For Public Release

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

TOP SECRET/[redacted] CANADIAN EYES ONLY

INTELLIGENCE ASSESSMENT

Overview of PRC Cyber Activities against Canada in 2021-2022

Intelligence Assessments Branch
Direction de l'évaluation du renseignement

Canadä

INTELLIGENCE ASSESSMENT

2023 07 20 TOP SECRET//[redacted]CANADIAN EYES ONLY CSIS IA 2023-24/46

Overview of PRC Cyber Activities against Canada in 2021 and 2022

In 2021–2022, the People's Republic of China (PRC) continued to pose the most significant cyber threat to Canada. PRC state actors conducted cyber intrusions [redacted] carrying out influence activities [redacted] the PRC is carrying out these cyber activities in order to gather intelligence that will aid PRC's goal of becoming a dominant international power [redacted]

Key Assessments

- PRC cyber targeting [redacted] was observed in both public and private sectors, [redacted]
- Canadian members of Parliament (MPs) and senators [redacted] victims of cyber targeting activities [redacted]
- Numerous federal government entities were targeted [redacted]
- [redacted]

- [redacted]

- [redacted] China poses a significant, complex and insidious cyber threat to the Government of Canada, Canadian critical infrastructure, Canadian private sector entities and technologies, and to the integrity of Canada's democracy. [redacted]

PRC cyber threat actors [redacted] target personally identifiable information (PII)

1. [redacted]

Global Governance

The Chinese party state's tech-enhanced authoritarianism is expanding globally [...] The CCP has a much more ambitious vision for harnessing a broad suite of current and emerging technologies in support of its own interests, including devices that might be seen as relatively benign, such as language translation technologies. By leveraging state-owned enterprises (SOEs), Chinese technology companies and partnerships with foreign partners – including Western universities – the CCP is building a massive and global data-collection ecosystem. The creation of that ecosystem gives the party control over large data flows. And, when the data is combined with artificial intelligence (AI) processing, the result can help build tools that can be used to shape, manage and control, including propaganda tools and the social credit system. Hoffman, Samantha. "Engineering global consent: The Chinese Communist Party's data-driven power expansion" p.3 (2019) *Australian Strategic Policy Institute.* (U)

[redacted]

(TS/[redacted] [redacted]

[1] Big Data is a term applied to the collection of datasets that are too large to be analyzed using traditional data-processing approaches. The term is associated with the explosion in data creation following the digital age of the 21st century; the collection, sale, analysis and exploitation of this data represents a major economic sector and indeed the primary economic value of much of the digital economy. All forms of predictive analysis, generative AI, and many other forms of data processing integral to the modern economy rely on Big Data. (U)

- In early January 2021, open sources indicated that PRC actors began actively exploiting several zero-day vulnerabilities within Microsoft Exchange Servers. Following the release of patches, in addition to using the zero day, threat actors also reverse engineered the patches to conduct exploitations. Most of the groups identified were conducting large-scale cyberespionage operations, including the acquisition of PII and IP. Victims of this exploitation campaign included state and local governments, policy think tanks, academic institutions, infectious disease researchers, law firms, defence contractors, and retailers worldwide. (U)

[redacted]

[redacted]

Microsoft Exchange Server involved wide sweeping and indiscriminate targeting

The Microsoft Exchange Server (MES) compromise has been described as one of the largest cyber exploitations to date. [redacted]

PRC government uses cyber as a means to conduct transnational repression activities

2. The Chinese government leveraged an array of tools—including cyber tools—to surveil, intimidate and coerce targeted individuals and groups abroad, including in Canada. [redacted]

[redacted]

[redacted]

- In October 2022, the Canadian branch of an international human rights organization detected a compromise by a likely Chinese state sponsored cyber group [redacted]

[redacted]

[redacted]

[redacted]

- On July 19, 2021, Canada joined a coalition of 39 countries in publicly attributing the Microsoft Exchange Network compromise (MES) campaign to the PRC. [redacted]

[redacted]

PRC leverages unique infrastructure to target Government entities

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] targeting of government officials in pursuit of political intelligence

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] (TS//[redacted] CEO)

- In [redacted] 2021, [redacted] that PRC cyber actors had targeted the House of Commons (HoC) [redacted] The threat actor [redacted] targeted work email accounts of *Parliamentarians* [redacted] with a tracking link email[5]. [redacted] members of the Inter-Parliamentary Alliance on China (IPAC), an international cross-party group of legislators [redacted] (TS//[redacted]

[redacted]

[redacted] targeting of personal accounts of GoC employees and politicians [redacted]

[redacted]

Threats to subnational governments

5. PRC cyber actors target Canadian municipal and provincial governments to gain access to the wealth of valuable information that often resides on their networks, [redacted] As providers of mostly routine government services used by Canadians, provincial and municipal governments hold a

[5] [redacted]

great deal of information of likely interest to PRC threat actors. [redacted]

[redacted]

[redacted]

Canadian universities [redacted]

6. Canadian universities represent high-value targets for PRC cyber actors. Universities serve as an invaluable source of data that align with PRC collection priorities to address its national economic development goals. The PRC's 14th Five-Year Plan outlined priorities for rapid advances in a number of technological fields, including energy, transportation, artificial intelligence (AI), computing, electronics, quantum, and sciences. Developing domestic Chinese research capacity is identified as key to the CCP's economic and political future. Illicit acquisition of foreign research and technology, including via cyber means, is considered a legitimate method to advance these goals. [redacted] (S)

[redacted]

- [redacted]

Science & technology remain a priority for PRC collection

7. [redacted] China is seeking to make advances in industries of economic value such as information technology, aviation, defence, maritime technology, and vaccines and virus treatments and is seeking breakthroughs in technologies that are critical to those sectors. [redacted] (S)

Military Civil Fusion (MCF)
According to the US Department of State, the MCF is an aggressive national strategy of the CCP designed to enable China to develop the most technologically advanced military in the world. The strategy aims to eliminate barriers between military, civilian, defence and commercial sectors of research within and outside the PRC, including illegally acquiring and diverting other nations' latest technology discoveries. (U)

[redacted]

[redacted] As a major mineral exporter and investor in global mining operations, Canada is highly involved in this sector[redacted]

Critical Infrastructure [redacted]

8. [redacted]

[redacted]

[redacted]

[redacted]

9 [redacted]

[redacted]

[redacted]

PRC [redacted] Canadian digital infrastructure [redacted]

[redacted]

[redacted]

11. [redacted]

[redacted]

[redacted]

(TS//[redacted] [redacted]

[redacted]

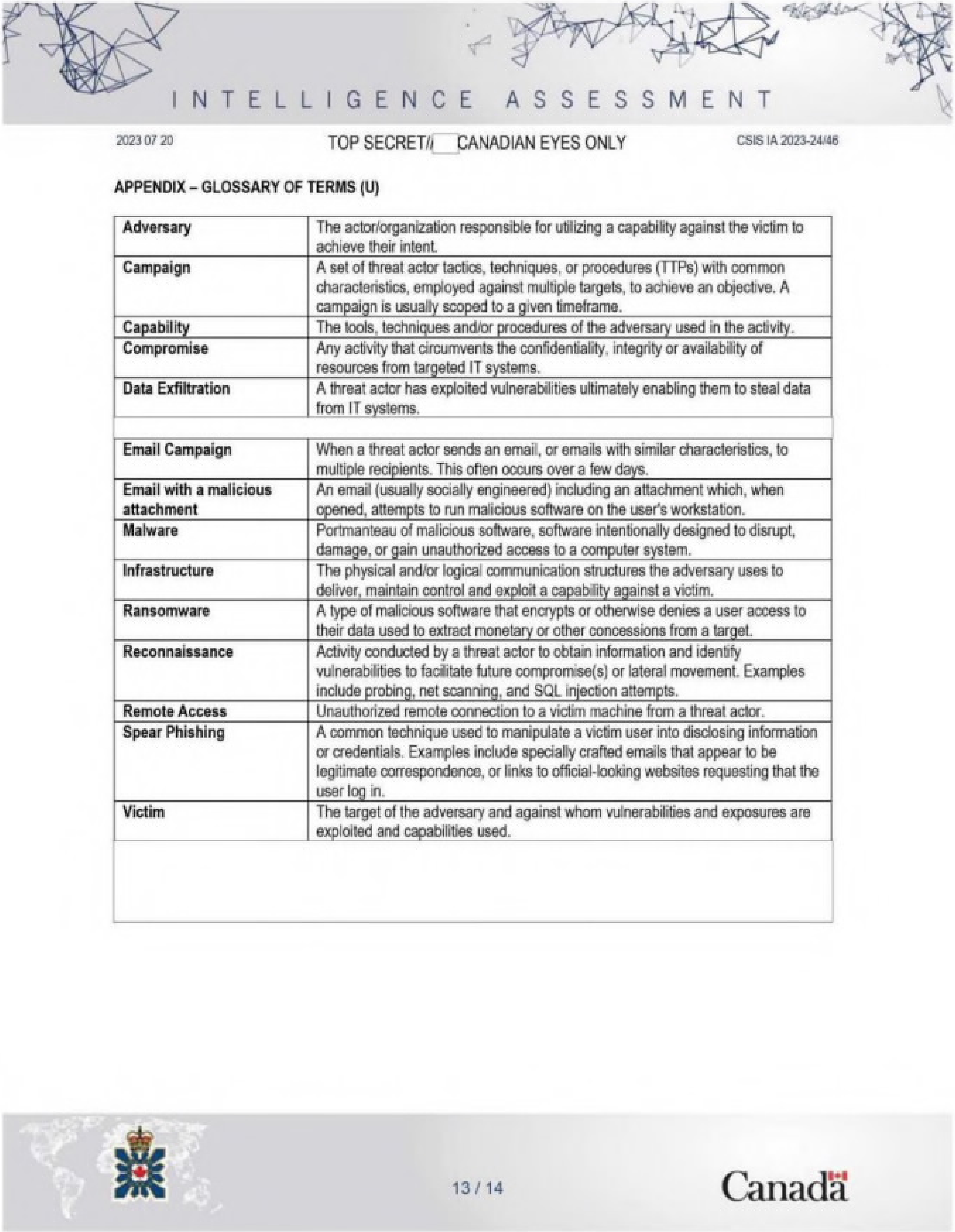
OUTLOOK

12. [redacted] The PRC is active in discovering and exploiting vulnerabilities to advance geopolitical objectives. [redacted]

13. PRC actors will continue to conduct malicious cyber operations against Canadian government networks and personnel. Cyber threat activity targeting Canadian government entities is almost certainly aligned with PRC objectives [redacted] the GoC will likely remain a priority target for PRC cyber collection activities. (TS//[redacted]

14. [redacted]

15. [redacted] in part due to PRC national regulations in effect since 2021 that require private industry to report to the PRC's Ministry of Industry and Information Technology any security vulnerabilities detected in their products within two days before issuing patches to fix the flaws or providing information on the vulnerabilities to the general public. [redacted] (S//CEO)



APPENDIX – GLOSSARY OF TERMS (U)

Adversary	The actor/organization responsible for utilizing a capability against the victim to achieve their intent.
Campaign	A set of threat actor tactics, techniques, or procedures (TTPs) with common characteristics, employed against multiple targets, to achieve an objective. A campaign is usually scoped to a given timeframe.
Capability	The tools, techniques and/or procedures of the adversary used in the activity.
Compromise	Any activity that circumvents the confidentiality, integrity or availability of resources from targeted IT systems.
Data Exfiltration	A threat actor has exploited vulnerabilities ultimately enabling them to steal data from IT systems.
Email Campaign	When a threat actor sends an email, or emails with similar characteristics, to multiple recipients. This often occurs over a few days.
Email with a malicious attachment	An email (usually socially engineered) including an attachment which, when opened, attempts to run malicious software on the user's workstation.
Malware	Portmanteau of malicious software, software intentionally designed to disrupt, damage, or gain unauthorized access to a computer system.
Infrastructure	The physical and/or logical communication structures the adversary uses to deliver, maintain control and exploit a capability against a victim.
Ransomware	A type of malicious software that encrypts or otherwise denies a user access to their data used to extract monetary or other concessions from a target.
Reconnaissance	Activity conducted by a threat actor to obtain information and identify vulnerabilities to facilitate future compromise(s) or lateral movement. Examples include probing, net scanning, and SQL injection attempts.
Remote Access	Unauthorized remote connection to a victim machine from a threat actor.
Spear Phishing	A common technique used to manipulate a victim user into disclosing information or credentials. Examples include specially crafted emails that appear to be legitimate correspondence, or links to official-looking websites requesting that the user log in.
Victim	The target of the adversary and against whom vulnerabilities and exposures are exploited and capabilities used.

INTELLIGENCE ASSESSMENT

2023 07 20 TOP SECRET//[redacted]CANADIAN EYES ONLY CSIS IA 2023-24/46

[redacted]

CSIS_PUBLICATIONS / SCRS_ PUBLICATIONS

THIS INFORMATION IS SHARED WITH YOUR ORGANIZATION FOR INTELLIGENCE PURPOSES ONLY AND MAY NOT BE USED IN LEGAL PROCEEDINGS. THIS DOCUMENT MAY NOT BE RECLASSIFIED, DISSEMINATED OR DISCLOSED IN WHOLE OR IN PART WITHOUT THE WRITTEN PERMISSION OF CSIS. THIS DOCUMENT CONSTITUTES A RECORD WHICH MAY BE SUBJECT TO EXEMPTIONS UNDER THE FEDERAL ACCESS TO INFORMATION ACT OR PRIVACY ACT OR UNDER APPLICABLE PROVINCIAL OR TERRITORIAL LEGISLATION. IF A REQUEST FOR ACCESS UNDER THESE ACTS IS MADE, THE RECEIVING AGENCY MUST CONSULT CSIS IN RELATION TO APPLYING THE AVAILABLE EXEMPTIONS. FURTHER, CSIS MAY TAKE ALL NECESSARY STEPS UNDER SECTION 38 OF THE CANADA EVIDENCE ACT OR OTHER LEGISLATION TO PROTECT THIS INFORMATION. IF YOU LEARN THAT THIS INFORMATION HAS OR MAY BE DISCLOSED, THAT THESE CAVEATS HAVE NOT BEEN RESPECTED OR IF YOU ARE UNABLE TO ABIDE BY THESE CAVEATS, INFORM CSIS IMMEDIATELY.