October 23 Statement on Spamouflage

- **In August 2023, Rapid Response Mechanism (RRM) Canada detected a Spamouflage campaign across several social media platforms targeting Canadian Parliamentarians across the political spectrum.**
- **RRM Canada detected this campaign as part of its regular monitoring activities and worked with [redacted] to corroborate its findings, including the link between the campaign and the Chinese government.**
- **Following this finding, Global Affairs Canada a) made clear to the Chinese Ambassador that this type of activity is completely unacceptable, b) reached out to the social media companies so that they can assess whether this campaign violates their terms and conditions and in that case request that they remove the content and networks involved c) spoke to the individual negatively affected by the campaign, and d) disclosed its findings publicly to shine light.**
- **We will continue to monitor our information environment for this type of malicious foreign campaigns and respond when appropriate.**

****

RESPONSIVE LINES

- Our government has made it clear to affected MPs that nothing observed by the RRM represents a threat to their safety, or that of their family.
- All MPs affected by this campaign have been offered a briefing by the RRM on the findings of our report and were given resources and advice on how to report any instances of suspected foreign interference.

[APG]

- We have proactively engaged with the affected platforms and notified them about our findings, resulting in most of the activity and network being removed.

ADDITIONAL QUESTIONS AND ANSWERS

Why didn't you publish the full report or provide additional details?

- While the analysis included in the report is not classified and is based on publicly available information, the report content is intended for the security and intelligence audience. It is crucial to protect our methodology; therefore, a limited portion of the report was removed. We also wanted to protect the identity of the individual who was targeted.

How were you able to attribute this operation to the Chinese government?

- As mentioned in the public statement, RRM Canada detected this campaign as part of its regular monitoring activities. The team consulted with [redacted], experts at the Australian Strategic Policy Institute and the Microsoft Threat Assessment Centre to corroborate its findings. Furthermore, Spamouflage has been publicly reported on by technology companies and threat intelligence experts, who have directly connected this bot network to China.

What actions have you undertaken to prevent further harassment/transnational repression of diaspora communities within Canada?

- Our government has established numerous mechanisms and online services for Canadians to anonymously report any suspected foreign interference such as the National Security Information Network web portal. Furthermore, the RCMP, CSIS and CSE have telephone and online reporting mechanisms that are monitored for anyone who would like to report suspected foreign interference or a threat to national security.

Why did you not publish your findings sooner?

- Due to the sensitive nature and implications of our findings, we had to tread carefully to ensure appropriate cross-governmental verification and partner consultation before releasing any public statement.

BACKGROUND

On October 23, 2023, GAC released a statement acknowledging that a 'Spamouflage' campaign connected to the People's Republic of China was detected by RRM Canada. Beginning in early August 2023, and accelerating in scale over the September long-weekend, a bot network left thousands of comments in English and French on the Facebook and X/Twitter accounts of Canadian Members of Parliaments (MPs).

This campaign targeted dozens of MPs from across the political spectrum, including the Prime Minister, the leader of the Official Opposition, and several members of Cabinet. “Parliamentarians affected by this “Spamouflage” campaign were notified and have been offered a briefing by the Rapid Response Mechanism on the findings of the report. It has also been made clear to them that nothing observed in this activity represents a threat to their safety, or that of their family.

These spam comments claimed that a critic of the Chinese Communist Party (CCP) in Canada had accused the various MPs of criminal and ethical violations. The Spamouflage campaign also included the use of likely “deepfake” videos, which are digitally modified by artificial intelligence, targeting the individual.

Spamouflage is a tactic that uses networks of new or hijacked social media accounts to post and amplify propaganda messages across multiple platforms. RRM Canada’s analysis suggests that the bot-network could be part of the well-known Spamouflage network which has been publicly reported on by technology companies (such as Meta and Microsoft) and threat intelligence experts (such as Graphika), who have connected the activity to China.

This tactic has also been studied and publicly reported on by the Australian Strategic Policy Institute (ASPI) which informed RRM Canada’s assessments.

Global Affairs Canada has proactively engaged the affected platforms, and notified them about the Spamouflage activity, resulting in much of the activity and network being removed.

RRM Canada assesses the goal of this operation was likely to:

- Discredit and denigrate the targeted MPs through seemingly organic posts, alleging impropriety, by posting waves of social media posts and videos that called into question the political and ethical standards of the MPs, using a popular Chinese-speaking figure in Canada; and
- Silence criticism of the CCP by getting MPs to distance themselves from the critic and discouraging wider online communities from engaging with them.