LESSONS FROM THE CAMBRIDGE ANALYTICA CRISIS: CONFRONTING TODAY'S (DIS)INFORMATION CHALLENGES

Date: November 27th, 2020

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 27, 2020, Dr. Emma Briant presented *Lessons from the Cambridge Analytica Crisis: Confronting Today's (Dis)information Challenges*, at the 2020 CASIS West Coast Security Conference. The presentation was followed by a question and answer period with other speakers. The key points of the discussion focused on digital mercenaries, surveillance capitalism, and Western government/military responses to foreign influence campaigns.

NATURE OF DISCUSSION

Presentation

Dr. Briant used Cambridge Analytica as a case study throughout her presentation to demonstrate the growth of a new industry of surveillance capitalism and how this is being used to exploit online source data to carry out foreign influence campaigns.

Question Period

The question and answer period focused on government vetting of cyber information companies, the ethical use of data, and privacy concerns.

BACKGROUND

Presentation

Throughout the War on Terror, a new industry of surveillance capitalism has developed which markets data collection and analysis services to governments,

militaries, and other organisations around the world. Firms in this industry use online data, mined from platforms like Facebook and Twitter to learn behavioral patterns and predict and manipulate them. This industry often employs complex corporate structures that can obscure data sharing and financial relationships between large networks of companies. These organisational structures that companies such as Cambridge Analytica used, can obscure the links that these companies may have to nefarious actors. Dr. Briant argued that because of this, governments must be careful when choosing to contract these types of companies. To demonstrate the potential security risks posed by these companies, Dr. Briant used the example of SCL Group - a company closely associated with Cambridge Analytica - working with NATO on strategic communications while at the same time period Cambridge Analytica was pitching services to a Russian oil company. She argued that it is highly likely that these simultaneous events were of strategic value to the Russian government as Cambridge Analytica is allegedly known to have exposed defense data to other governments and campaigns in the past.

Today, data privacy is paramount. There needs to be stronger policies when it comes to how we tackle data use and data privacy in our society because these same campaigns that are utilizing data in very unethical ways domestically are also being exploited by foreign adversaries. This will take an overall whole of society response to disinformation and propaganda wars with clear guidance, better oversight, and a separation of domestic and foreign cyber capabilities. Additionally, a move towards more open source and non-profit tech should be encouraged. This work needs to be done with international cooperations so that companies cannot exploit discrepancies in jurisdiction. By pursuing this important policy, it will make our societies more secure and safe.

Question Period

It is necessary to track what companies are doing by perhaps building a database of who is working for who and what they are doing. There are clearance procedures to vet individuals, but this is not done with company networks. Requesting companies to declare who else they are working for when they want to work for a government should not be considered excessive. A licensing system that would create an incentive for companies that follow certain ethical rules could also be beneficial to prevent another Cambridge Analytica. Working for the American, Canadian, or British government should be considered a privilege since it gives companies prestige, which they can use later as a reference. This has a higher value than the amount they get pay under any contract. Furthermore,

there should be a balance between requiring more information to vet people that have the necessary experience and allowing any cronyism to develop once they have been in the job for a long time. Understanding the technologies and methods used will enable people to vet and hire personnel more effectively, safely, and ethically.

KEY POINTS OF DISCUSSION

Presentation

- The War on Terror fueled the development of an industry of surveillance capitalism.
- Companies, such as Cambridge Analytic, use complex corporate structures to obscure affiliations.
- Digital mercenaries often work with potentially malicious actors and foreign governments.
- Western governments must do more to protect themselves and civilians from foreign influence in campaigns.

Question Period

- Government vetting of private data analytics and surveillance companies must be improved to increase security.
- There should be increased industry transparency for these types of companies.

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