CYBER SECURITY, DATA PROTECTION, AND PRIVACY IN A CONTESTED GEO-POLITICAL ENVIRONMENT

Date: November 25, 2022

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 25, 2022, Aaron Shull, Managing Director, and General Counsel for the Centre for International Governance Innovation (Canada) presented on *Cyber Security, Data Protection, and Privacy in a Contested Geo-Political Environment.* The presentation was followed by a question-and-answer period with questions from the audience and CASIS Vancouver executives. The key points discussed were privacy rights—their limitations, relationship with technology, and overall value— as well as data exploitation and the need for improving cyber security postures for Small and Medium-sized Enterprises (SMEs).

NATURE OF DISCUSSION

Presentation

Mr. Shull provided insight into the interplay between cybersecurity and privacy, outlining the complex system of interactions between them at various levels of organisation. While the tension between cybersecurity and privacy is a critical factor, international human rights law—supported by several United Nations conventions—aims to heighten and protect the right to privacy. Likewise, the national level has several domestic frameworks that perform similar functions.

Question & Answer Period

Mr. Shull discussed privacy rights—their limitations, overall value, and relationship with technological comfort—as well as the possibility of personal data exploitation within future theatres of war. He also spoke on the domestic

industries and sectors that were currently ill-equipped to manage national threats through private–public sector collaboration.

BACKGROUND

Presentation

Mr. Shull noted that threats to sensitive user data and privacy have raised questions regarding what tools are available at the international and national level to address cybersecurity and privacy issues, as the number of global malware attacks continues to grow exponentially. Mr. Schull stated that the complexity of the interplay between cybersecurity and privacy is based on its integration of the roles involving businesses, standards, and individuals within a multi-stakeholder environment. At the international level, the right to privacy is a fundamental human right that is enshrined in several UN covenants; however, they are lax in regulating conduct in cyberspace. A suggested reason is the "gray zone" in which international law operates, meaning that current standards and frameworks can be ineffective in keeping pace with rapid technological changes, leading to adversarial actors exploiting the gray zone by interpreting existing frameworks to their full breadth. Mr. Shull stated that this issue can be alleviated somewhat at the national level—the development of Bills C-26, 27, and 59 provide policymakers with options for improving cybersecurity. C-26 allows for supply chain considerations, while C-27 provides a framework for private sector privacy and artificial intelligence legislation. C-59 is the most significant, as it gives the Communications Security Establishment (CSE) authority to conduct offensive and defensive cyber operations, as well as formulate a response based on a pattern of escalation. This model of escalation is indicative of the ecosystem in which cyberattacks transpire.

Mr. Shull suggested that the undermining of privacy by adversarial states and the scope of malware exploits by criminal enterprise requires reinforcing key vectors in the form of businesses, individuals, standards, and design so that the universal right to privacy can be upheld. Businesses—especially SMEs that are key factors to the Canadian economy—can benefit from undergoing cybersecurity certification provided by Cyber Secure Canada to achieve a baseline level of cybersecurity. The initiative is intended to underscore the safety and security principle of Canada's Digital Charter and ensure security of national digital and data platforms; thus, businesses that become certified would promote greater confidence in their business practices, as well as gain a competitive advantage. However, the current lack of awareness around this certification means that its advantages are going unnoticed.

Mr. Shull stated that optimal designs and up-to-date standards are key factors that should underpin regulatory frameworks seeking to improve SME cybersecurity practices, positing that well-developed standards provide consistency and act as an equaliser that gives regulatory frameworks the capacity to keep pace with the fast-changing cyberspace environment. Through standards and regular compliance enforcement, companies can be better protected. Regarding design, Mr. Shull contended that contemporary designs are failing to prioritise privacy, owing to a focus on data collection, use, amalgamation, and disclosure. This can have a significant impact on a user's ability to manage their data, as the choice of design can affect the ability to provide consent regarding the data they wish to provide. In this sense, individuals are the most vulnerable component since they are the least able to protect themselves from data breaches and can suffer the greatest consequences if it occurs.

Mr. Shull closed by discussing policy making, the ecosystem of cyber campaigns and criminality, design incentives, and cyberspace and privacy regulations. The current ecosystem is characterised by fast-changing technology and escalating cyber warfare between states. Criminal enterprises are also becoming more active through their increased malware activities. Collectively, this points to a cycle of warfare that will likely be defined by rapid escalation on behalf of offensive and defensive actors. As a result, Mr. Shull stated that policymakers face two obstacles. The first is addressing the lack of market incentives towards design that is privacy prioritising and secure and the second is educating individuals on key personal security measures, such as data trolls and differentiating between privacy secure and insecure software and applications. Mr. Shull added that policymakers must also seek to balance investigation and enforcement with compliance support, while noting that the slow and politically-charged legislative process means that there can be difficulty in keeping pace with technological evolution. Mr. Shull suggested that a possible solution would be to create governor-in-council powers that link standards, best practices, and certification programs to regulations that are aimed at creating cyber and privacy safeguards, which is an important long-term consideration.

Question & Answer Period

Mr. Shull provided clarity on his discussion of privacy rights, reiterating that, while the right to privacy was being undermined by state actors, one should not expect this right to extend towards cybersecurity. Currently, there is a dichotomy between the emphasising of privacy rights by state actors and an undermining of them as well, which does not point to there being a human right to cybersecurity in the near future.

In terms of the privacy rights relationship with tech-savviness, Mr. Schull found that individuals gravitate towards what is convenient and cost-effective, and are not likely to look at the downstream effects of influences that are subtly introduced by business models and advertising campaigns. Individualised ad targeting, sophisticated targeting algorithms, "nudge units", and cognitive biases arising from "lizard brains", play a role in commercialising attention. This could lead to problems as corporations continue to prioritise profits over social cohesion and well-being

Mr. Schull posited that the principle of distinction and proportionality means that armed forces are easily distinguishable from non-state actors and irregular forces; however, armed forces members that are outside the theatre of war remain vulnerable to adversarial aggression through cyber warfare. This new phenomenon in targeting behaviour is likely to increase in the future.

Mr. Schull stated that SMEs need to be prioritised and supported with a solid cybersecurity posture before strategic focus can be placed on larger and more significant entities. The approach should focus on ensuring that SMEs can achieve the baseline standards in cybersecurity, while saving the private-public sector collaboration for larger corporations.

KEY POINTS OF DISCUSSION

Presentation

- The current ecosystem is characterised by fast-changing technology, escalating cyber warfare between states, and increased malware exploits by criminal enterprises, creating a cycle of rapid escalation between adversaries.
- Canada's national security bill, Bill C-59, is significant because it gives the Communications Security Establishment (CSE) authority to conduct offensive and defensive cyber operations

- Policymakers face problems addressing the lack of market incentives regarding design that is privacy prioritising and secure, largely because consumers are unable to differentiate between software and applications that are privacy protective and secure, and those that are not.
- Policymakers should balance investigation and enforcement with compliance support.
- Governor-in-Council powers are a necessary substitute for the political process, due to its inability to keep pace with the evolving technological

environment. The purpose behind these powers should be to link standards, best practices, and certification programs to regulations aimed at creating cyber and privacy safeguards.

Question & Answer Period

- Armed forces members outside the theatre of war are vulnerable to personal data breaches through state-sponsored cyber-attacks. This is likely to increase in the future.
- Individualised ad targeting, targeting algorithms, and cognitive biases play a role in commercialising one's attention. This can lead to problems in the future as corporations continue to prioritise profits over societal cohesion and well-being
- It is crucial that SMEs can achieve baseline cybersecurity standards through certification before focusing on private-public sector collaboration, which will mainly involve larger corporations

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