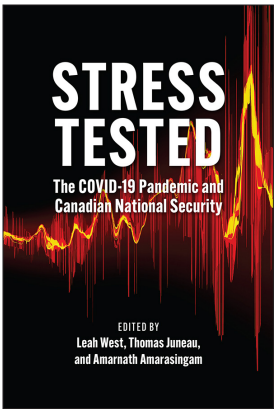
UNIVERSITY OF CALGARY
Press



STRESS TESTED: THE COVID-19 PANDEMIC AND CANADIAN NATIONAL SECURITY

Edited by Leah West, Thomas Juneau, and Amarnath Amarasingam

ISBN 978-1-77385-244-7

THIS BOOK IS AN OPEN ACCESS E-BOOK. It is an electronic version of a book that can be purchased in physical form through any bookseller or on-line retailer, or from our distributors. Please support this open access publication by requesting that your university purchase a print copy of this book, or by purchasing a copy yourself. If you have any questions, please contact us at ucpress@ucalgary.ca

Cover Art: The artwork on the cover of this book is not open access and falls under traditional copyright provisions; it cannot be reproduced in any way without written permission of the artists and their agents. The cover can be displayed as a complete cover image for the purposes of publicizing this work, but the artwork cannot be extracted from the context of the cover of this specific work without breaching the artist's copyright.

UNIVERSITY OF CALGARY
Press
press.ucalgary.ca

Acknowledgement: *We acknowledge the wording around open access used by Australian publisher,* **re.press**, *and thank them for giving us permission to adapt their wording to our policy* http://www.re-press.org

2

Exploiting Chaos: How Malicious Non-state Actors Leverage COVID-19 to Their Advantage in Cyberspace

Casey E. Babb and Alex S. Wilner

Introduction

Since the beginning of 2020, while societies and economies around the world have struggled to cope with the realities of the COVID-19 pandemic, cyberspace has given governments, businesses, and general end-users the ability to work, play, and connect in new and innovative ways. With everything from workspaces and classrooms to family gatherings and exercise routines forced online, the Internet has enabled people across the globe to carry on and maintain a sense of normalcy during very abnormal times.

However, at the same time, while the world has been focused on the health, economic, political, and social ramifications of the pandemic, terrorist organizations, fringe groups, and extremist communities around the world have become emboldened, finding opportunity to exploit the situation, incite hate, (re)mobilize, and promote their ideologies online in novel ways. These groups—which we loosely classify as malicious non-state actors for the purposes of this chapter—have been primarily focused on exploiting and contributing to the diffusion of information during the pandemic for their own strategic gain. These actors are not primarily interested in for-profit criminal activities, but rather seek to weaponize the information environment toward other objectives. From synagogues and

Jewish organizations worldwide being "Zoom bombed" with antisemitic messages (Schiffer 2020), to the Islamic State and al-Qaeda suggesting online that martyrs are immune to the virus (Hunter 2020) or that the coronavirus is a divine punishment targeting non-believers (Hanna 2020), to white supremacist groups using platforms such as Telegram and Gab to spread propaganda (Perrigo 2020), COVID-19 has added a new dimension to malicious online activities. Indeed, the European Union's counterterrorism chief, the US Department of Homeland Security, the US National Counterterrorism Center, and the Federal Bureau of Investigation (FBI), among others, have all issued statements warning of the potential ways militant and extremist groups are leveraging the pandemic to their advantage (Baker 2020; Bertrand 2020; FBI 2020).

Surprisingly, aside from a handful of senior-level government speeches highlighting these trends, comparatively little has been said about these challenges in Canada, despite the government having become increasingly concerned with individuals and groups who espouse extremist views, spread propaganda, and promote violence online (CSIS 2019; Vigneault 2021; Public Safety Canada 2019). The current situation compels us to explore a central question: How are malicious non-state actors using cyber space to exploit the pandemic for their own strategic gain, and what might these trends mean for Canada's national security over the coming years? Informed primarily by international trends, the intent of this chapter is threefold. First, it will serve as a primer on how various types of dangerous non-state actors are manipulating the information environment and exploiting increased user connectivity for strategic gain. Specifically, we have homed in on three distinct yet overlapping online trends that have proven to be particularly detrimental to national security: delegitimation, recruitment, and incitement. Second, we provide a concise snapshot of what these trends may mean for Canada, and how some of these online activities have or could take shape domestically. Third, we hope our analysis will support the Government of Canada in the years to come as it assesses the national security implications and fallout from the pandemic and develops appropriate policy responses and mitigation strategies for addressing nefarious online activities.

Hostile Cyber Activities: Types and Trends

On 15 February 2020, Tedros Adhanom Ghebreyesus, Director General of the World Health Organization, noted that the world was not only fighting an epidemic—it was "fighting an infodemic" (Ghebreyesus 2020). Indeed, since the onset of COVID-19, the Internet and social media have facilitated the global circulation and proliferation of an unprecedented amount of problematic information. "Crisis informatics"—which is the interdisciplinary academic study of how people rely on technology to cope with and respond to uncertainties—suggests that to a degree, this is to be expected (Starbird 2020). When information is sparse or conflicting, it is natural that people will look to fill the information gap, ease their anxieties, get answers, and participate in a sort of "collective sensemaking" (Stephens et al. 2020). However, the extent to which we are witnessing disinformation, misinformation, and individuals intentionally capitalizing on the information void is unique, both in terms of volume and in the ways in which this online discourse has been injurious to national security. In part, this is a result of worldwide social distancing measures and a surge in user engagement with online technologies. This has led to a proliferation of online groups and communities dedicated to COVID-related conspiracy theories, anti-science discourse, and fighting government regulations during the pandemic. In some cases, the distinction between anti-lockdown measures and broader anti-government rhetoric has been blurred, with deadly consequences. The storming of the United States Capitol on 6 January 2021—seemingly instigated, abetted, and encouraged by former President Donald Trump—is a case in point: dis- and misinformation mixed with real and perceived individual and group grievances led to physical altercations, violence, and mayhem.[1]

That said, for the purposes of this chapter, we have identified a number of distinct yet complementary and overlapping types of information circulating online during the pandemic, which academics, health-care professionals, and policy-makers should monitor and study further as the pandemic drags on and, perhaps more importantly, once it ends. Doing so may enable the government to better understand the long-term residual effects of these activities while also providing online users and consumers with greater knowledge with which to identify and combat inaccurate and

potentially dangerous information during future large-scale crises and disasters. In this context, what follows is a discussion of three different forms of pandemic-related (or pandemic-induced) extremist information and activity, categorized as delegitimation, recruitment, and incitement.

Delegitimation

Throughout the last year, governments and authorities around the world have faced extraordinary pressure. Not only have they had to deal with containing the virus, they have also had to defend their public health measures and the subsequent economic repercussions those measures may have created. In some instances, governments have failed to (expeditiously) recognize the seriousness of the virus, while others have struggled to cope with the fallout. Either way, authorities everywhere have faced unprecedented scrutiny. As a result, various types of malicious non-state actors have used social media and messaging apps to capitalize on the situation and further delegitimize governments. In some cases, they have provided goods and services where the state has failed, while in other instances they have provided support for people and communities affected by strict public health measures (Hegazi 2020; Heffes and Somer 2020). Strategically, this type of activity serves at least two primary purposes. First, it delegitimizes and undermines trust in governments and authorities in affected areas, sowing distrust, chaos, and division. Second, it legitimizes whichever group has stepped up to provide support while also reinforcing their extremist narratives and recruitment strategies (Binetti et al. 2020; Daymon 2020).

Illustrations of this kind of activity abound; consider these disparate examples. Al-Shabaab, al-Qaeda's branch in Somalia, used various platforms to blame the African Union Mission in Somalia and the "international crusaders" for bringing the virus to Africa (Joscelyn 2020). Likewise, Nigeria's Boko Haram has suggested through audio recordings disseminated online that "infidels" such as Muhammadu Buhari, the President of Nigeria, Idris Deby, the former President of Chad, and Muhammed Issoufu, the President of Niger, are responsible for the virus, which is God's punishment against non-believers and secular Muslims (Campbell 2020). In Afghanistan, the Taliban have taken a different approach, launching a public-health-awareness campaign, publicly signalling via Twitter their willingness to co-operate with international health

organizations, and using other online platforms such as WhatsApp to share images of government health-care workers assisting patients (Kapur and Saxena 2020). The Islamic State of Iraq and Syria (ISIS or Daesh, in its Arabic acronym) has also tapped into social media and online publications to discredit governments, arguing that these governments have intentionally withheld information on the virus from citizens, while presenting themselves as a better alternative to imposed public health measures (Phelan et al. 2020). Similarly, in Mexico, international criminal groups and syndicates, such as the Gulf Cartel, have distributed aid boxes in territories they control or seek to control bearing labels with the names and logos of the different groups; these efforts are then promoted on social media (Binetti et al. 2020; Cordoba 2020). Similarly, videos showing Alejandrina Giselle Guzman Salazar, daughter of drug lord Joaquin "El Chapo" Guzman, providing aid packages to those in need were widely circulated on Facebook (Jorgic 2020).

Far-right groups in Italy, Germany, the Netherlands, Austria, Spain, Belgium, France, and elsewhere have undertaken similar strategies, using social media to publicize their alternative economic support efforts while espousing anti-government rhetoric, which in many cases is also being supported by far-right nationalist parties to which they have links (Youngs 2020). In the United States and Canada, far-right extremist groups like the Proud Boys, the Three Percenters, and the Oath Keepers, as well as other loosely organized or affiliated organizations, have used social media and other fringe platforms like Telegram and Gab to fuel a range of anti-government conspiracy theories. On the Telegram messenger app, experts have also identified "accelerationists"—those who seek to erode liberal democracy in order to develop white ethnostates—and "ecofascists"—who extol genocidal solutions to environmental problems. Both groups continually and openly discuss recruitment strategies, white supremacy, and anti-government ideologies (Wilson 2020). That said, conspiratorial messaging, hate speech, and extremist rhetoric is not exclusive to the far right. During the pandemic, far-left movements—who use the same social media, encrypted networks, and messaging apps to spread their messages—have also capitalized on increased Internet usage and pandemic-related hardships and anxieties to aggressively push populist, anti-government, and anti-elite narratives. Often, this messaging is

antisemitic, conspiratorial in nature, and rooted in pre-existing beliefs that predate the pandemic. These include suggestions that Jews are part of a white majority establishment set on exploiting people of colour, or that Jews (and Israel) were involved in creating or spreading the virus and profiting from the vaccines (Schwartz 2020; Rowe 2020).

While the majority of damaging and disruptive online discourse related to the pandemic is conspiratorial in nature, its underlying anti-government messaging not only suggests that government responses to the pandemic are malevolent, but also that these fringe groups know the "real truth" about the pandemic. As Neil MacFarquhar (2020) has written, the pandemic has become a "battle cry" for US extremists: "various violent incidents have been linked to white supremacist or anti-government perpetrators enraged over aspects of the pandemic," including public health measures ranging from mask wearing and curfews to stay-at-home orders, state-wide lockdowns, and vaccine mandates and passports. Evidently, undermining trust and confidence in governments has been a key strategy of various groups who purport to be able to provide an alternative option.

Recruitment

Many of these same groups also use the pandemic as an opportunity to recruit new followers to their cause, movement, and organization, recruits who perceive these groups and their ideologies as "more capable or more honest than . . . governments" (Bloom 2020). Echoing this theme, the Soufan Center argued in April 2020 that "the fallout from the coronavirus pandemic is likely to provide a boost to extremists from across the ideological spectrum. COVID-19 is a rare event that offers a range of terrorist and extremist groups with an opening to bolster or promote their ideologies and narratives," expanding their base as a result (Soufan Center 2020).

For instance, the ISIS-affiliated Al-Qitaal Media Center shared a message in its online magazine suggesting that the virus is a divine punishment and that only true believers are immune (Binetti 2020). Likewise, ISIS has implied online that the virus is God's punishment for anyone who does not adhere to the group's interpretation of Islam, suggesting that individuals who join ISIS will develop a form of immunity (Qandil 2020). In Indonesia, Malaysia, and the Philippines, reports suggest there has been an uptick in ISIS propaganda and online recruitment efforts during

the pandemic, with one expert explaining that "the group is actively recruiting and indoctrinating supporters through online platforms such as Facebook" (Lee et al. 2020). Al-Qaeda has also claimed the virus is an expression of God's wrath, and a message to non-believers to turn (or return) to Islam (Qandil 2020).

Far-right extremists are likewise trying to capitalize on the pandemic for recruitment purposes. Groups including the Hundred-Handers and the Nordic Resistance Movement in Europe have been spreading conspiracy theories, hate speech, and xenophobic propaganda to attract new supporters (Dodd 2020). In fact, authorities in the United Kingdom have suggested that right-wing extremist groups, even more so than religiously inspired terrorist organizations, "have been much more pro-active during the lockdown to try and reach young people" (Smith 2020). In July 2020, the United Nations Security Council's Counter-Terrorism Committee Executive Directorate, whose member states include the United States, the United Kingdom, Ireland, France, Norway, and Estonia, among others, wrote in a "Trends Alert" that "extreme right-wing terrorist groups and individuals have sought to co-opt the pandemic, using conspiracy theories to attempt to radicalize, recruit and inspire plots and attacks" (CTED 2020). In Canada, researchers have also noticed a significant spike in engagement with far-right extremist material online, with weekly searches for "violent, far-right keywords" increasing by nearly 20 per cent following lockdowns across a number of major Canadian cities (Britneff 2020). Researchers at the UK-based Institute for Strategic Dialogue concur, finding nearly seven thousand right-wing extremist channels, pages, and individual accounts linked to Canadians across seven social media platforms, designed to mobilize, recruit new members, broadcast disinformation, and harass opponents, among other activities. Cumulatively, this content reached over eleven million users worldwide (Davey, Hart, and Guerin 2020).

In sum, the pandemic's toll since early 2020—reflected in such things as economic turmoil, job losses and unemployment, physical and social isolation, psychological, individual and communal hardship, political uncertainty and instability, and increased online activity and engagement—has created an ideal recruitment opportunity for many different types of malicious non-state actors. Taking advantage of our collective situation, various groups across the globe are broadcasting their message to an

expanding online community, hoping to identify and attract potential followers, broaden their appeal, and recruit new members along the way.

Inciting Violence and Intimidation

Finally, in addition to online efforts to delegitimize governments and recruit new members, many of these same groups have also used cyberspace during the pandemic to incite violence and intimidate opponents. For example, ISIS has publicly urged supporters to carry out attacks on "overburdened health care systems in various Western countries" (CEP 2020), while right-wing extremist groups in the United States and Europe have used social media to encourage biological attacks using the virus itself, with specific emphasis on the targeting of medical centres and minority communities (Avis 2020). Early reports also suggest that much of the violence that occurred during the January 2021 Capitol riots in Washington, DC, was openly and deliberately planned on far-right conspiratorial websites and forums such as Parler, Gab, TheDonald, and MeWe. Analysis conducted by Advanced Democracy found that over 80 per cent of the top posts on TheDonald the day of the riots featured calls for violence (Wamsley 2021). Likewise, the same researchers found that nearly fifteen hundred posts during the week leading up to the riots were from QAnon-related accounts. QAnon is a pre-pandemic, international, and largely far-right conspiracy theory that suggests that a cabal of Democratic-leaning, Satan-worshipping pedophiles are mobilized against President Trump (see Argentino and Amarasingam, this volume). Many of these posts had violent connotations and promoted acts of aggression. Similar videos shared via TikTok generated hundreds of thousands of views (Wamsley 2021). Anna Schecter has suggested that "right-wing extremists" were "using channels on the encrypted communication app Telegram to call for violence against government officials on January 20 [2021]," the day of President Biden's inauguration, "with some extremists sharing knowledge of how to make, conceal and use homemade guns and bombs" (Schecter 2021).

Research and reports suggest similar online discourse is also espoused in Canada, with a number of cases illustrating the dangerous, sometimes deadly linkages between violent language online and physical harm and attacks offline. For example, in Toronto in March 2020, Derek

Soberal, a founder of the Occupy Canada activist group, filmed himself on Facebook speaking about his political views before stabbing himself multiple times and setting himself on fire near a gas station. Evidence suggests his self-immolation was the result of his becoming engrossed by COVID-19 conspiracy theories (Bell 2020). In another episode, in July 2020, Corey Hurren, a reservist in the Canadian Armed Forces, breached the grounds of Rideau Hall with a loaded firearm; his intention was to arrest and/or harm Prime Minister Justin Trudeau. Hurren had apparently become fixated with QAnon conspiracy theories circulating online and had expressed an inability to cope with the government's lockdown measures (Brewster 2020; Tunney 2021). Hurren, who pled guilty to seven charges, was sentenced to six years in prison in March 2021 (Canadian Press 2021). In addition, in December 2020, a Toronto man who regularly posted antisemitic and racist conspiracy theories related to the pandemic was arrested in what the Toronto Police Service described as their "biggest single-day drug and firearm seizure" (Collen 2021). In his apartment, the suspect, Daniel Dubajic, had nearly fifteen thousand rounds of ammunition, sixty-five firearms, and millions of dollars' worth of narcotics. Also, in January 2020, a Quebec man linked to social media accounts that referred to COVID-19 as a "scamdemic" urged Canadians to "start shooting the police," and he spoke about storming Parliament to "clean up house." He was arrested with eighteen firearms in his possession (Bell 2021). There have also been other incidents in Western Canada with an apparent nexus to online conspiratorial and fabricated information: a Calgary man used Facebook to threaten purposefully spreading the virus to Indigenous communities (Fletcher 2020), and a Vancouver man attacked a ninety-two-year-old Asian Canadian (suffering from dementia) while shouting anti-Asian slurs related to COVID-19 (Young 2020).

These and other incidents point to the potential for online hate speech and conspiracy theories to motivate extremists to conduct or participate in acts of violence, a trend that long predates the pandemic. The difference today, however, is the way the pandemic itself, along with societal responses to COVID-19, have seemingly amplified these concerns. Indeed, the sheer volume of extremist content available online and the number of platforms used to spread it grow daily.

Potential Impacts on Canada's National Security

Over the last number of years, the Government of Canada has undertaken a range of efforts designed to address and curb dangerous online activities. These include supporting initiatives like Tech Against Terrorism—a consortium designed to create a digital repository to notify companies when new terrorist content is detected—as well as the Youth Summit on Countering Violent Extremism Online. More recently, and specifically in response to COVID-19, the federal government also allocated $3.5 million in funding to "amplify the current efforts of eight organizations supporting citizens to think critically about the health information they find online," with an emphasis on identifying mis- and disinformation as well as racist and misleading information related to the pandemic (Canadian Heritage 2020). We also know that Canada's security and intelligence community is aware of and continuously tracking these emerging and evolving threats and the risks they pose. An April 2020 briefing note, for instance, prepared by the Canadian Security Intelligence Service (CSIS) and obtained by Global News noted that "ideologically motivated violent extremists and others are using the COVID-19 pandemic as an opportunity to promote disinformation and alternative narratives regarding both the cause of the pandemic and potential societal outcomes" (Bell 2020). Furthermore, CSIS Director David Vigneault said in February 2021 that "COVID-19 has created a situation ripe for exploitation by threat actors seeking to cause harm or advance their own interests. With many Canadians working from home, threat actors are presented with even more opportunities to conduct malicious online activities" (Vigneault 2021). Likewise, the Canadian Centre for Cyber Security recently wrote that "cyber threat actors are taking advantage of people's heightened levels of concern and legitimate fear around COVID-19, trying to spread misinformation and scam people out of their money or private data" (CCCS 2020).

And yet the actual national security implications of these online activities during the pandemic are still not well understood. This is no fault of Canada's security and intelligence community; rather, it simply reflects the fact that the threat environment (including the pandemic itself) is evolving and unfolding in such a way that it risks outpacing the government's ability to assess, act, and preempt emerging concerns. What

is more, COVID-related conspiracy theories and the online (and physical) activities that stem from them are far from having run their course. These and other as yet unforeseen security challenges will continue to emerge in the coming months and years. Also, while Canada's security and intelligence community does have a vital role to play in investigating and supporting broader government and law enforcement efforts to counter security threats stemming from the various challenges explored in this chapter, these same agencies cannot (and should not) counter the expression of public or individual opinion, however disagreeable these opinions may be to the vast majority of Canadians. As other contributors to this volume have noted, Canada's response to the social, political, and ideological challenges spurred by COVID-19 requires activities that go well beyond those reserved for the security and intelligence community, including providing counter-narratives, supporting marginalized communities, establishing deradicalization programs, and otherwise facilitating activities that address the underlining factors that contribute to individual discontent and the growth of extremist mindsets, including systemic racism, economic inequality, and polarizing electoral processes.

In terms of Canada's national security—and in light of the government's prioritization of curbing the spread of the disease and launching large-scale inoculation campaigns across the country—terrorist organizations, right- and left-wing extremist movements, and criminal syndicates will not only continue pursuing the online strategies identified in this chapter, but will also likely continue developing, improving, and adjusting their activities in order to capitalize on the post-COVID environment. In other words, as the pandemic evolves, so will the online narratives peddled by various threat actors. Regardless of the situation, malicious groups will find ways to pivot, adapt, and exploit people's insecurities, the unknown, human suffering, and other epistemic, existential, and social factors that contribute to individuals' susceptibility to destructive and inaccurate information. That said, Canada's security and intelligence community should pay particular attention to online activities engineered to undermine the Government of Canada, to recruit new members to terrorist organizations and extremist groups, and to incite or motivate acts of violence. These online trends are proliferating worldwide, and Canada is no exception.

The Internet will remain a favoured domain for dangerous non-state actors and individuals to carry out their work and achieve their objectives. From our perspective, these are still early days in terms of dealing with the pandemic and addressing its collateral damage, including its effect on malicious online activity. There have already been numerous arrests across Canada of individuals who have made online threats against journalists, politicians, and public health officials (Montpetit 2020), and the environment remains rife for increased extremist activity and real-world physical attacks. Furthermore, exogenous factors, including a fragile Canadian (and global) economy, continued lockdown measures across the country, a seemingly permanent shift to the amount of time we all spend online, and a new and untested US administration, point to a range of potential trigger points that could lead to heightened levels of malicious online activity. In our view, the key themes covered in this chapter—delegitimation, recruitment, and incitement—represent the three most common and deleterious trends related to extremist use of the Internet to have been exacerbated by the COVID-19 crisis. Ongoing and more comprehensive research and analysis will be required to fully understand and respond to the ways in which the Internet has been weaponized during the pandemic.

Funding

The larger research project from which this chapter stems was awarded two grants (August 2021), one from the Canadian Network for Research on Terrorism, Security and Society Small Research Projects program (# 50658-10054), and one from the Department of National Defence's Mobilizing Insights in Defence and Security (MINDS) program's COVID-19 Challenge award.

NOTE

1 Generally speaking, the term "disinformation" is used to describe intentional—often strategically designed—attempts to shape the information environment and to mislead and confuse individuals. Similar to, but distinct from, disinformation is "misinformation," which tends to describe untrue or misleading information disseminated without the intent to deliberately mislead people or maliciously shape the information environment.

REFERENCES

Avis, William. 2020. "*The COVID-19 Pandemic and Response on Violent Extremist Recruitment and Radicalization*." K4D Helpdesk Report 808. Brighton, UK: Institute of Development Studies. https://reliefweb.int/sites/reliefweb.int/files/resources/808_COVID19%20_and_Violent_Extremism.pdf.

Baker, Luke. 2020. "Militants, Fringe Groups Exploiting COVID-19, Warns EU Anti-terrorism Chief." *Reuters*, 30 April 2020. https://www.reuters.com/article/us-health-coronavirus-eu-security/militants-fringe-groups-exploiting-covid-19-warns-eu-anti-terrorism-chief-idUSKBN22C2HG.

Bell, Stuart. 2020. "Neo-Nazis, Extremists Capitalizing on COVID-19, Declassified CSIS Documents Say." *Global News*, 7 December 2020. https://globalnews.ca/news/7501783/neo-nazis-extremists-capitalizing-coronaviruscovid-19-csis/.

———. 2021. "RCMP Arrest Quebec Man Linked to Social Media Accounts that Call COVID-19 a Scam, Talk of Taking Arms to Parliament." *Global News*, 26 January 2021. https://globalnews.ca/news/7600018/rcmp-quebec-man-linked-to-social-media-account/.

Bertrand, Natasha. 2020. "DHS Warns of Increase in Violent Extremism Amid Coronavirus Lockdowns." *Politico*, 23 April 2020. https://www.politico.com/news/2020/04/23/dhs-increase-in-coronavirus-inspired-violence-205221.

Binetti, Soraya, Fabrizio De Rose, Mariana Diaz Garcia, and Francesco Marelli. 2020. *Stop the Virus of Disinformation: The Risk of Malicious Use of Social Media during COVID-19 and the Technology Options to Fight It*. Torino, IT: United Nations Interregional Crime and Justice Research Institute. http://www.unicri.it/sites/default/files/2020-11/SM%20misuse.pdf.

Bloom, Mia. 2020. "How Terrorist Groups Will Try to Capitalize on the Coronavirus Crisis." *Just Security*, 3 April 2020. https://www.justsecurity.org/69508/how-terrorist-groups-will-try-to-capitalize-on-the-coronavirus-crisis/.

Brewster, Murray. 2020. "Military Reviewing What Its Intelligence Branch Knew about Rideau Hall Attacker." *CBC News*, 21 August 2020. https://www.cbc.ca/news/politics/rideau-hall-attackranger-1.5694022.

Britneff, Beatrice. 2020. "Searches for Extremist Content Spiked after Canada's Coronavirus Lockdown: Report." *Global News*, 12 June 2020. https://globalnews.ca/news/7054410/coronavirus-extremist-content-searches-canada/.

Campbell, John. 2020. "Boko Haram's Shekau Labels Anti-COVID-19 Measures an Attack on Islam in Nigeria." Council on Foreign Relations, 17 April 2020. https://www.cfr.org/blog/boko-harams-shekau-labels-anti-covid-19-measures-attack-islam-nigeria.

Canadian Heritage. 2020. "Online Disinformation." Government of Canada, last modified 17 August 2020. https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html#special.

Canadian Press. 2021. "Military Reservist Who Rammed Rideau Hall Gate with Truck Sentenced to Six Years." *CTV News*, 10 March 2021. https://www.ctvnews.ca/canada/military-reservist-who-rammed-rideau-hall-gate-with-truck-sentenced-to-six-years-1.5340945.

CEP (Counter Extremism Project). 2020. "Online Extremists Exploit Coronavirus Pandemic to Incite Violence and Encourage Terrorism." *Counter Extremism Project*, 3 April 2020. https://www.counterextremism.com/blog/online-extremists-exploit-coronavirus-pandemic-incite-violence-encourage-terrorism.

Collen, Dan. 2020. "Antisemitic Anti-masker Arrested with 65 Illegal Guns, $18 Million in Street Drugs." Canadian Anti-Hate Network, 18 January 2021. https://www.antihate.ca/antisemitic_anti_masker_arrested_65_illegal_guns_18_million_street_drugs.

Cordoba, Jose de. 2020. "Mexico's Cartels Distribute Coronavirus Aid to Win Popular Support." *Wall Street Journal*, 14 May 2020. https://www.wsj.com/articles/mexicos-cartels-distribute-coronavirus-aid-to-win-popular-support-11589480979.

CSIS (Canadian Security Intelligence Service). 2019. "CSIS 2018 Public Report." Government of Canada, last modified 21 June 2019. https://www.canada.ca/en/security-intelligence-service/news/2019/06/release-of-csis-2018-public-report.html.

———. 2020. "Staying Cyber-Healthy during COVID-19 Isolation." Government of Canada, last modified 9 April 2020. https://cyber.gc.ca/en/news/staying-cyber-healthy-during-covid-19-isolation.

CTED (Counter-Terrorism Committee Executive Directorate). 2020. "Member States Concerned by the Growing and Increasingly Transnational Threat of Extreme Right-Wing Terrorism." CTED, April 2020. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_trends_alert_extreme_right-wing_terrorism.pdf.

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

Daymon, Chelsea. 2020. "The Coronavirus and Islamic State Supporters Online." Global Network on Extremism and Technology, 13 March 2020. https://gnet-research.org/2020/03/13/the-coronavirus-and-islamic-state-supporters-online/.

Dodd, Vikram. 2020. "Fears of Rise in UK Terrorist Recruits as Anti-radicalisation Referrals Collapse." *Guardian*, 22 April 2020. https://www.theguardian.com/uknews/2020/apr/22/fears-of-rise-in-uk-terrorism-recruits-after-anti-radicalisation-referrals-collapse-coronavirus.

FBI (Federal Bureau of Investigation). 2020. "Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments." FBI Alert Number I-040120-PSA, 1 April 2020. https://www.ic3.gov/media/2020/200401.aspx.

Fletcher, Robson. 2020. "Calgary Police Charge Man over Threat to Spread COVID-19 to Indigenous People." *CBC News*, 1 April 2020. https://www.cbc.ca/news/canada/calgary/calgary-police-covid-19-threats-charge-investigation-1.5517980.

Ghebreyesus, Tedros Adhanom. 2020. "Remarks by the Director-General of the World Health Organization at the Munich Security Conference." World Health Organization, 15 February 2020. https://www.who.int/director-general/speeches/detail/munich-security-conference.

Hanna, Andrew. 2020. "What Islamists Are Doing and Saying on COVID-19 Crisis." Wilson Center, 14 May 2020. https://www.wilsoncenter.org/article/what-islamists-are-doing-and-saying-covid-19-crisis.

Heffes, Ezequiel, and Jonathan Somer. 2020. "Inviting Non-state Armed Groups to the Table." Briefing Note, Center for the Study of Armed Groups, December 2020. https://cdn.odi.org/media/documents/odi-ec-nonstatearmedgrioups-briefingnote-dec20-proof01a.pdf.

Hegazi, Farah. 2020. "Climate Change, Disease and the Legitimacy of Armed Non-state Actors." Stockholm International Peace Research Institute, 1 July 2020. https://www.sipri.org/commentary/essay/2020/climate-change-disease-and-legitimacy-armed-non-state-actors.

Hunter, Brad. 2020. "Terror Will Make You Immune to COVID-19: ISIS to Fanatics." *Toronto Sun*, 24 March 2020. https://torontosun.com/news/world/isis-tells-fanatics-that-terror-will-make-them-immune-to-covid-19.

Jorgic, Drazen. 2020. "El Chapo's Daughter, Mexican Cartels Hand Out Coronavirus Aid." *Reuters*, 16 April 2020. https://www.reuters.com/article/us-health-coronavirus-mexico-cartels/el-chapos-daughter-mexican-cartels-hand-out-coronavirus-aid-idUSKBN21Y3J7.

Joscelyn, Thomas. 2020. "How Jihadists Are Reacting to the Coronavirus Pandemic." Foundation for Defense of Democracies, 6 April 2020. https://www.fdd.org/analysis/2020/04/06/how-jihadists-are-reacting-to-the-coronavirus-pandemic/.

Kapur, Roshni, and Chayanika Saxena. 2020. "The Taliban Makes the Most of Covid-19 Crisis in Afghanistan." Lowy Institute, 27 April 2020. https://www.lowyinstitute.org/the-interpreter/taliban-makes-most-covid-19-crisis-afghanistan.

Lee, Noah, Tia Asmara, Ronna Nirmala, Mark Navales, and Shailaja Neelakantan. 2020. "Southeast Asian Analysts: IS Steps Up Recruitment in Indonesia, Malaysia, Philippines." *BenarNews*, 23 September 2020. https://www.benarnews.org/english/news/indonesian/SEA_ISIS-Threat-09232020163502.html.

MacFarquhar, Neil. 2020. "The Coronavirus Becomes a Battle Cry for U.S. Extremists." *New York Times*, 3 May 2020. https://www.nytimes.com/2020/05/03/us/coronavirus-extremists.html.

Montpetit, Jonathan. 2020. "Quebec Extremists Radicalized by COVID-19 Conspiracy Theories Could Turn to Violence, Experts Warn." *CBC News*, 17 September 2020. https://www.cbc.ca/news/canada/montreal/qanon-quebec-anti-mask-conspiracy-theory-violence-1.5726891.

Perrigo, Billy. 2020. "White Supremacist Groups Are Recruiting with Help From Coronavirus—and a Popular Messaging App." *Time*, 8 April 2020. https://time.com/5817665/coronavirus-conspiracy-theories-white-supremacist-groups/.

Phelan, Alexandra, Nuri Veronika, Helen Stenger, and Irine Gayatri. 2020. "COVID-19 and Violent Extremist Groups: Adapting to an Evolving Crisis." Monash University, 28 April 2020. https://lens.monash.edu/@politics-society/2020/04/28/1380103/covid-19-and-non-state-armed-groups-adapting-to-an-evolving-crisis.

Public Safety Canada. 2019. *2018 Public Report on the Terrorist Threat to Canada: Building a Safe and Resilient Canada*. Ottawa: Department of Public Safety and Emergency Preparedness, April 2019. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pblc-rprt-trrrsm-thrt-cnd-2018/pblc-rprt-trrrsm-thrt-cnd-2018-en.pdf.

Qandil, Mohamed Mokhtar. 2020. "Terrorism and Coronavirus: Hyperbole, Idealism, and Ignorance." Washington Institute, 28 April 2020. https://www.washingtoninstitute.org/policy-analysis/terrorism-and-coronavirus-hyperbole-idealism-and-ignorance.

Rowe, Daniel J. 2020. "Anti-Semitic and Anti-Asian Incidents on the Rise during COVID-19: Reports." *CTV News*, 4 May 2020. https://montreal.ctvnews.ca/anti-semitic-and-anti-asian-incidents-on-the-rise-during-covid-19-reports-1.4924306.

Schecter, Anna. 2021. "Extremists Move to Secret Online Channels to Plan for Inauguration Day in D.C." *NBC News*, 12 January 2021. https://www.nbcnews.com/politics/congress/extremists-move-secret-line-channels-plan-inauguration-day-d-c-n1253876.

Schiffer, Zoe. 2020. "White Supremacists Are Targeting Jewish Groups on Zoom." *Verge*, 15 April 2020. https://www.theverge.com/2020/4/15/21221421/white-supremacist-zoombombers-target-jewish-community-zoom.

Schwartz, Felicia. 2020. "Coronavirus Sparks Rise in Anti-Semitic Sentiment, Researchers Say." *Wall Street Journal*, 20 April 2020. https://www.wsj.com/articles/coronavirus-sparks-rise-in-anti-semitic-incidents-researchers-say-11587405792.

Smith, Victoria. 2020. "Far-Right 'Exploiting Coronavirus Crisis to Try to Recruit People.' " *Leading Britain's Conversation*, 5 October 2020. https://www.lbc.co.uk/news/far-right-exploiting-coronavirus-crisis-to-try-to-recruit-people/.

Soufan Center. 2020. "IntelBrief: The Coronavirus Will Increase Extremism Across the Ideological Spectrum." Soufan Center, 13 April 2020. https://thesoufancenter.org/intelbrief-the-coronavirus-will-increase-extremism-across-the-ideological-spectrum/.

Starbird, Kate. 2020. "How a Crisis Researcher Makes Sense of Covid-19 Misinformation." *OneZero*, 9 March 2020. https://onezero.medium.com/reflecting-on-the-covid-19-infodemic-as-a-crisis-informatics-researcher-ce0656fa4d0a.

Stephens, Keri K., Jody L. S. Jahn, Stephanie Fox, Piyawan Charoensap-Kelly, Rahul Mitra, Jeannette Sutton, Eric D. Waters, Bo Xie, and Rebecca J. Meisenbach. 2020. "Collective Sensemaking Around COVID-19: Experiences, Concerns, and Agendas for our Rapidly Changing Organizational Lives." *Management Communication Quarterly* 34, no. 3 (June 2020): 426–57. https://doi.org/10.1177%2F0893318920934890.

Tunney, Catharine. 2021. "Corey Hurren Pleads Guilty to 8 Charges Tied to Rideau Hall Incident." *CBC News*, 5 February 2021. https://www.cbc.ca/news/politics/corey-hurren-rideau-hall-plea-1.5902362.

Vigneault, David. 2021. "Remarks by Director David Vigneault to the Centre for International Governance Innovation." CSIS, 9 February 2021. https://www.canada.ca/en/security-intelligence-service/news/2021/02/remarks-by-director-david-vigneault-to-the-centre-for-international-governance-innovation.html.

Wamsley, Laurel. 2021. "On Far-Right Websites, Plans to Storm Capitol Were Made in Plain Sight." *NPR*, 7 January 2021. https://www.npr.org/sections/insurrection-at-the-capitol/2021/01/07/954671745/on-far-right-websites-plans-to-storm-capitol-were-made-in-plain-sight.

Wilson, Jason. 2020. "Disinformation and Blame: How America's Far Right Is Capitalizing on Coronavirus." *Guardian*, 19 March 2020. https://www.theguardian.com/world/2020/mar/19/america-far-right-coronavirusoutbreak-trump-alex-jones.

Young, Ian. 2020. "Coronavirus: Suspected Racist Attacker of 92-Year-Old Asian Man Identified by Vancouver Police after 'Overwhelming' Public Response." *South China Morning Post*, 24 April 2020. https://www.scmp.com/news/world/united-states-canada/article/3081328/coronavirus-vancouver-police-identify-suspect.

Youngs, Richard. 2020. "Coronavirus and Europe's New Political Fissures." *Carnegie Europe*, June 2020. https://carnegieendowment.org/files/Youngs_Coronavirus_and_fissures.pdf.