Circular Notice to Parliamentarians

OCTOBER 2023

Probable PRC "Spamouflage" Campaign Targeting Canadian Parliamentarians

The Government of Canada maintains the strength and resilience of Canada's democratic institutions through vigilance, including by monitoring the digital information environment for threats to democracy, such as foreign information manipulation and interference.

Summary – Spamouflage Activity

In September 2023 Global Affairs Canada's (GAC's) Rapid Response Mechanism (RRM) Canada tracked a bot network likely connected to the People's Republic of China (PRC) targeting the Prime Minister, several members of Cabinet, the leader of the Official Opposition, and dozens of other Members of Parliament on popular social media platforms such as Facebook, X/Twitter, and YouTube.

Those MPs specifically targeted by this campaign are being informed. However, your accounts may have also been implicated in the activity through the tagging system available on social media platforms. Nothing observed in this activity represents a threat to your safety, or that of your family.

The Spamouflage campaign primarily targeted the Prime Minister; however, it accuses dozens of other MPs of criminal and ethical violations, and sought to attribute these allegations to a well-known critic of the Chinese Community Party (CCP) in Canada and popular Chinese-language vlogger. The Spamouflage campaign also included the use of likely "deepfake" videos, digitally modified by artificial intelligence, sharing a likeness of the Chinese-language vlogger.

Analysis by RRM Canada suggests that the bot-network is part of the well-known Spamouflage network. Spamouflage has been publicly reported on by technology companies and threat intelligence experts, who have directly connected the activity to the PRC. The same bot networks involved in this campaign were engaged in the spreading of disinformation claiming that the Hawaiian wildfires were caused by a secret US military "weather weapon", and have been connected to disinformation about Japan's Fukushima water release in August.

Background – Spamouflage

"Spamouflage" should be considered a tactic or technique, not an entity. It is a network of new or hijacked social media accounts that posts and amplifies propaganda messages across multiple social media platforms – including Facebook, X/Twitter, Instagram, YouTube, Medium, Reddit, TikTok, and LinkedIn. The word is a portmanteau of "spam" and "camouflage", intended to portray the covert and hidden attempts to spread spam-like content and propaganda among more benign, human-interest-style content. Spamouflage networks are largely contained within their own

[APG]

echo chambers of fake users, and rarely garner organic social media engagement from real users.

On August 29, 2023, Meta released its standard quarterly Adversarial Threat Report, which featured a significant section detailing the company's efforts to take down accounts linked to Spamouflage operations. The company affirmed that Spamouflage activity is linked to PRC law enforcement entities.

Reporting Foreign Interference

In your role as an elected Member of Parliament, you are of interest to those states that seek to influence or interfere with Canadian democratic institutions. But there are things you can do to protect yourself from foreign information manipulation and interference:

- Make use of reporting and flagging functions on social media platforms where you have a presence. While some companies actively patrol and police malign and inauthentic behaviour, others rely on user reports to begin a takedown process.
- Be careful with the information you share (in public, to the media or private), and take note of unexpected online interactions. This is especially pertinent in how you handle sensitive information.
- Be aware of inappropriate requests which involve money, and question the source of suspicious donations or "gifts".
- Take note of unnatural social interactions, frequent requests to meet privately, out-of-place introductions or engagements, gifts and offers of all expenses paid travel.
- Practice good cybersecurity hygiene: use strong passwords, enable two-factor authentication, and don't click on links or open attachments unless you are certain of who sent them and why.

If you wish to report suspected foreign interference activity or other issues of national security concern, the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), the Communications Security Establishment's Canadian Centre for Cyber Security all have telephone and online reporting mechanisms. We will give you these details to keep on hand:

- To report suspicious incidents which may be of concern to national security, contact the RCMP's National Security Information Network at 1-800-420-5805, or by email at RCMP.NSIN-RISN.GRC@rcmp-grc.gc.ca
- To report non-urgent potential national security threats or suspicious activities, contact CSIS at 613-993-9620, or 1-800-267-7685, or by completing the web form: https://www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html
- To report non-urgent potential cyber security threats or incidents, contact the Canadian Centre for Cyber Security at 1-833-CYBER-88 (1-833-292-3788) or by completing the web form: https://www.cyber.gc.ca/en/incident-management
- Of course, to report a threat or immediate danger, call 9-1-1 or contact local police.

[APG]

Letter to affected Parliamentarians (47 MPs)

From: Deputy Minister of Foreign Affairs

Hello,

This letter is to inform you that your accounts on social media platforms Facebook and Twitter were targeted in the Spamouflage campaign outlined in the attached circular: *Probable PRC "Spamouflage" Campaign Targeting Canadian Parliamentarians.*

Global Affairs Canada observed the activity targeting 47 Members of Parliament, from across the political spectrum and spanning multiple geographic regions of Canada

Nothing observed by Global Affairs Canada represents a threat to your safety, or that of your family. It is our assessment that the information operation was intended to negatively impact your reputation, not to cause you physical harm or endanger your family.

As noted in the attached circular, there are numerous resources available from Canada's security and law enforcement agencies to report suspected foreign interference.

The Government of Canada will continue to monitor the digital information environment for foreign information manipulation and respond when necessary and appropriate, including through public disclosure and diplomatic engagement.

[APG]