WEAPONIZED MISINFORMATION A.K.A #FAKENEWS

Date: September 10, 2019

Disclaimer: This briefing note contains summaries of open sources and does not exclusively represent the views of the Canadian Association for Security and Intelligence Studies.

Executive Summary

Misinformation in the form of "fake news" can potentially be weaponized by malicious actors to undermine Canada's national security and government infrastructure. Developing a comprehensive database to track and understand potential threat actors and their use of fake news can potentially provide actionable intel, thereby exposing and publicly challenging fake news items. Fake news has been used to negatively influence the reputation of government officials and to incite violence between ethnic groups. Fake news utilizes confirmation bias (the tendency to interpret new evidence as confirmation of one's existing beliefs or theories) through disseminating meticulously crafted messages to targeted audiences, who are selected based on their online activities.

Purpose Statement

The purpose of this briefing note is to examine the use of misinformation, with a focus on fake news as a potential weapon of information warfare. This may inform any responses to the threat of misinformation that are potentially being utilized to undermine Canada's national security, Canada's democratic process, and the integrity of Canadian institutions.

The Security Problem

The dissemination of misinformation, particularly in the form of fake news distributed through social media channels, can be exploited by organizations and individual actors to spread fear, invoke hatred, or subvert the confidence of Canadian citizens in the Government of Canada, its elected officials, institutions and policies. Since social media provides an audience, it gives creators of fake news the power to nefariously unite or divide populations who put their trust in "news" items they see online.

Background

Evidence suggests that Canadians are susceptible to fake news. Earlier this year, it was reported that a web-based news service operating as *The Buffalo Chronicle* had published a fake news story about the Bank of Montreal allegedly offering bribes to avoid government prosecution, as well as additional stories alleging that political power struggles were taking place within the Liberal party (Ling, 2019). All aspects of this story were fake and were shared on social media. Moreover, the

story from the Buffalo Chronicle was allegedly shared on Twitter by two sitting members of Parliament (Ling, 2019).

Misinformation in the form of fake news can be utilized to incite violence. In Nigeria, Berom vigilantes appear to have been motivated by fake news to attack and kill Fulani Muslims. Furthermore, according to Matthias, the PR officer for Plateau State police, killings motivated by fake news are common occurrences in Plateau State (Adegoke, 2018).

It has been argued that the increase in the ability for individuals to "access, create, and share information," in combination with limits to the amount of information individuals can "attend to from outside sources" has created an environment that is conducive for the spread of fake news (Hills, 2019, p. 323). This is due to a heightened reliance on bias by individuals to process information, in an environment that is over-saturated with sources of information (Hills, 2019). Canadian academics suggested that in the past, one could see what information the public was exposed to through reading the newspaper, which acted as a central source for news and information on current events. However, it is now more difficult to understand what information the public is exposed to due to varying information being delivered to varying targets, through multiple media outlets (Semple, 2019).

Algorithms and other AI-driven systems can be deployed to flag false or misleading content that is then removed. However, as evidenced by a fake news detection algorithm evaluating video footage of the 2019 Notre Dame fire, as related to the 9/11 attacks, this approach arguably still faces some key technical challenges (Timberg & Harwell, 2019). Furthermore, this approach also requires the continued cooperation and support of private stakeholders (social media service providers) to be implemented and achieve sustainable results.

Key Considerations and Implications

Misinformation could be used to interfere with the upcoming October 2019 Federal Election. It has been suggested that foreign actors could be motivated to influence the upcoming Canadian Federal Elections because of Russia and Canada's colliding interests in the "Arctic,… Ukraine and…Baltic states" (Sevunts, 2019, para. 2). Patterns of foreign influence in the past can be seen in the Alberta General Election in April 2019. The election reportedly saw both domestic and foreign influence through inauthentic social media accounts (Tunney, 2019). The election in Alberta allegedly drew foreign attention because its energy industry affected foreign interests and would have international implications (Tunney, 2019).

The problem is not necessarily the difficulty in confronting misinformation, the problem is arguably the weaponization of confirmation bias by an adversary. This can involve the deliberate targeting of populations who are believed to hold a particular worldview, with specific messaging and effectively conducting a precision PSYOPS campaign. Arguably, this has become feasible by utilizing social media for conducting target reconnaissance, maximizing exposure and creating an element of plausible deniability. Potentially contentious topics can be identified on social media and then linked to false reports that are created to appear to be from a legitimate looking news

source. As has been noted, "propaganda preys on pre-existing grievances" and social media provides a useful tool for identifying such grievances (Greenspon & Owen, 2017, para. 10). Bot-nets can be utilized to spread stories, increasing the probability that a human will engage and share the story with their private contacts and social media audience. This can assist in hiding the influence of bot-nets in spreading fake news, as well as continuing to spread misinformation.

Although it is unclear if extremist groups have or will play a direct role in creating fake news, evidence suggests they have engaged with this type of material online, and may continue to play an active role in disseminating fake news (Solon, 2018). Furthermore, violent actions undertaken by extremists may be motivated in part as a result of their engagement with fake news and a perceived escalation of grievances.

Alternative Perspectives to be Considered

There may be measures that can be deployed to effectively mitigate the problem of "weaponized confirmation bias," through the use of fake news by educating the public. It has been argued that the general population can be "inoculated" against fake news through educational materials, including but not limited to the use of interactive media (games), in which the participant acts as a purveyor of fake news (Guerrini, 2018; Foster, 2019). Exposure to qualified fake news traits and examples could potentially mitigate the impact of widely-spread misinformation. However, the current low engagement with these fake news games arguably presents a key challenge with this approach (Smith, 2018). Furthermore, the voluntary nature of this method may present a key challenge in getting the message to the general public.

What is Not Known

The full impact of "social bots" (software-controlled profiles or pages) that have been used to facilitate and support the spread of misinformation is not entirely known (Shao et al., 2017). A quantitative analysis of the effectiveness of misinformation-spreading attacks based on social bots is required to fully understand their impact.

Furthermore, the exact impact that fake news has had on any public perceptions or on public opinions regarding specific issues is not yet clear. This will arguably remain as an unknown until the development of a more sophisticated set of metrics can be developed to measure the impact of fake news. Moreover, the full extent that any planned and coordinated operations aimed at spreading misinformation have already occurred in Canada is not currently known.

Finally, until it is addressed in a court of law, it may not be fully known as to what extent any legislation or other such measures undertaken by the government, seeking to limit or penalize the publication and/or the dissemination of fake news, will be considered permissible under the Charter of Rights and Freedoms.

Next Steps

- Conduct additional research on the role and use of social bots in spreading fake news, with a focused analysis of Canadian content.

- Investigate fake news stories that have received significant engagement online. Focus on whether there is any evidence to support any measures of coordination or organization in how the content was distributed and/or the intention behind the creation of the content.
- Determine whether any metrics that apply to online content (eg; marketing) can be utilized to assist in the creation of metrics designed to specifically measure the impact of fake news.

References

Adegoke, Y. (2018) Like. Share. Kill. Retrieved 1st June, 2019 from https://www.bbc.co.uk/news/resources/idt-sh/nigeria_fake_news

Blackwell, T. (2017, November 20). Russian fake-news campaign against Canadian troops in Latvia includes propaganda about litter, luxury apartments. Retrieved from https://nationalpost.com/news/canada/russian-fake-news-campaign-against-canadian-troops-in-latvia-includes-propaganda-about-litter-luxury-apartments

Foster, H. (2019, March 19). #StrongerWithAllies: Meet the Latvian who leads NATO's fight against fake news. Retrieved from https://www.atlanticcouncil.org/blogs/new-atlanticist/strongerwithallies-latvian-leads-nato-s-fight-against-fake-news/

Greenspon, E., & Owen, T. (2017, May 29). 'Fake news 2.0': A threat to Canada's democracy. Retrieved from https://www.theglobeandmail.com/opinion/fake-news-20-a-threat-to-canadas-democracy/article35138104/

Guerrini, F. (2018, August 1). NATO's Latest Weapon: A Facebook Game For Fake News Countering. Retrieved from https://www.forbes.com/sites/federicoguerrini/2018/07/31/natos-answer-to-fake-news-a-facebook-game-to-spot-online-misinformation/#76013ffc3226

Hills, T. T. (2019). The dark side of information proliferation. *Perspectives on Psychological Science*, *14*(3), 323-330.

Ling, J. (2019, March 22). How Canada flunked its first big fake news test. Retrieved from https://www.citynews1130.com/2019/03/22/big-story-fake-news/

Semple, J. (2019, September 14). Canadian academics, scientists fight back against online election disinformation. Retrieved from https://globalnews.ca/news/5901707/canadian-academics-scientists-election-disinformation/

Sevunts, L. (2019, September 13). Kremlin disinformation campaigns could target Canada's federal election: expert. Retrieved from https://www.rcinet.ca/en/2019/09/12/kremlin-disinformation-campaigns-could-target-canadas-federal-election-expert/

Shao, C., Ciampaglia, G. L., Varol, O., Flammini, A., & Menczer, F. (2017). The spread of fake news by social bots. *arXiv preprint arXiv:1707.07592*, 96-104

Smith, A. (2018, July 27). NATO launches The News Hero Facebook game to counter Russia's info war. Retrieved from https://www.nbcnews.com/news/world/nato-launches-news-hero-facebook-game-counter-russia-s-info-n895241

Solon, O. (2018, January 17). Social media firms warned of new type of online extremism at Senate hearing. Retrieved from https://www.theguardian.com/technology/2018/jan/17/social-media-firms-warned-of-new-type-of-online-extremism-at-senate-hearing

Timberg C. and Harwell D. (2019) Notre Dame fire: YouTube tool to fight fake news accidentally links Paris blaze to 9/11 terror attack (16 April, 2019) Retrieved 1st June, 2019 from https://www.independent.co.uk/news/world/europe/notre-dame-fire-youtube-video-911-terror-attack-hoax-fake-news-a8871906.html

Published by the Journal of Intelligence, Conflict and Warfare and Simon Fraser University, Volume 2, Issue 2.

Available from: https://jicw.org/