THREAT RESILIENCE IN THE REALM OF MISINFORMATION, DISINFORMATION, AND TRUST

Date: November 21, 2022

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 21, 2022, Phil Gratton, an executive public servant at the Canadian Security Intelligence Service (CSIS), currently on interchange as Associate Faculty with the Canada School of Public Service's (CSPS) Digital Academy, gave a presentation on *Threat Resilience in the Realm of Misinformation, Disinformation, and Trust* at the 2022 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 the harms caused by state-sponsored disinformation campaigns, the use of artificial intelligence (AI) to facilitate and counter the spread of disinformation, as well as the importance of critical thinking and collaborative response to build resilience against these threats.

NATURE OF DISCUSSION

Presentation

The central theme throughout Mr. Gratton's presentation was the impact of disinformation on our society, democratic processes, critical infrastructure, and economy. He also discussed how artificial intelligence can not only be used to facilitate disinformation campaigns but how it could be used to counter such campaigns as well. Mr. Gratton developed this presentation in collaboration with CSPS colleague Aïcha-Hanna Agrane, a policy analyst with expertise in global affairs, cybersecurity, and countering disinformation.

Question & Answer Period

During the question-and-answer period, Mr. Gratton discussed the importance of building trust in our institutions and the need to collaborate with academia to ensure government messaging is supported by evidence and facts.

BACKGROUND

Presentation

The presentation began with musings on the emergent quality of technology and disinformation and how this quality can present a risk for Canadian society and international geopolitics. As explained, disinformation is misleading and provocative content intended to manipulate, cause damage, or misguide, which often fosters mistrust of our media institutions and government. Some citizens find themselves in a situation where they no longer believe what they are reading and can get easily swayed by disinformation considering how skillfully it is produced and disseminated.

One of the primary concerns of disinformation campaigns is foreign interference and espionage, in which hostile state actors spread disinformation to discredit other governments' institutions to reach their strategic goals. They often do this by gaining influence and attacking social cohesion, which can threaten democracy by polluting public debate. Foreign interference can harm not only democratic processes but also critical infrastructure and economic stability.

The erosion of trust is one of the most concerning consequences of disinformation, and it has had a major impact on our public institutions, including the government, public service, health sector, and media. Hostile state actors often use disinformation techniques aiming to influence Canadians' political views, interfere with the country's political systems, create division, and exacerbate distrust in Canadian public institutions.

In terms of countering disinformation campaigns, the Canadian government has been taking steps to increase public awareness to ensure people are able to distinguish fact from fiction. However, in the end, it will be a shared responsibility between the institutions and the people to counter disinformation. There are only so many countermeasures a government can put in place before they become oppressive, so it is up to individuals to think critically, verify their sources, and be mindful about what they are reading, hearing or watching.

At this point in the presentation, the conversation shifted towards artificial intelligence and how it has, nefariously, increased the effectiveness and pervasiveness of disinformation. Two examples were provided to illustrate the points: deep fakes and bots. Deep fakes can destroy our trust in visual and auditory proof, which not only destroy reputations but can also cause second-order damage to democratic processes, thwart diplomatic efforts, and cause irreparable economic damage. Bots, on the other hand, are automated programs that mimic human behaviour and are often used to amplify the reach of disinformation. These AI technologies are not only the source of false information but also undermine the legitimacy of factual information by creating doubt.

While AI technologies can facilitate the spread of disinformation, they can also be used to counter it. Some AI tools can carry out linguistic analysis of text to reveal the difference between text written by humans and that generated by a computer. Similarly, algorithms can identify traces of hateful wording and reveal fake images and manipulated videos through reverse engineering. AI can also accelerate the process of tracing the origin of disinformation. However, while AI technologies can be helpful in countering disinformation, they still require human effort and specialized knowledge, which is not always at hand for most people to whom the disinformation is targeted. As such, it was argued that effective responses to disinformation will require a mix of technical solutions, organizational and governance changes, and commitment to societal digital literacy.

Question & Answer Period

During the question-and-answer period, Mr. Gratton provided his top three takeaways for civilians to keep in mind regarding disinformation and building trust in our institutions. First, it is important for people to realize that building trust is a shared responsibility. Governments cannot simply bombard the public with messages about what to believe. It is equally important for citizens to better educate themselves and gain greater digital literacy. Second, Mr. Gratton reiterated that trust is a two-way street. If the government expects the public to trust their messaging, they also need to trust Canadian citizens to make their own decisions; a shared notion of trust is essential. And finally, it is important for the public to understand that disinformation can pollute the general discourse and affect a wide range of people, regardless of their background. Ostensibly well-educated, arguably more intelligent, prominent figures can fall for disinformation just as easily as anyone, so well designed are disinformation campaigns today.

In response to a question regarding collaboration between government agencies and educational institutions, Mr. Gratton indicated that engagement with academia was paramount to ensure their messaging is aligned and devoid of spin. He clarified that the majority of messaging being put forward by the government is based on studies and research that academia has already conducted. Mr. Gratton emphasized that it is important to ensure that any message from the government is supported by evidence and facts. This level of support goes a long way to build trust and credibility between institutions and the public. Mr. Gratton provided the Canadian Security Intelligence Service as an example to illustrate how transparency and engagement with other educational and academic institutions has opened a dialogue and facilitated the sharing of information. This is an effort to reduce the mistrust of intelligence organizations, who tend to be secretive by mandate.

KEY POINTS OF DISCUSSION

Presentation

- Disinformation campaigns by hostile state actors are often implemented to discredit other governments' institutions to reach their strategic goals by gaining influence and attacking social cohesion. Overall, disinformation threatens democracy by polluting public debate.
- Disinformation campaigns harm not only democratic and social processes but also physical critical infrastructure, economic stability, and prosperity.
- Disinformation has led to a significant loss of trust in our various institutions, especially our public institutions, including the government and public service, health sector, and media.
- Artificial Intelligence is often used to facilitate and amplify disinformation campaigns, often through deep fakes and bots; however, AI can also be used to counter disinformation campaigns.
- Effective responses to disinformation attacks is a shared responsibility that will require a mix of technical solutions, organization changes, procedural shifts, and commitment to digital literacy.

Question & Answer Period

- Building trust in our institutions is a shared responsibility between our government and Canadian citizens.
- Disinformation can pollute the general discourse and affect a wide range of people, regardless of their background.

- Collaboration between government agencies and educational institutions is essential to ensure any messages being put forward by the government are supported by evidence and facts from academic research.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University
Available from: https://jicw.org/