PROTECTING DIGITAL DEMOCRACY: THREATS AND RESPONSES

Date: November 18, 2024

Disclaimer: This briefing note contains the encapsulation of views presented by the speaker and does not exclusively represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

On November 18th, 2024, Ms. Jennifer Irish presented *Protecting Digital Democracy: Threats and Responses* for this year's West Coast Security Conference. The presentation was followed by a question-and-answer period with questions from the audience and CASIS Vancouver executives. The key points discussed were threats to digital democracy and the core response imperatives: intervention and inoculation.

NATURE OF DISCUSSION

Ms. Irish's presentation focused on the growing threat of digital authoritarianism and the need for democracies, like Canada, to enhance their responses. She highlighted the importance of employing a two-pronged strategy of "intervention" and "inoculation" to combat disinformation, misinformation, and malinformation, with a focus on countering digital threats. The main focus was the manipulation of information by foreign state actors, particularly Russia and China, which threatens democratic processes and public trust.

BACKGROUND

Ms. Irish stated that democracies need to improve their responses to digital authoritarianism by employing a two-factor approach of intervention and inoculation. She described "digital authoritarian regimes" employing technology for surveillance, repression and global propaganda. Additionally, "intervention" is a methodology which includes a variety of techniques such as topic rebuttal, counternarratives, and technique rebuttal to swiftly debunk misinformation and discredit threat actors. "Inoculation" encapsulates measures aimed at enhancing resiliency to manipulated information, including strategies of providing accurate,

SFU LIBRARY DIGITAL PUBLISHING

fact-based counternarratives to populations in advance of exposure and tools to identify and understand disinformation misinformation.

“Disinformation” was defined as verifiably false information that is deliberately created and shared with the intent to confuse, manipulate, or mislead. “Misinformation” is “incorrect or misleading information that is shared without intent to deceive or cause harm, and "malinformation” refers to truthful information that is intentionally shared in a harmful context or for malicious purposes. Disinformation propagated by external threat actors is also knowns as “Foreign Information Manipulation and Interference” and the main perpetrators have been Russia and China, with a but that Canada needs to be aware of other main threat actors such as India, Iran, and non-state organizations. She explained that mitigation measures to counter manipulated information through “intervention and inoculation” can be pursued via counternarratives, fact-checking initiatives, “pre-bunking,” and digital literacy programs distributed to the greater public.

Lastly, Ms. Irish profiled digital authoritarianism, discussing the extensive coordination across the Chinese governmental bodies, including the military, to unify the messaging. Their aims are pointed at international adversaries including Western democracies like Canada, targeted territories like Taiwan, and vulnerable diaspora populations that live abroad, whose perceptions of their adopted home countries are specifically targeted. China uses advanced AI and other digital tools to manipulate information and make misinformation more insidious. She explained that Russia operates a disinformation ecosystem using a more distributed approach through proxies, amplifying disinformation on social media to fabricate narratives, conspiracies, and half-truths. Examples from both regimes were given, the creation of cloned media outlets by Russian state-sponsored social media influencers and electoral inference in USA and Europe, and Chinese state-run news organizations spreading “spamaflauge” in an attempt to discredit leaders, including in Canada.

Question and Answer

What exactly is “sowing discord” and can you give any examples?

The foreign actors who we have been studying, particularly Russia, will take a very sensitive issue, a wedge issue, and try to amplify the narrative that will make it more difficult to have an informed public debate around it. For example, Russia has propagated narratives that homosexuality is being promoted in Western countries, including Canada. One example is on climate change.

Disinformation narratives can distort the public's understanding of the crisis or solutions to it including through what we call "greenwashing," where a corporation or government is misrepresenting a solution that claims to be trying to reach net zero emissions but is actually a perpetrator. The tactic of foreign actors in "sowing discord" is mainly aimed at amplifying polarization by propagate an extreme narrative, which makes it difficult for the public to understand the issue and have a discourse around the results. In the case of climate change, it can cause a delay in remedies or an inability to find solutions to respond to the crisis.

When does misinformation and disinformation reach the legal threshold?

When you are dealing with misinformation against people, legal resources are underdeveloped. There are options such as libel and slander, and with fraud being another inroad when countering disinformation that meets that threshold. One asset in Canada is we do have good hate speech laws and those can certainly be brought into operation, especially hate speech that incites violence. One area of shocking concern is the amount of gender-based misinformation out there. For example, Deep Porn and AI generated images of sometimes very vulnerable young women have resulted in them taking their lives in some cases. It really is truly tragic. There should be accountability for this, and it should include the tech platforms that make this available. The On-Line Harms legislation would have represented an advancement in legal remedies. An area for further work is related to trying to define accountability for tech platforms, which will allow for more efficiency by addressing the source as opposed to the consumer-end.

Can you elaborate on the vulnerable populations" as you referred to it in your presentation?

There exist diasporas who are very reliant on closed media and foreign language outlets like WeChat. That vulnerability was taken advantage of by China by distorting narratives around the Chinese community in Canada to impact their vote, for example through s false narratives propagated that some Canadian politicians wanted to do away with WeChat. As some of these diaspora populations count on WeChat to transfer money to family members, so disinformation narratives that put that ability in question obviously would be extremely impactful. Other examples include young women who are being exploited through to visual disinformation, and disinformation narratives directed at persons e going through gender transitions. In terms of our approach to resilience, we should be conscious that some parts of our population will be more vulnerable than others in our approach and our outreach. It is critical to be

generating generic resilience tool kits that will help all our populations think critically about what they see, understand it, and be prepared for particularly damaging narratives that might be based on their vulnerability or more other identifiable attributes.

KEY POINTS OF DISCUSSION

- Digital authoritarianism is on the rise and therefore becoming more coordinated between state actors.
- Misinformation and disinformation and malinformation have damaging or distorting impacts. In terms of foreign interference, FIMI needs to be better understood given the potential to distort public discourse upon which the exercise of democracy depends.
- Canada has significant vulnerabilities to misinformation, disinformation, and malinformation as well as FIMI, therefore they need to be addressed in policy and practice.
- Canada has a unique opportunity to leverage the Public Commission Inquiry on Foreign Interference to implement effective methods to counter misinformation, disinformation, and malinformation.
- Intervention and Inoculation, in combination, are promising strategic tools for western democratic countries.

FURTHER READING

Irish, J. (2024). LEADING SECURITY AND INTELLIGENCE: CURRENT TRENDS AND ESSENTIAL ABILITIES. *The Journal of Intelligence, Conflict, and Warfare*, *6*(3), 170–174. https://doi.org/10.21810/jicw.v6i3.6387

McMahon, D. & Nikoula, D. (2024, July). *Cognitive Warfare: Securing Hearts and Minds.* Information Integrity Lab. Universty of Ottawa. https://infolab.uottawa.ca/common/Uploaded%20files/PDI%20files/InfoLab%20-%20Cognitive%20Warfare,%20Securing%20Hearts%20and%20Minds.pdf

Françoys L. & Irish, J. (2024, January). *Understanding the Threat and Challenge of Visual and Multimodal Disinformation (VMD) Summary of a Collaborative Study by the Computer Research Institute of Montreal with The Information Integrity University of Ottawa.* Information Integrity Lab. University of Ottawa.

.https://infolab.uottawa.ca/common/Uploaded%20files/PDI%20files/InfoLab%20English%20CRIM%20Report%20Final%20(digital).pdf

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org