives and manipulate public opinion. This could exponentially amplify the disinformation threat to companies and brands, and erodes trust in the economy. For corporate leaders and economic policymakers, it is time to sound the alarm.

This white paper aims to fill the knowledge gap about disinformation and its intersection with Canadian companies and corporate brands. It begins by **defining disinformation, and related concepts of misinformation and malinformation**, within a broader lexicon that commonly labels these types of content as "fake news" or "propaganda". It **identifies the most common disinformation threat actors** (i.e. hostile state actors, hacktivists, disgruntled employees, cybercriminals, and rival firms), and **outlines the tools and tactics they employ by threat actors** to create and amplify disinformation on social media, including exploiting algorithms, trolls and bots, and AI-generated content. It describes the **ways disinformation is used to target companies** and presents survey data showing how **Canadian consumers are experiencing disinformation** and how it influences their brand perceptions.

Recognizing that Canada's corporate leaders are seeking practical solutions for addressing the threat of online disinformation in today's information ecosystem, the next section offers forward-thinking actions companies can take. These fall in three categories:

1. **Establishing** internal policies and capabilities for **responding** to malicious disinformation, including incident response plans, threat monitoring and digital literacy training.
2. **Tracking – and engaging in – the policy and regulatory processes** underway to address online harms and disinformation in Canada and other jurisdictions.
3. **Monitoring social platforms' performance in addressing disinformation** and creating a safe environment for corporate brands, corporate communication and online advertising.

As a final note, industry leaders must recognize that disinformation is a threat not just to their companies and the bottom line, but to Canada's economy, democracy and social cohesion. The erosion of trust in markets, democratic institutions and the bonds of citizenry all undermine the operating environment for Canada's businesses – not to mention the country itself. In sum, Canadian businesses have a big stake in combatting disinformation and ensuring a safe, secure and trustworthy information ecosystem for all.

1. Introduction

The spread of falsehoods is as old as communications itself. Yet, what is unique to our age, with the advent of the Internet and social media, is the rapidly accelerating volume and velocity of the spread of false information, whether for tarnishing reputations, stoking ethnic tensions, influencing political campaigns, or casting doubt on scientific consensus and public health interventions during the COVID-19 pandemic[1]. Sometimes, individuals spread falsehoods unwittingly: labelled misinformation. Of greater concern is the intentional spreading of false information to cause harm, known as *disinformation*[2]. Research assessing Canadians' ability to distinguish fact from falsehood shows a clear correlation between news consumption on social media and belief in disinformation[3]. The inverse is true for those relying on "legacy media", such as TV and news websites. This is concerning as survey research indicates that more and more Canadians are turning to social media for news, health information, product advertisements and much more.

Online disinformation, increasingly recognized as a threat to democracy, social cohesion and economic security, is prompting government policy and legislative interventions[4]. In Canada, the federal government has proposed and introduced several measures to address the spread of disinformation. This includes establishing voluntary guidelines for social media platforms, and measures to monitor and mitigate foreign disinformation during election campaigns. These, and other measures by platforms themselves, are discussed in detail in this paper.

There is another important, and less discussed, target of online disinformation: Canadian companies. Online disinformation activity has been identified as a growing threat to companies, corporate brands and executives – and, more broadly, to Canada's economic security[5]. Disinformation can take the form of manipulated videos showing what appears to be faulty products, fake letters written to appear from executives making changes to corporate strategy, or other types of falsehoods to make headlines or undermine trust. Threat actors have used disinformation to negatively impact company share prices, public perceptions, and customer trust[6]. Once online, corporate disinformation can be reposted and spread unwittingly, take on new forms, or even be tied to larger conspiracy theories. To take one prominent example of the impacts of online disinformation, a 2022 survey found that 10% of Canadians believed there was truth to the claim that Bill Gates used the pandemic to push a vaccine with a microchip capable of tracking people[7].

Rapid advances in technology have the potential to exponentially amplify the disinformation threat. New generative AI tools like ChatGPT, which can create text, images, and videos that are indistinguishable from real content, are making it easier and cheaper to spread false narratives and manipulate public opinion. Groups ranging from global democracy advocate Freedom House and technology consultancy Gartner have predicted that generative AI will "supercharge" disinformation online and through social platforms[8]. Researchers and media reports are finding that AI-generated deep fake images and videos, and other forms of synthetic media, are proving much more difficult for individuals to identify as false. Studies have found that some AI-generated images of faces are perceived as more realistic than real images, which Dr. Amy Dawel of the Australian National University attributes to human "thinking styles that make us more vulnerable on the internet and more vulnerable to misinformation[9]." For corporate leaders and economic policymakers concerned about the risks to companies and brands, and public trust in the economy, it is time to sound the alarm.

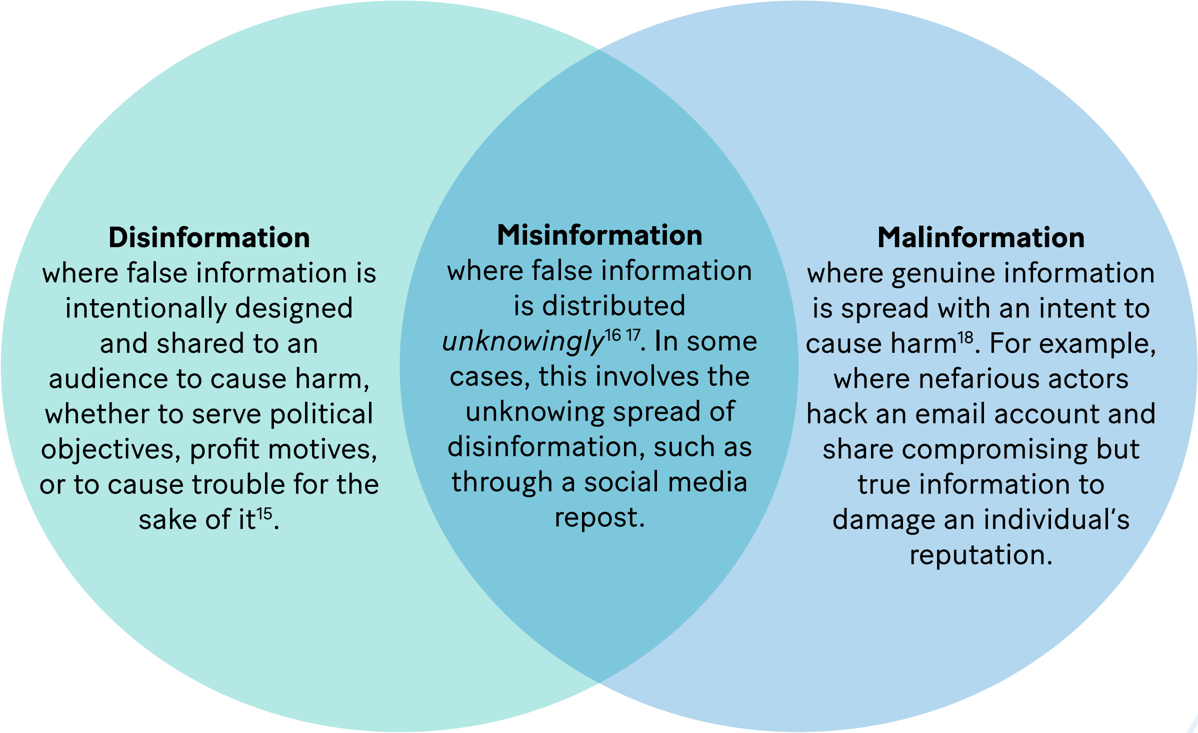
This white paper aims to fill the knowledge gap about disinformation and its intersection with Canadian companies and corporate brands. The first part of the paper describes the current environment for corporate online disinformation, and its relationship to broader developments in society, technology and policy. The second part offers proactive actions companies can take to understand, monitor and respond to malicious online disinformation. This paper is informed by a variety of sources, including a national survey of 1,500 Canadians over the age of 18[10], a focus group discussion with Canadian executives in IT, law, and communications roles, and academic literature, government publications and media reports on disinformation.

2. The Disinformation Threat to Canadian Companies

2.1 Defining Disinformation

The phenomenon of spreading false information to serve an objective is not new, nor is it the exclusive product of digital society[11]. Yet, the advent of the Internet and modern digital technologies have increased the speed in which false information travels, particularly through social media, making its ability to scale unprecedented[12]. Academic and policy discussions surrounding online disinformation have gained traction since the middle of the last decade, spurred by high profile international events including the 2016 US presidential election, "Brexit", and the Cambridge Analytica scandal. New terms have emerged in the common lexicon such as "fake news", alongside long-standing phrases like "propaganda" (typically linked to state or military use), "information warfare" and "influence operations[13]." All contribute to what disinformation expert Claire Wardle collectively refers to as "information disorder.[14]"

The spread of false information is commonly defined under three related but distinct terms :



Disinformation
where false information is intentionally designed and shared to an audience to cause harm, whether to serve political objectives, profit motives, or to cause trouble for the sake of it[15].

Misinformation
where false information is distributed *unknowingly*[16][17]. In some cases, this involves the unknowing spread of disinformation, such as through a social media repost.

Malinformation
where genuine information is spread with an intent to cause harm[18]. For example, where nefarious actors hack an email account and share compromising but true information to damage an individual's reputation.

These three concepts, often used interchangeably, are distinct but often intersecting, which can create confusion. For example, it is often difficult to determine which of these categories applies to false information. Making a determination requires identifying the original source of false online information; and then determining the actor's intent in creating and sharing it. The spread of disinformation by a malevolent actor can also lead to misinformation, where other unwitting actors then share the deceptive information. The Canadian Centre for Cyber Security distinguishes the terms, but describes them collectively as MDM[19].

The spread of false information also occupies a unique place in the online safety and cyber security landscape. Disinformation typically displays the common elements of a cyber threat, i.e. a threat actor, a target, an attack vector for distribution, a detrimental impact – but is not typically listed with phishing, malware, denial of service (DoS) and other types of threats in cyber security technical standards, learning manuals and other resources[20]. However, disinformation can contribute to those types of attacks. For example, phishing attacks, the most common form of social engineering threat, share false or deceptive information in ways that target human cognitive weakness, usually in order to enable financial or personal information theft or fraud. While the economic motivation might be different, the deceptive tactics can be similar. At the same time, disinformation has typically been considered a category of "online harm" experienced by Canadians and subject to the policies of major social platforms[21], but is not within the scope of current legislative proposals such as Canada's proposed Online Harms Act (see section 3.2).

A note to readers: **this white paper uses the term "disinformation" throughout** as it is the most widely recognized term for sharing false information, but also reflects the malicious intent to spread false information to deceive.

2.2 Disinformation Threat Actors, Tools and Tactics

The Internet has become the essential source of information for Canadians, whether they are seeking public services, news and entertainment or products and services on Amazon or at the local bookstore. The general intent of online disinformation is to influence Canadians through false or deceptive information. For some threat actors, the deeper intent is to degrade trust in online spaces, exploit divisions in society, and grow mistrust among citizens and towards key institutions[22]. Efforts to pollute the information ecosystem risk the further erosion of shared values in Western societies, and the continued decline of trust in governments, companies and media[23].

In this environment, certain types of targets in the corporate sector are more susceptible to disinformation campaigns. High profile CEOs and corporate leaders, particularly those with significant social media presence, can be targeted to damage reputations or injure brands by proxy. Businesses that take vocal public positions on political, social or environmental issues can also be potential targets. Companies engaging in a major financial event, such as an IPO, merger or acquisition or significant product launch, could also be vulnerable[24].

Experts point to numerous threat categories for online disinformation. A significant one relates to **national security and geopolitics**. Government intelligence agencies report that state actors deliberately create and amplify conspiratorial content with the aim of undermining public trust and exploiting social divisions within rival countries[25]. A related category is disinformation as part of **electoral interference** efforts[26] [27]. There are also **public safety** threats to individuals, communities, or social movements through online targeting, which in some instances leads to offline threats of physical violence[28]. Some disinformation threats cut across these categories. For example, during the COVID-19 pandemic, the influx of disinformation in Western countries like Canada posed a broad threat to social cohesion and trust in democratic institutions, while also undermining public health authorities and a direct threat to the health and safety of citizens[29].

Recognizing that threats can have impacts across these categories, this white paper focuses on disinformation targeting companies and brands. As a starting point, it is important to identify the most common threat actors responsible for spreading disinformation and their varying motivations.

Hostile state actors may be motivated by ideology, a desire to favourably shape the discourse on domestic and international events, or to sow distrust towards political institutions and democracy more broadly including by exploiting social divisions[30]. Canada's National Cyber Threat Assessment identifies China and Russia as key propagators of disinformation in the Canadian information ecosystem[31]. Focus group participants relaying their experiences with false information online reinforced this assessment, with one respondent describing Russia as "best in the art" of employing disinformation. In June 2022, cybersecurity reports linked China to a disinformation campaign that used thousands of inauthentic social media accounts to target rival mining companies in the West, including a Canadian company developing a rare earth mine in northern Saskatchewan[32].

Hacktivists, non-state actors generally motivated by the desire for social and political change, pursue activism through malicious cyber activities. Some express distrust towards neo-liberal or business elites, who they believe are responsible for economic, environmental or social disarray[33]. While hacktivists often view their actions as civil disobedience, state security and intelligence agencies consider such groups or individuals to be significant threats[34]. For example, hacking companies in sectors like mining or oil and gas to leak sensitive documents online, in support of environmental causes[35]. Hacktivists have also been linked to foreign states, such as groups targeting Ukrainian-aligned countries like Canada, in some cases targeting businesses as a means to threaten a nation's economic security[36].

Disgruntled employees, motivated by a pursuit of retribution or economic justice from the organization or industry they work in, are a disinformation threat of particular concern for businesses. For instance, a staged photo of RyanAir employees shown sleeping on the ground at an airport went viral in an attempt to portray unfair labour practices[37].

Cybercriminals are motivated by financial profit, often deploying disinformation to gain access to company systems, employees or data as a means to acquire illicit gains. Disinformation can be a useful social engineering instrument[38], whereby threat actors seek to deceive individuals or employees to share information to enable criminal activities[39]. Internal company help desks have become a popular choice for threat actors in applying social engineering tactics. Threat actors will try to convince such workers to unwittingly provide assistance, such as by resetting forgotten passwords[40]. They also use convincing fake messages or AI-generated deepfakes to trick employees into triggering ransomware attacks, or injecting malware into online advertisements or articles that when clicked are deployed into company or client devices[41]. Cybercriminals can also be aligned with foreign adversaries. Russian state-backed criminal groups have been a particular threat, flooding online spaces with disinformation, spam and malware[42].

Threat actors spread disinformation through online and traditional media. This often involves using fake personas to introduce, amplify and spread false narratives through fake websites, chat rooms, discussion forums, comments sections on news and other websites[43]. However, **social media platforms** are the most significant tool for disseminating online disinformation. According to a national representative survey in 2022, 98% of adult Canadians use at least one type of social media. Increasingly, this includes using the platforms to stay up to date with news, with Facebook (32%), YouTube (24%) and Instagram (16%) being particularly popular[44]. Respondents who use social media specifically to access news report higher levels of false information than those who do not use social media as a channel for news (i.e. they use traditional media to access news). The same survey reveals that the use of these three platforms for news is associated with higher levels of encountering false information (64% encounter at least a few times per month) than those who do not (56%)[45]. TikTok is also an emerging news source for younger Canadians, with 30% of those aged 16-23 saying they use the platform to stay up to date with the news. Canadians' use of social media for news has become an exploit for bad actors who amplify false content, challenging peoples' ability to decipher between legitimate and illegitimate claims.

The design of social media platforms also makes them effective vectors for spreading disinformation. Algorithms on the major platforms reinforce user choices by providing or recommending content from similar sources, which is effective in keeping users engaged. This can also create 'echo chambers'[46] [47]. Research shows that outrageous and sensationalized content is significantly more likely to go viral[48]. This can lead users to more extreme forms of content with a higher likelihood of being disinformation[49]. However, the extent of this algorithmic amplification differs across social media platforms. Focus group respondents described how threat actors' choice of platform depends on their objective, with certain platforms better suited to meeting their objectives.

A number of **tactics** are employed by threat actors to amplify disinformation on social media

Exploiting algorithms to gather and analyze data on how users respond to content: This includes analyzing what would appear to be innocuous interactions such as the contents of posts, likes, shares, metadata, and much more. Internal documents from Facebook also show that 'misinformation, toxicity, and violent content are inordinately prevalent among reshares'[50].

Flowing disinformation across different platforms, including private messaging apps: In addition to public platforms like Facebook and X (formerly Twitter), a recent survey found that a large majority of Canadians (83%) use at least one private messaging application such as WhatsApp or Facebook Messenger[51]. These applications are also increasingly used to share news, with 21% of respondents claiming to do so[52]. Studies also reveal a correlation between those who use these platforms for news and increased belief in COVID-19 conspiracy theories[53] [54]. Disinformation flows can be difficult to detect, such as where content flows between platforms. For instance, it can be initially posted in a private channel on Discord or Telegram, and then shared and amplified on public platforms like Facebook.

Using trolls and bots to amplify disinformation: Investigative work has identified state-sponsored "troll factories" — well-staffed organizations such as the now infamous Internet Review Agency in Russia — that coordinate social media campaigns[55]. Trolls spread false narratives or bully and harass individuals and communities online, discouraging the expression of voices. These activities can be automated through the use of bots, which are designed to automatically produce content and interact with humans in ways that mimic real human behaviour[56]. Trolls or bots can be used, for instance, to amplify content aimed at boycotting a brand[57].

Employing coordinated inauthentic behaviour (CIB) efforts: This involves a concerted use of fake accounts to mislead users on a platform[58]. This differs from bots, as CIB efforts are mainly carried out by humans. The scale of this problem has been revealed in recent announcements by platforms on the mass removal of user accounts. One example in 2023 was Meta's removal of over 7,500 accounts reportedly linked to a Chinese influence campaign[59]. Yet, platforms have been criticized for lacking proper enforcement of terms of use that prohibit CIB, and for subjectivity, a lack of transparency, or political influence in account removal decisions.

Engaging social media influencers: Social media influencers are people who have built an online reputation and following, usually based on their knowledge or expertise on a particular topic. While influencers can be unwitting amplifiers, they are being hired in some cases by companies to purposefully manipulate opinion on social media in what has become a growing 'disinformation for hire' industry[60]. This can be attractive for malicious corporate actors as it provides a degree of credibility.

AI generated content: Developments in AI — particularly generative AI — are enabling the creation of more realistic and believable content, including videos, images, and text. There are many recent instances of the use of deceptive synthetic media (such as deep fake videos), whether in the Russia-Ukraine conflict, spoofing celebrities by repurposing their faces and voices, or virally depicting Pope Francis in a Balenciaga jacket. To target companies, cybercriminal scams have used AI to clone a director's voice and ask unsuspecting employees to transfer money to a bank account[61].

Finally, other types of digital tools and media are also commonly used for spreading online disinformation, including standalone "fake news" **websites** and **blogs**, or **emails** and **text messages** used for deceptive phishing attacks. Legacy media such as TV and radio can also spread disinformation, whether intentionally or unwittingly. Social media, however, remains the most significant and challenging tool for companies and other stakeholders to grapple with, due to its unique reach and scale.

2.3 Disinformation Targeting Companies and Brands

There is a long history of disinformation in business, both used by firms as a strategy or tactic to advance corporate interests and where firms are the target of disinformation by various threat actors.

There are various ways companies use disinformation to target competitors or adversaries. Longstanding disinformation tactics include altering financial reports to fraudulently improve market sentiment, or creating falsified news articles in obscure publications to create counter-narratives or defame a rival firm[62]. In the social media age, these tactics have become far less costly, easier and more quickly deployed. Yet, there is evidence that deploying disinformation in corporate communication may offer short-term benefits but can have long-term consequences if it comes to light, including tarnished brand reputation and legal liability[63].

Disinformation is also used by external actors to target businesses and their executives. Although corporate disinformation may serve political objectives, companies can be targeted by actors with other motivations: "financial ones (manipulating share prices), emotional ones (aversion to brand or corporate leaders) or by disgruntled employees, among others"[64]. A study by Rodriguez-Fernandez about disinformation in Spain found that companies were the second most common target, after political parties[65]. Targeted companies were from different sectors including fashion, department stores, transport companies, energy and hospitality. Most of the disinformation from the study involved false give-aways and job offers. The research also revealed that 31% of disinformation content targeted individuals, including spokespersons or representatives, compared to the organization itself (69%)[66]. The impacts of disinformation can be on brand perception or directly on the share price, as was the case with PepsiCo for the month following false reports about alleged statements the CEO made about Donald Trump supporters[67]. Consumers' perception of brands can also be tied to how closely their advertisements appear next to toxic content on platforms such as conspiracy theories. To prevent perceptions of companies appearing to endorse disinformation, several Canadian brands have pulled their advertisements from the social platform X amid a rise in hateful content since its takeover by Elon Musk[68].

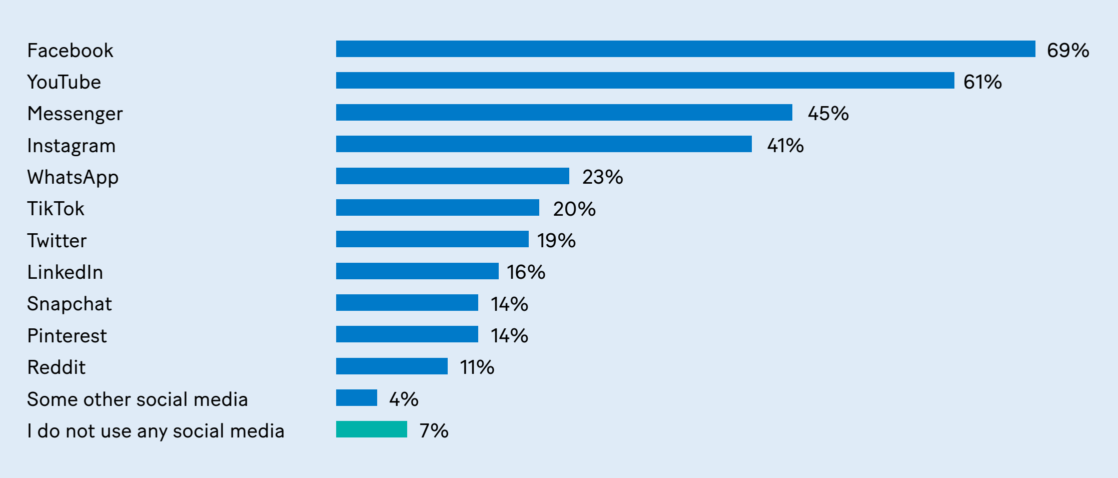
In the focus group session, participants reported growing concern over another vector of disinformation: **impersonations, both of prominent corporate executives, and of the business itself.** Threat actors engage in impersonations for either financial, reputational or geopolitical reasons. Impersonation or identity theft are common tactics used by threat actors, deployed by creating a replica online identity or through hacking social network credentials[69]. Threat actors have hacked into companies' social media accounts for defacement or "doxxing", where personal identifiable information about people or organizations is publicly revealed[70]. The most high profile recent example was following X's launch of paid-for verified accounts, when impersonator accounts parodied the brands of McDonald's, Nintendo, Eli Lilly, Tesla, Coca-Cola and Lockheed Martin, and many others[71].

Other research finds that company-targeted disinformation can **negatively affect employees and their experiences.** Belief in disinformation can spill over to the workplace, impacting employees and posing risks to productivity, workplace culture and cohesion, and retention[72] [73]. According to one study, conspiracy theories can negatively impact productivity by causing conflict among employees, reducing the quality of their work and resulting in signs of withdrawal from colleagues[74].

2.4 How Canadian Consumers Experience Disinformation

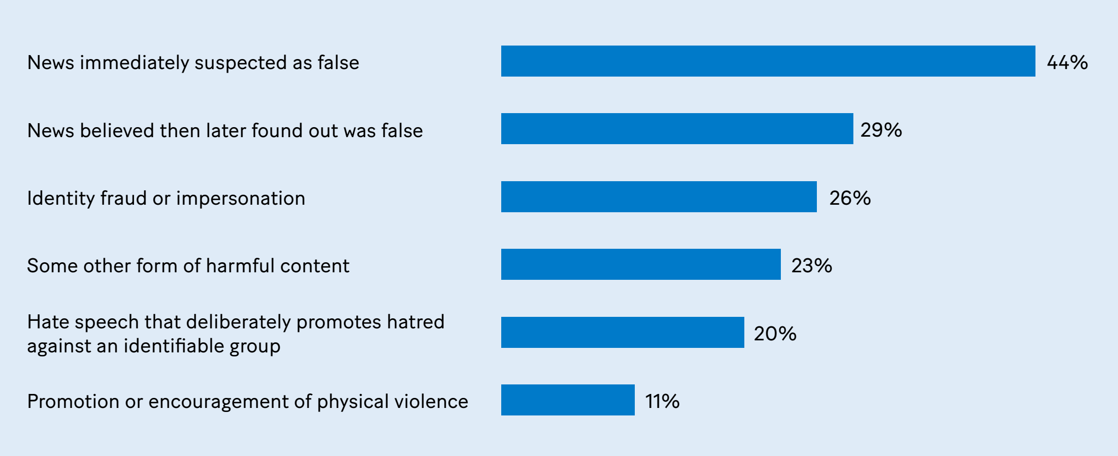
Canadians' use of social media is strong and growing[75]. The survey conducted for this white paper found high levels of social media use among Canadians. It reveals that Facebook (69%), YouTube (61%), Messenger (45%) and Instagram (41%) are the most widely used on a weekly basis, with other services at lower but still significant levels of use (see Figure 1).

Figure 1: Canadians' Online Platform Use on a Weekly Basis



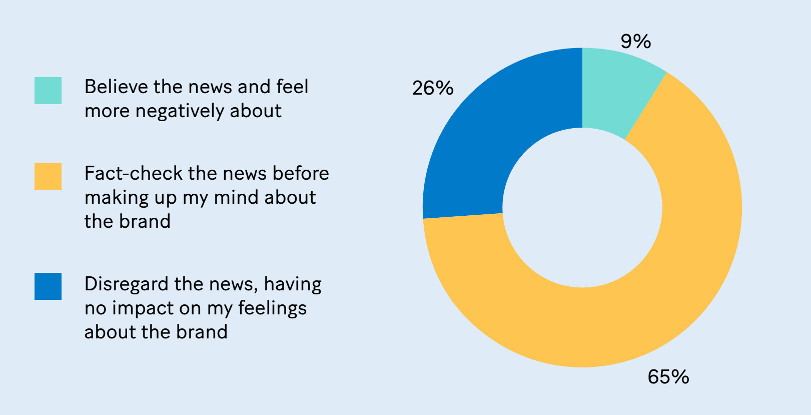
The growing use of social media platforms by Canadians also coincides with an **increase in user exposure to harmful online content, of which, false information (44%) was the most common** type (see Figure 2). This was followed by fraud/impersonation (26%), hate speech (20%), and promotion of physical violence (11%). Further, 51% of respondents reported that in the past year, their encounters with harmful content have increased. Respondents with incomes higher than $100K (62%), as well as those in the Prairies (61%) and Ontario (57%), are more likely to say they see an increase in harmful content[76]. While respondents generally reported that they experienced an increase in harmful online content, this was particularly significant for younger Canadians. Respondents aged 18-34 were more likely to say they experienced news they believed but later turned out to be false (37%), hate speech (33%) and promotion of violence (20%).

Figure 2: Canadians' Harmful Online Content Experienced in Past Year



When asked about exposure to negative news about a brand online, there were also significant differences across demographic groups. Two-thirds of Canadians (65%) said they would fact-check negative news about a brand they see online before coming to a conclusion about it (see Figure 3), while nearly two in ten (17%) Canadians repost without fact-checking. Particularly notable are younger respondents aged 18-34 who are more likely (17%) to believe the negative news and feel more negatively about the brand afterwards. This stands in contrast to older Canadians aged 55+, who are more likely (34%) to dismiss negative news about a brand they read online. The longer-lasting effects of corporate disinformation on younger Canadians is particularly noteworthy; this may lead to negative cumulative effects for companies as younger Canadians' decisions are more easily influenced, triggering decisions including whether to continue to do business with the targeted companies. Such reactions can be have a ripple effect, reaching other consumers through reposts, potentially garnering support for boycotts.

Figure 3: Canadians' Views After Negative News About a Brand Online



3. Moving Forward: Proactive Actions for Canadian Businesses

Canada's corporate leaders understandably feel threatened and unprepared to plan for, and respond to, the deluge of online disinformation in today's information ecosystem. The impacts of malicious disinformation targeting on a firm can be significant, touching everything from share price and stakeholder value, to the reputation of the company, brand, CEO and executive team, to perceptions of products and services among critical audiences. But there are a number of proactive avenues for action, whether through engagement in public affairs, tracking the product and policy changes that social media companies make, or other initiatives that can be taken directly by organizations. This section presents opportunities in each of these categories.

3.1 Establish Internal Policies and Capabilities for Responding to Disinformation

To prepare for, and respond to, disinformation campaigns, companies must be proactive. This requires developing an understanding of the larger social, political and technical context for their business activities, including volatile geopolitical issues today. Some larger companies, for instance, have hired experts to provide geopolitical advice including civil servants, politicians and former diplomats[77]. Indeed, companies, and senior executives in particular, need to understand social media as a complex, and chaotic, online information ecosystem, with a number of voices competing to be heard. This includes a broad range of threat actors with diverse objectives that drive them to manipulate public opinion on social media. Companies need to be aware of the specific risks to the organization of online disinformation, whether related to partners, investors, employees, products and services, or other vectors that could be weaponized as part of a disinformation campaign. Experts are calling on companies to better prepare for these threats, and identifying various measures they can take[78].

Businesses can then take actions to build more proactive strategies that cut across all organizational levels, from front-line staff to senior executives. This could include:

Developing a **Disinformation Incident Response Policy (DIRP)** that defines the organization's protocols and procedures, akin to or as part of its cybersecurity incident response policy. The Policy can act as a framework to guide the organization's strategy, preparations and response in the event a disinformation campaign is detected, outlining the actions, personnel, resources, and tools involved, assigning roles for different members of the team. Components of a DIRP can include risk assessment, focusing on organization-specific vulnerabilities; resilience-building tactics, such as audience engagement, openness and transparency and proactive sharing of accurate information (known as "pre-bunking"); ongoing social media monitoring and early warning systems; and incident response strategies and tactics for countering disinformation. Key organizational leadership roles will typically include team members from information technology and cyber security, communications, marketing and brand, public relations, privacy and data and legal counsel, as well as the executive team.

Creating **social media monitoring teams** to engage on major social platforms and track in- and out-bound content, audience trends and potential threats. Companies can develop in-house capacity, or purchase from a service provider in the rapidly growing market for ventures that combat mis- and disinformation. For example, Viral Nation is a Canadian firm that offers both defensive social media monitoring and screening services for brand safety and reputation management, as well as brand advocacy and social influencer solutions. Yet, because identifying disinformation is a complex and often subjective task, experts note that software tools for monitoring will have varying levels of efficacy[79].

Establishing **early warning systems** for potential disinformation campaigns, to allow for rapid response to contain and mitigate spread. In the event a malicious online campaign is detected, companies can trigger its incident response policy and be ready to proactively counter the disinformation and/or report the activity to the social platform and advocate for moderation of the content and suspension or removal of threat actor accounts, if applicable. Strategic communications will play a central role in mitigating the impacts of disinformation. The DIRP would include details outlining proactive and reactive corporate communications responses including how, when and in what contexts to respond. As surveys suggest Canadians typically fact-check news, quick corporate responses to rapidly address false information can be critical to protecting corporate and brand integrity. If foreign actors or criminal activities are suspected, companies can also report to the Canadian Centre for Cyber Security or law enforcement.

Improving **digital literacy among employees** to create a culture of resiliency. Companies can offer training and ongoing support to employees to equip them to identify disinformation. This can be undertaken through partnerships with civil society groups and universities, who can assist companies in offering employee resources and workshops on digital literacy. This not only helps to mitigate the effects of disinformation on a company but adds to the digital information and democratic resiliency of the larger collective. Similar approaches have launched in Germany and the United States[80].

Resources for Developing a DIRP

A few publicly available resources exist that can support organizational planning and preparedness for disinformation threats. The Government of Canada recently introduced a Countering Disinformation guidebook, which is geared to public servants but offers practical information for other organizations, with links to other Canadian and international resources[81]. The UK government has developed the RESIST toolkit, a more general purpose resource aimed at countering the impacts of disinformation faced by organizations by providing guidance on detection, prevention and response[82]. Consultancies also offer guidance and advisory services for combating disinformation in the corporate sector[83].

Summary of Actions Companies Can Take:

1. Develop a Disinformation Incident Response Policy to guide the organization's strategy, preparation and response in the event of a disinformation event.
2. Create social media monitoring capacity, within an internal team or through an external partner, to proactively identify disinformation threats.
3. Establish early warning systems for potential disinformation campaigns, which can rapidly trigger incident response activities.
4. Improve digital literacy among employees through training and ongoing support for identifying disinformation and other online threats to the organization.

3.2 Track Policy and Regulatory Initiatives to Address Disinformation

The policy discussions, government interventions and legal regimes for addressing online disinformation are evolving quickly, and Canadian businesses can both participate in these processes and track and support their progress including, for example, the proposed federal online safety bill. Other voices, including the Business Council of Canada, have called for businesses to establish closer ties with government to allow greater information sharing, inform policy discussions and bridge economic and national security[84].

To date, Canada has yet to introduce a law specifically aimed at regulating online disinformation. Recent proposed legislative efforts have focused on online safety for citizens, children and consumers[85]. Most significant is Canada's proposed **Online Harms Act**, tabled in February 2024, which would place duties on social media platforms, require efforts to reduce exposure to harmful content in seven categories, and change the Criminal Code and other legislation to toughen penalties for hate speech and crimes, among other provisions[86]. The bill does not directly address disinformation as one of the categories of harmful content, though disinformation activities could contribute to the categories of online harms, such as child bullying, fomenting hatred, or inciting violence. The proposed legislation is contentious given the inherent requirement to strike the right balance between freedom of expression and government regulation. One approach gaining traction in liberal democracies is regulating systems and algorithms of platforms as opposed to content, including establishing transparency requirements on how algorithms operate[87].

Certain government interventions have focused on addressing threats to elections on social media. With major social media platforms including Facebook, X, Google, TikTok, and LinkedIn, the Government of Canada introduced a voluntary code of conduct known as the **Canada Declaration on Electoral Integrity Online**. The voluntary code requires the signatories to continue their efforts at removing fake accounts and inauthentic content, with the aim to safeguard the integrity of federal elections[88]. The federal government has also established the **Critical Election Incident Public Protocol** to coordinate a rapid response to threats, including disinformation campaigns during an election[89]. This involves national security agencies monitoring threats in real-time. It also includes a panel of senior public servants who work to determine whether a threat is significant enough to notify the public. This is assessed based on the threat's potential to disrupt an election – a threshold generally considered to be high[90].

Canadian efforts have also focused on the international domain. Canada is the lead on the **G7 Rapid Response Mechanism**, an initiative meant to strengthen coordination between G7 members on identifying and responding to foreign threats, including disinformation. As part of this mechanism, Canada conducts regular analysis of foreign social media activity, sharing knowledge on potential threats to members and coordinating international responses[91]. It also serves as the early warning system for the **Security and Intelligence Threats to Elections (SITE) Task Force** which consists of several of Canada's security and intelligence organizations to prevent covert or criminal activities from influencing or interfering with Canadian elections.

Finally, the federal government has promoted **digital literacy**, primarily through the **Digital Citizen Initiative**. The program offers funding to non-profit organizations and post-secondary institutions across Canada to improve research and learning materials, as well as promote public awareness programs and tools to encourage critical assessment of digital media[92]. Such efforts run in parallel to digital literacy taught as part of school curriculums in Canada. Almost all provinces and territories have added digital literacy in their programming.

Summary of Actions Companies Can Take:

5. Track the development of online safety and disinformation policy in Canada and in the organization's other markets, to stay informed about potential impacts on your operations.
6. Engage directly in the policy development process for combatting disinformation, through internal public affairs and government relations activities, external advisors or industry associations.

Other Jurisdiction on Disinformation Regulation

Businesses operating transnationally can also monitor actions in other jurisdictions, particularly those that have proposed or enacted more stringent laws or regulation to target disinformation. **Germany's** *Network Enforcement Act* (NetzDG) requires companies to remove illegal content or face heavy fines[93]. **Malaysia** issued an *Emergency Ordinance* in 2021 criminalizing "fake news" related to COVID-19[94]. **Singapore** introduced the *Online Falsehoods and Manipulation Act* (POFMA) criminally charging anyone convicted of knowingly spreading "false statements"[95].

Other jurisdictions are requiring social platforms to embed new design features into their services, akin to the automobile industry introducing airbags and seatbelts into vehicles in previous generations. **California** has introduced the *Age Appropriate Design Code Act*, which introduces measures to protect children's privacy and personal information, and limit the types of content children are exposed to by, for example, blocking age inappropriate advertisements. The law follows the UK's approach, which introduced a Children's code in 2021[96], and recently passed into law its Online Safety Bill that, among its various provisions, requires platforms to remove certain types of misinformation.

The most significant legislative initiative to date for regulating social platforms is the European Union's Digital Services Act (DSA), passed in 2022, which introduces several measures to mitigate illegal content online including by establishing platform transparency requirements around recommendation systems, obligations to share data with researchers to better understand online harms, independent audits of platforms to assess risk of harm of platform activities and creating a mechanism for trusted flaggers of disinformation[97]. **Australia** also has had a voluntary code of conduct on disinformation for online platforms since 2021, and is currently considering legislation that targets it more directly through the *Combating Misinformation and Disinformation Bill*, 2023.

3.3 Monitor Social Platforms' Performance in Reducing Disinformation

Social media platforms are constantly refining and changing their products, in response to changing user demands, legal and regulatory requirements, or public pressures regarding issues like disinformation spread. Corporate leaders should stay abreast of these changes and understand their business impacts.

Platform's terms of use and community standards for users, and their content moderation and enforcement operations, are critical in addressing disinformation and other harms on platforms. Platforms can remove content and user accounts who repeatedly spread disinformation, particularly illegal disinformation such as identity fraud. However, concerns remain over users recreating accounts or moving to other more smaller networks with little to no content moderation[98]. Businesses should monitor changes in these policies, and can engage platforms to report violations. Businesses can do so by establishing closer relationships and partnerships with researchers, universities, tech companies and industry associations. Companies can also hire individuals with expertise at the intersections of technology, policy and geopolitics.

Platforms can deploy other technological interventions to mitigate the spread of disinformation, both proactively and reactively. This includes:

Inoculation, a proactive approach based on the premise that individuals can be protected from believing in disinformation by viewing examples of it beforehand[99]. This can, for instance, take the form of short videos on social media on how users may be manipulated and to learn to distinguish between true and false content[100]. In research, the strategy has shown promising results, but questions remain over scalability.

Accuracy nudges, a proactive intervention to encourage users to verify information they encounter online, on the premise that users will not knowingly share content they believe is false. Nudges encourage users to slow down and think about the veracity of information they encounter before they share or repost. During the COVID-19 pandemic, X (then Twitter) and Instagram made platform changes to nudge users to find credible sources when encountering health related content[101]. Although studies reveal mixed results, researchers believe the effects could be meaningful if scaled across social media and used alongside other tools and interventions[102].

Algorithmic controls are another proactive intervention platforms can make to deprioritize and reduce the visibility of content that has been independently verified as disinformation[103].

Warning labels are a reactive intervention, applied after a particular piece of content has been fact-checked or determined to be synthetic or a deep fake. Some applications of warning labels are labour intensive, relying on human intervention thus limiting its scalability[104]. Other forms that rely more on automation, like machine learning, raise questions over consistency, reliability and efficacy[105].

Summary of Actions Companies Can Take:

7. **Monitor which social platforms are best applying terms of use policies** and content moderation, and other technical interventions, to actively combat disinformation *(can be part of the social media monitoring action in section 3.3)*.

8. **Leverage advertising spend**, directing online marketing resources to platforms that are limiting disinformation and create the least risk to the company and corporate brand.

9. **Engage directly with social platforms** in the event the company is targeted with disinformation, to seek rapid moderation and take-down of content that violates platform terms of use *(can be part of incident response activities outlined in section 3.3)*.

4. Conclusion

While disinformation can spread through various communications mediums, rapid digitization and social media have enabled threat actors with a diversity of malicious objectives to spread false information at unprecedented speeds and volumes, at negligible cost. New technology, like generative AI, will amplify this trend. While disinformation has traditionally been viewed primarily as a threat in the context of geopolitical competition, democracy and electoral processes, or the direct public safety of citizens, another important category of threat is to Canada's companies, large and small.

This white paper outlines the various types of threat actors and motivations for targeting Canadian companies, the online tools and tactics they are using, and the ways consumers report experiencing disinformation. It also describes the ways companies themselves use disinformation to advance their own strategic interests. Where companies are targeted, disinformation has the potential to negatively impact brand reputation, consumer trust, and share prices, as well as workplace productivity, culture and cohesion. Disinformation is also increasingly recognized as a threat to Canada's national and economic security.

Yet, companies are not defenceless in confronting this threat. The white paper also outlines several proactive steps firms can take. First, they can track and engage in the policy and regulatory processes underway to address online harms and disinformation in Canada and in other jurisdictions. Second, they can monitor social platforms' performance in addressing disinformation and creating a safe environment for corporate brands, corporate communication and online advertising. Third, and most important, companies can establish internal policies and capabilities for responding directly to malicious disinformation that targets them.

As a final note, industry leaders must recognize that disinformation is a threat not just to their companies and the bottom line, but to Canada's economy, democracy and social cohesion. The erosion of trust in markets, democratic institutions and the bonds of citizenry all undermine the operating environment for Canada's businesses, not to mention the country itself. In sum, Canadian businesses have a big stake in combatting disinformation and ensuring a safe, secure and trustworthy information ecosystem for all.

Acknowledgements

Authors

Joe Masoodi focuses on public policy issues related to new and emerging technologies. His research interests are situated at the intersection of surveillance, security and human rights. Joe has conducted research and written on the risks and implications of disinformation and online harms, contact tracing apps, facial recognition and workplace surveillance.

André Côté is a mission-driven consultant offering strategic advice, research and other services to a range of clients, and has acted as a senior advisor to the Deputy Premier of Ontario and the Minister of Advanced Education and Skills Development. André is the former Chief Operating & Strategy Officer with NEXT Canada, a national non-profit incubator for entrepreneurs and start-ups. He is an experienced ed tech innovator, having worked with Toronto Metropolitan University's Leadership Lab and as a former Board Member with eCampus Ontario. André is the current Director of Policy & Research and Head of Secure & Responsible Tech Policy Program at The Dais, Toronto Metropolitan University.

Toronto Metropolitan University

ROGERS cybersecure catalyst

Rogers Cybersecure Catalyst is Toronto Metropolitan University's national centre for training, innovation and collaboration in cybersecurity. Headquartered in Brampton, Ontario, and offering programs and services across Canada, the Catalyst empowers individuals and organizations to seize the opportunities and tackle the challenges of cybersecurity.

Toronto Metropolitan University

the dais

The Dais is Canada's platform for bold policies and better leaders. We are a public policy and leadership think tank at Toronto Metropolitan University, connecting people to the ideas and power we need to build a more inclusive, innovative, prosperous Canada.

How to Cite this Report:

Joe Masoodi and André Côté, Understanding and Responding to Disinformation Targeting Canadian Companies. Toronto Metropolitan University, May 2024.

350 Victoria St, Toronto, ON M5B 2K3

This project was supported by:

RBC®

Contributors and Reviewers:

Charles Finlay
Judith Borts
Sumit Bhatia

References

1 Brennen, J. Scott. "Misinformation: The evidence on its scope, how we encounter it, and our perceptions of it." Reuters Institute, University of Oxford. April 18, 2019. https://reutersinstitute.politics.ox.ac.uk/news/misinformation-evidence-its-scope-how-we-encounter-it-and-our-perceptions-it.

2 Wardle, Claire. "Understanding information disorder." First Draft News. September 22, 2020. https://firstdraftnews.org/long-form-article/understanding-information-disorder/.

3 Andrey, Sam. Online Harms. Toronto: The Dais, 2023. https://dais.ca/reports/survey-of-online-harms-in-canada/.

4 Miro-Llinares, Fernando, and Jesús C. Aguerri. "Misinformation about fake news: A systematic critical review of empirical studies on the phenomenon and its status as a 'threat'." European Journal of Criminology 20, no. 1 (April 2021): Pp.1-19. doi:10.1177/1477370821994059.

5 Business Council of Canada. Economic security is national security: the case for an integrated Canadian strategy.

6 Atkinson, Claire. "Fake news can cause 'irreversible damage' to companies – and sink their stock price." NBC news. April 25, 2019. https://www.nbcnews.com/business/business-news/fake-news-can-cause-irreversible-damage-companies-sink-their-stock-n995436

7 Andrey, Sam. Online Harms. Toronto: The Dais, 2023. https://dais.ca/reports/survey-of-online-harms-in-canada/

8 See Shahbaz, Funk, Brody, Vesteinsson, Baker, Grothe, Barak, Masinsin, Modi, Sutterlin eds. "Freedom on the Net 2023: The Repressive Power of Artificial Intelligence." Freedom House, 2023. freedomonthenet.org; and Gartner. "Gartner Predicts 50% of Consumers Will Significantly Limit Their Interactions with Social Media by 2025." December 14, 2023. https://www.gartner.com/en/newsroom/press-releases/2023-12-14-gartner-predicts-fifty-percent-of-consumers-will-significantly-limit-their-interactions-with-social-media-by-2025

9 Thompson, Stuart A. "Test Yourself: Which Faces were Made by AI?" New York Times. January 19, 2024. https://www.nytimes.com/interactive/2024/01/19/technology/artificial-intelligence-image-generators-faces-quiz.html

10 The survey was conducted online via the Ipsos I-Say panel in English and French, from August 14 to August 17, 2023. The margin of error for a comparable probability-based sample is +/-2.9 percentage points, 19 times out of 20

11 Levi, Simona. FakeYou: Fake News y Desinformación. Barcelona, Spain: Rayo Verde Editorial, 2021

12 Bradshaw, Samantha. "Influence Operations and Disinformation on Social Media." CIGI. November 23, 2020. https://www.cigionline.org/articles/influence-operations-and-disinformation-social-media

13 Bradshaw, Samantha. "Influence Operations and Disinformation on Social Media." CIGI. November 23, 2020. https://www.cigionline.org/articles/influence-operations-and-disinformation-social-media

14 Ibid

15 Wardle, Claire. "Understanding information disorder." First Draft News. September 22, 2020. https://firstdraftnews.org/long-form-article/understanding-information-disorder/

16 Wardle, Claire, & Hossein Derakhshan. Thinking about 'information disorder': Formats of misinformation, disinformation, and malinformation. In Journalism, fake news & disinformation: Handbook for journalism education and training. Paris: UNESCO, 2018 https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf

17 Lim, Gabrielle, and Joan Donovan. "The Internet is a Crime Scene." Foreign Policy. January 20, 2021. https://foreignpolicy.com/2021/01/20/internet-crime-scene-capitol-riot-data-information-governance/

18 Wardle, Claire. "Understanding information disorder." First Draft News. September 22, 2020. https://firstdraftnews.org/long-form-article/understanding-information-disorder/

19 See Canadian Centre for Cyber Security. "National Cyber Threat Assessment 2023-2024." 2022. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

20 Caramancion, Kevin Matthe, Yueqi Li, Elisabeth Dubois, and Ellie Seoe Jung. "The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats." Data 7, no. 4: 49. 2022. https://doi.org/10.3390/data7040049

21 See Andrey, Sam. "Survey of Online Harms in Canada." The Dais, March 2023. https://dais.ca/reports/survey-of-online-harms-in-canada/; and Meta. "Policies." Transparency Centre, accessed March 2024 https://transparency.fb.com/policies/community-standards/misinformation

22 Canadian Centre for Cyber Security. "National Cyber Threat Assessment 2023-2024." 2022. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

23 See Edelman. "2024 Edelman Trust Barometer - Canada." March 2024 https://www.edelman.ca/trust-barometer/2024-edelman-trust-barometer

24 PwC. "Disinformation attacks have arrived in the corporate sector. Are you ready?" February 2021. https://www.pwc.com/us/en/tech-effect/cybersecurity/corporate-sector-disinformation.html

25 Communications Security Establishment. National Cyber Threat Assessment 2023-2024. Ottawa: Canadian Centre for Cyber Security, 2022. https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf

26 Cadwalladr, Carole. "The Great British Brexit robbery: How our democracy was hijacked." The Guardian. May 7, 2017. https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

27 Borgesius, Frederik J. Zuiderveen., Judith Moller, Sanne Kruikemeier, Ronan Ó Fathaigh, Kristina Irion, Tom Dobber, Balazs Bodo & Claes de Vreese. "Online political microtargeting: Promises and threats for democracy." Utrecht Law Review 14, no.1 (February 2018): 82-96. doi:10.18352/ulr.420

28 Al-Jizawi, Noura, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft & Ron Deibert. Psychological and emotional war: digital transnational repression in Canada. Toronto: Citizen Lab, University of Toronto, 2022. https://citizenlab.ca/2022/03/psychological-emotional-war-digital-transnational-repression-canada/

29 Barnes, Julian E & David E. Sanger. "Russian Intelligence Agencies Push Disinformation on Pandemic." The New York Times. July 28, 2020. www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html

30 Communications Security Establishment. National Cyber Threat Assessment 2023-2024. Ottawa: Canadian Centre for Cyber Security, 2022. https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf

31 Ibid

32 Mandiant, "Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance", (June 28, 2022) https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies

33 Sharevski, Filipo & Kessell, Benjamin. (2023). Fight Fire with Fire: Hacktivists' Take on Social Media Misinformation. https://doi.org/10.48550/arXiv.2302.07788

34 Communications Security Establishment. "Cyber Threats to Canada's Democratic Process. Government of Canada." 2018. https://www.cyber.gc.ca/sites/default/files/cyber/publications/cse-cyber-threat-assessment-e.pdf

[35] Lorenzo Franceschi-Bicchierai. "Meet the environmental hacktivists trying to 'sabotage' mining companies.' Vice. (2022, Aug 16). https://www.vice.com/en/article/5d39j3/meet-the-environmental-hacktivists-trying-to-sabotage-mining-companies

[36] Tunney, Catherine. Intelligence agency calls for a 'heightened state of vigilance' against Russian-aligned hacks. CBC. (2023, Jan 26). https://www.cbc.ca/news/politics/cse-russia-ukraine-tanks-killnet-1.6727393

[37] Guy, Jack. "Ryanair fires staff for allegedly faking photo of sleeping on airport floor," CNN. (2018, Nov 7). https://www.cnn.com/2018/11/07/europe/ryanair-photo-staff-sacked-scli-intl/index.html

[38] Balaban, David. "Social engineering and the disinformation threat in cybersecurity," Forbes. (2023, Jun 16). https://www.forbes.com/sites/davidbalaban/2023/06/16/social-engineering-and-the-disinformation-threat-in-cybersecurity/

[39] European Union Agency for Cybersecurity. "What is social engineering," ENISA. (n.d.). https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

[40] Margi Murphy, "Attacking the help desk: how attackers talk their way into company networks." Bloomberg. (October 3, 2023). https://www.bloomberg.com/news/articles/2023-10-03/mgm-cyberattack-shows-how-hackers-deploy-social-engineering

[41] Balaban, David. "Social engineering and the disinformation threat in cybersecurity,"

[42] Antoniuk, Daryna. "Russian hacking tool floods social networks with bots, researchers say," The Record. (2023, Oct 30). https://therecord.media/russian-hacking-tool-creates-bots

[43] OECD. "Disinformation and Russia's War of Aggression against Ukraine: Threats and Governance Responses." OECD. (2022, Nov 22). https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/

[44] Andrey, Sam. Online Harms. Toronto: The Dais, 2023. https://dais.ca/reports/survey-of-online-harms-in-canada/

[45] Ibid

[46] Hameleers, Michael, Toni van der Meer, & Rens Vliegenthart. "Civilized truths, hateful lies? Incivility and hate speech in false information – evidence from fact-checked statements in the US," Information, Communication & Society 25, no. 11 (2020): 1596–1613. https://doi.org/10.1080/1369118X.2021.1874038

[47] Kozyreva, Anastasia, Stephan Lewandowsky, S, & Ralph Hertwig. "Citizens Versus the Internet: Confronting Digital Challenges With Cognitive Tools," Psychological Science in the Public Interest 21, no. 3 (2020): 103–156. https://doi.org/10.1177/1529100620946707

[48] Hagey, Keach & Jeff Horwitz. "Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead. Internal memos show how a big 2018 change rewarded outrage and that CEO Mark Zuckerberg resisted proposed fixes." Wall Street Journal (Online). September 15, 2021. https://www.proquest.com/docview/2572526410/citation/8ECA31679DEF4C74PQ/1

[49] Ibid

[50] Ibid

[51] Masoodi, Mohammed Joe & Sam Andrey. "Understanding the Use of Private Messaging Apps in Canada and Links to Disinformation," IEEE Technology and Society Magazine 41, no. 3 (2022): 58-70

[52] Ibid

[53] Ibid

[54] Stecula, Domink, Mark Pickup, and Clifton van der Linden. "Who believes in COVID-19 conspiracies and why it matters." Policy Options. July 6, 2020. https://policyoptions.irpp.org/magazines/july-2020/who-believes-in-covid-19- conspiracies-and-why-it-matters/

[55] Silverman, Craig & Jeff Kao. "Infamous Russian Troll Farm Appears to be Source of Anti-Ukraine Propaganda." ProPublica. March 11, 2022. https://www.propublica.org/article/infamous-russian-troll-farm-appears-to-be-source-of-anti-ukraine-propaganda

[56] Ferrara, Emilio, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini. "The Rise of Social Bots." Communications of the ACM 59, no.7 (2016), 96–104. doi.org/10.1145/2818717

[57] Maria Aspan. "The Trolling of Corporate America." Forbes. October 2, 2023. https://fortune.com/2023/10/02/the-trolling-of-corporate-america/

[58] Douek, Evelyn. "What does "Coordinated Inauthentic Behavior" Actually Mean?" Slate. July 2, 2020. https://slate.com/technology/2020/07/coordinated-inauthentic-behavior-facebook-twitter.html

[59] Roush, Ty. "Meta Removes Over 7500 accounts Linked to Chinese Influence Campaign." Forbes. August 29, 2023. https://www.forbes.com/sites/tylerroush/2023/08/29/meta-removes-over-7500-facebook-accounts-linked-to-chinese-influence-campaign/?sh=34336f972cff

[60] Fisher, Max. "Disinformation for hire, a shadowy industry is quietly booming," New York Times. (2021, Jul 25). https://www.nytimes.com/2021/07/25/world/europe/disinformation-social-media.html

[61] Brewster, Thomas. "Fraudsters cloned company director's voice in $35 million heist, police find," Forbes. (2021, Oct 14). https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=654a80a17559

[62] See Kane, Edward J. 2003. "Continuing Dangers of Disinformation in Corporate Accounting Reports." NBER Working Paper 9634, National Bureau of Economic Research, Cambridge, MA; and Brah, Elizabeth. "Corporations Are Juicy Targets for Foreign Disinformation," FP. December 5, 2023.

[63] Dishman, Paul & Philip Nitse. "Disinformation Usage in Corporate Communications: CI'ers Beware". Competitive Intelligence Review 10, no.4 (January 2001): pp. 20–29. doi:10.1002/(SICI)1520-6386(199934)10:4<20::AID-CIR5>3.0.CO;2-L

[64] Reid, Aaron. "What's the damage? Measuring the impact of fake news on corporate reputation can act as a guide for companies to navigate a post-truth landscape." Communication Director. January 17, 2017. https://www.communication-director.com/issues/fake-news-real-threats/whatsdamage#.W7xY73szaii

[65] Rodríguez-Fernández, Leticia. "Disinformation and organisational communication: A study of the impact of fake news". Revista Latina de Comunicación Social, (2019): pp.1-19. doi:10.4185/RLCS-2019-1406en

[66] Ibid

[67] Reid, Aaron. "What's the damage? Measuring the impact of fake news on corporate reputation can act as a guide for companies to navigate a post-truth landscape." Communication Director. January 17, 2017. In Rodríguez-Fernández, Leticia. "Disinformation and organisational communication: A study of the impact of fake news". Revista Latina de Comunicación Social, (2019): p. 4

[68] Jonathan Monpetit. "Bell media, Angus reid, and other Canadian brands halt ads on X amid extremism concerns," CBC. (2023, Dec 12). https://www.cbc.ca/news/canada/canadian-brands-advertising-x-extremism-1.7055823

[69] Rodríguez-Fernández, Leticia. "Disinformation and organisational communication: A study of the impact of fake news"

[70] Sharevski, Filipo & Kessell, Benjamin. "Fight Fire with Fire: Hacktivists' Take on Social Media Misinformation."(2023)

[71] Ryan Mac., et al. "A verifiable mess: Twitter users create havoc by impersonating brands," New York Times. https://www.nytimes.com/2022/11/11/technology/twitter-blue-fake-accounts.html

72 Chloe Taylor. "Workers are avoiding their colleagues because of conflicting political views and employers are afraid to choose sides HR expert says," Fortune. https://fortune.com/2022/07/27/workers-avoiding-colleagues-conflicting-political-views-employers-afraid-choose-sides-gartner/

73 Stephanie Papas. "What employers can do to counter election misinformation in the workplace," American Psychological Association. (2022, Nov 4). https://www.apa.org/topics/journalism-facts/workplace-fake-news

74 Terri Tompkins and Bruce Barkis. "Conspiracies in the workplace: symptoms and remedies," GBR, 24, no.1 (2021). https://gbr.pepperdine.edu/2021/03/conspiracies-in-the-workplace/

75 Andrey, Sam. Online Harms. Toronto: The Dais, 2023. https://dais.ca/reports/survey-of-online-harms-in-canada/

76 It is unclear why respondents from the Prairies report higher levels of harmful content and is worth exploring further in research

77 Alim, Arjun Neil, Michael O'Dwyer, and Leo Lewis. "Companies on the hunt for geopolitical advice as tensions rise." Financial Times. October 17, 2023. https://www.ft.com/content/608a43e2-710c-4918-84d6-e0d75511918e

78 Matthew, Ferraro. "Disinformation is harming businesses. Here are 6 ways to fight it." CNN. June 10, 2019. https://www.cnn.com/2019/06/10/perspectives/disinformation-business/index.html

79 Government of Canada. "Countering Disinformation: A Guidebook for Public Servants." Democratic Institutions. February 2024. https://www.canada.ca/en/democratic-institutions/services/protecting-democratic-institutions/countering-disinformation-guidebook-public-servants.html#toc6

80 Government of the UK. "RESIST 2 Counter Disinformation Toolkit." Government of the UK. January 11, 2022. https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/

81 PwC. "Disinformation attacks have arrived in the corporate sector. Are you ready?" February 2021. https://www.pwc.com/us/en/tech-effect/cybersecurity/corporate-sector-disinformation.html

82 Glasner, Joanna. "It's no lie: Startups fighting disinformation are raking in cash." Crunchbase News. February 14, 2023. https://news.crunchbase.com/ai-robotics/venture-startups-disinformation-primer-vinesight/

83 Eddy, Melissa. "A new place to learn civics: the workplace." New York Times. October 29, 2023. https://www.nytimes.com/2023/10/29/world/europe/businesses-civics-education.html

84 Business Council of Canada. Economic security is national security: the case for an integrated Canadian strategy. Business Council of Canada, 2023

85 Canadian Constitution Foundation v. Canada (Attorney General), 2019 ONSC 5795; Budget Implementation Act, Statutes of Canada 2021, c. 23 (Division 36). https://laws-lois.justice.gc.ca/eng/AnnualStatutes/2021_23/page-30.html#h-129

86 See Government of Canada. "Proposed Bill to Address Online Harms." 26 February 2024. https://www.canada.ca/en/canadian-heritage/services/online-harms.html

87 Guest, Peter. "The UK is poised to force a bad law on the internet." Wired. September 6, 2023. https://www.wired.com/story/the-uk-is-poised-to-force-a-bad-law-on-the-internet/

88 "Canada Declaration on Electoral Integrity Online." Government of Canada. August 18, 2021. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/declaration-electoral-integrity.html

89 "Critical Election Incident Public Protocol." Government of Canada. September 7, 2021. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol.html

90 Platt, Brian. "The 'Critical Election Incidents' protocol: How the government plans to fight against interference in the election." National Post. July 9, 2019. https://nationalpost.com/news/politics/the-critical-election-incidents-protocol-how-the-government-plans-to-fight-against-interference-in-the-election

91 "Combatting foreign interference." Government of Canada. March 19, 2020. https://www.canada.ca/en/democratic-institutions/news/2019/01/combatting-foreign-interference.htm

92 "Backgrounder - Helping Citizens Critically Assess and Become Resilient Against Harmful Online Disinformation." Canadian Heritage. June 28, 2022. https://www.canada.ca/en/canadian-heritage/news/2019/07/backgrounder--helping-citizens-critically-assess-and-become-resilient-against-harmful-online-disinformation.html

93 Tworek, Heidi, & Paddy Leerssen. "An analysis of Germany's NetzDG law." Translantic High Level Working Group on Content Moderation Online and Freedom of Expression (April 2019). https://dare.uva.nl/search?identifier=3dc07e3e-a988-4f61-bb8c-388d903504a7

94 Schuldt, Lasse. "The rebirth of Malaysia's fake news law – and what the NetzDG has to do with it." Verfassungs Blog. April 13, 2021. https://verfassungsblog.de/malaysia-fake-news/

95 Protection from Online Falsehoods and Manipulation Act 2019, Singapore Statutes Online. https://sso.agc.gov.sg/Act/POFMA2019?TransactionDate=20191001235959

96 Denham, Elizabeth and Jonathan Tam. "UK and California Age Appropriate Design Rules: Similar principles, subtle difference." IAPP. April 25, 2023. https://iapp.org/news/a/uk-and-california-age-appropriate-design-rules-similar-principles-subtle-differences/

97 European Commission. "The Digital Services Act." European Commission. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

98 Honigberg, Brad. "Why Deplatforming Just Isn't Enough." Center for Strategic & International Studies (blog). February 11, 2021. https://www.csis.org/blogs/strategic-technologies-blog/why-deplatforming-just-isnt-enough

99 Van der Linden, Sander. Foolproof: Why Misinformation Infects Our Minds and How to Build Immunity. W.W. Norton & Company, 2023

100 Roozenbeek, Jon, Sander Van Der Linden, Beth Goldberg, Steve Rathje & Stephan Lewandowsky. "Psychological inoculation improves resilience against misinformation on social media." Sciences Advances 8, no.34 (2022).DOI:10.1126/sciadv.abo6254

101 Ampolpittayanant, Monrawee and Agung Yudha. "Helping you find reliable public health information on Twitter." Twitter (blog). December 20, 2019. https://blog.twitter.com/en_sea/topics/company/2019/Helping-you-find-reliable-public-health-information-on-Twitter

102 Van der Linden, Sander., and Jon Roozenbeek. "Fake news: a simple nudge isn't enough to tackle it – here's what to do instead." The Conversation. June 11, 2021. https://theconversation.com/fake-news-a-simple-nudge-isnt-enough-to-tackle-it-heres-what-to-do-instead-162454

103 Krishnan, Nandita, Jiayan Gu, Rebekah Tromble, Lorien C. Abroms. "Research note: Examining how various social media platforms have responded to COVID-19 misinformation." Harvard Kennedy School (HKS) Misinformation Review, (December 2021). doi:10.37016/mr-2020-85

104 Thornhill, Calum, Quentin Meeus, Jeroen Peperkamp & Bettina Berendt. "A Digital Nudge to Counter Confirmation Bias." Front. Big Data 2, no.11 (June 2019). doi: 10.3389/fdata.2019.00011

105 Roozenbeek, Jon, Eileen Culloty & Jane Suiter. "Countering misinformation: Evidence, knowledge gaps, and implications of current interventions." European Psychologist, 28, no.3, (2023): 189–205. https://doi.org/10.1027/1016-9040/a000492

the dais

Toronto
Metropolitan
University

ROGERS
cybersecure
catalyst