ENGAGING THE PRIVATE SECTOR FOR NATIONAL SECURITY

Date: November 23, 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 23, 2020, Robert Gordon presented on the topic of Engaging the Private Sector for National Security at the 2020 CASIS West Coast Security Conference. The presentation was followed by a moderated question and answer period. Key points of discussion included: federal level engagement with the private cybersecurity sector, the level of the cyber threat environment that the private sector is dealing with, and the requirement for a collaborative approach in the national security environment.

NATURE OF DISCUSSION

Presentation

Robert Gordon discussed the new cybersecurity environment and what changes have been occurring in this space. He also offered solutions used in this space.

Question Period

During the question period Robert Gordon discussed the importance of understanding data for states to establish defensive strategies.

BACKGROUND

Presentation

With the onset of the COVID-19 pandemic in 2020, the cybersecurity forecast has become increasingly gloomy. Canada's Minister of National Defence, the Hon. Harjit S. Sajjan, spoke about cybersecurity as being one of the most serious economic national security challenges that Canada is facing. With data being the

new currency and connectivity being high, what is considered as critical infrastructure could be re-evaluated.

In the 10 sectors that Canada traditionally considers critical infrastructure, it is estimated that about 80% of that entire infrastructure is either owned, operated, or regulated by somebody other than the federal government. With this much infrastructure not being covered by the federal government, it again calls into question what is considered as critical in critical infrastructure.

Over the past few years, there have been significant changes in Canada's national approach to cybersecurity strategies. When looking at engaging the private sector, the federal government is now moving forward in ways that it has never done before. This includes the establishment of a new cyber centre, which shares government technical expertise and fuses what is being looked at in their foreign intelligence watching capabilities between departments.

This increased collaborative approach is sharing knowledge from an international level to the private sector, and the Five Eyes countries are now starting to issue joint warnings to the private sector for the first time. Similar alerts were issued by the private sector and the Canadian Centre for Cyber Security in Canada regarding hospitals being targeted with ransomware attacks. In October 2020, the National Security Agency also alerted companies about Chinese state actors exploiting vulnerability, and these same issues and concerns are applicable to Canada. For Canadian companies that operate internationally, this can benefit their overall businesses because they are starting to see strong information released by their government.

Specifically, Canadian organizations are being hit across the spectrum. Statistics Canada now estimates that 20% of Canadian businesses are being impacted by cyber threats. According to the Conference Board of Canada 2020 report, almost 30% of the businesses that responded have seen an increase in cyber attacks, insider threats, and data breaches since the pandemic began. What this demonstrates is that cybercriminals have been taking advantage of the COVID-19 pandemic to increase what they're doing, with many focusing on ransom demands. Attacks coming into the corporate network are now migrating over to operational environments and have the ability to shut-down corporations.

A solution the private sector is starting to realize is that working together improves their cyber resilience and that sharing threat knowledge of what is happening actually works. Sharing cyber threat information should not be considered a competitive issue; all companies should understand the threat

environment that they are working in. Companies can compete on the products and services they provide, but everyone should operate from a basic understanding of what the cyber threat environment is and work accordingly. This is becoming recommended practice throughout the national cybersecurity strategy. The Canadian Cyber Threat Exchange (CCTX), for example, is the hub that allows Canadian companies to share and collaborate.

Question Period

To understand what prevents states from effectively using data to establish defensive strategies, we need to understand who owns the data and what kind of data is needed. There are a lot of data owners and there is also a lot of data of varying quality. Looking at this from a national perspective requires making nationally informed decisions, deciding what part of the data to focus on, and deciding how to process it. Once someone analyses the data, states need to determine how they will transmit that data and whether they would like to share it. For example, if they want to share it at a NATO level or any other group, a lot of these issues will influence decisions. If some of that data was from a private sector perspective, it is necessary to look at the competitive issues within that particular sector. Therefore, it is crucial to understand what data is, to think about how it will be used, and how to build up that stack right from the beginning.

KEY POINTS OF DISCUSSION

Presentation

- This data centric world is now calling for a re-evaluation of what is considered critical infrastructure.
- The establishment of a new cyber centre is part of a new step forward in collaboration between government and the private sector in Canada.
- Sharing knowledge from an international level to the private sector is also a new step moving forward.
- The private sector is starting to realize that working together improves their cyber resilience and that sharing threat knowledge works.

Question Period

- To understand what prevents states from effectively using data to establish defensive strategies, we need to understand who owns the data and what kind of data is needed

- It is crucial to understand what data is, to think about how it will be used, and how to build up that stack right from the beginning.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/