Exploiting Chaos: How Malicious Non-State Actors Are Using COVID-19 to Their Advantage in Cyberspace

Casey E. Babb, Ph.D
Alex Wilner, Ph.D,
Norman Paterson School of International Affairs
Carleton University

Corresponding Author
Casey Babb, caseybabb3@cmail.carleton.ca

TSAS RB 2023-03

TSAS
canadian network for research on terrorism, security and society

Overview

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 nonstate actors for the purposes of this research —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. That being said, the intent of this research – which was presented in more detail as a book chapter in *Stress Tested: The COVID-19 Pandemic and Canadian National Security* (West, Juneau, and Amarasingam 2021) – was to assess how malicious non-state actors have been using cyber space to exploit the pandemic for their own strategic gain, and what might these trends could mean for Canada's national security over the coming years. All told, we focused specifically on three distinct yet overlapping online trends that have proven to be particularly detrimental to national security: delegitimation, recruitment, and incitement.

Summary of Findings

The first main online trend we observed and studied was deligitimation. Throughout the last several years, 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).

The second stream of online activity we studied were recruitment efforts. Many of the same groups seeking to deligitimize governments have also used 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).

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 suggested 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 QAnonrelated 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. Many of these posts had violent connotations and promoted acts of aggression.

From a policy perspective, the 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 pre-empt emerging concerns. 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 we have focused on, 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. Ultimately, 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.

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.

Babb, Casey and Alex S. Wilner. (2021). "Exploiting Chaos: How Malicious Non-state Actors Leverage COVID-19 to Their Advantage in Cyberspace" in West, Leah, Thomas Juneau and Amarnath Amarasingam, *Stress Tested: The COVID-19 Pandemic and Canadian National Security,* University of Calgary Press.

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/howterrorist- groups-will-try-to-capitalize-on-the-coronavirus-crisis/.

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-extremistsexploit- coronavirus-pandemic-incite-violence-encourage-terrorism.

Hanna, Andrew. 2020. "What Islamists Are Doing and Saying on COVID-19 Crisis." Wilson Center, 14 May 2020. https://www.wilsoncenter.org/article/what-islamistsare- 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-briefingnotedec20-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-legitimacyarmed- 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-tellsfanatics- that-terror-will-make-them-immune-to-covid-19.

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.

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/.

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-andignorance.

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

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-ideologicalspectrum/.

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-atthe-capitol/2021/01/07/954671745/on-far-right-websites-plans-to-storm-capitolwere- made-in-plain-sight.