TOP SECRET//SI//CANADIAN EYES ONLY

Communications Security Establishment | Centre de la sécurité des télécommunications

Canadian Cyber Operations

Summary

- The cyberspace has become, and remains, a strategic domain for adversarial states given the low-cost and high impact of cyber operations. States such as Russia and the PRC have used cyber operations to target critical infrastructure, advance foreign policy, and as a tool of statecraft.
- Non-state actors, such as violent extremists, use cyber networks and online platforms to recruit and radicalize.
- CSE engages in active and defensive cyber operations collaboratively with the CAF and allies to reduce the threat posed by foreign cyber operations and to disrupt networks that pose a critical threat to Canadian national security.
- s. 39 - Cabinet Confidence

Intent

(U//OUO) This paper provides an overview of CSE and CAF's cyber operations. The paper further explores existing capacity gaps and recommendations to help bridge these gaps as part of upcoming policy discussions.

Introduction

(U) Foreign cyber operations are a comparatively cost-effective, versatile, agile, and far-reaching tool for addressing foreign violent extremist threats, particularly in situations where traditional means, such as law enforcement or kinetic activities, would not be feasible or effective.

(S//CEO) Cyberspace will continue to be an active military and warfighting domain for adversarial states, such as Russia.

(TS//SI) CSE has been conducting Active Cyber Operations activities since early 2020.

(TS//SI) While CSE has standing authority to counter foreign cyber threats to Canada's democratic processes and related institutions – which included attempts by state, state-affiliated, and non-state cyber threat actors to manipulate online information or disseminate false information in order to influence voters' opinion and behaviours –

GCdocs #75411304

Canada

(S//CEO) Cyber operations are operations conducted through cyberspace that produce tangible outcomes, such as shutting down networks, disrupting communications, and denying access.

(S//CEO) Sometimes thought as "offensive" cyber operations, they can be used to disrupt, degrade, influence, respond to or interfere with the capabilities, intentions or activities of state and non-state threat actors, to achieve a desired effect or outcome.

(S//CEO) While cyber operations are by their nature always conducted through cyberspace, they can be designed to have effects in the real world (e.g. disrupting the ability of an adversary's military to deliver fuel, ammunition and other necessities to its forces).

Threat Landscape

Russia

(TS//SI) Russia employs active cyber operations to disrupt Canadian and allied equities to pursue foreign policy and statecraft objectives. Russia presents cyber threat in numerous environments,

(S//CEO) Since the start of the war, Russia has conducted active cyber operations against Ukrainian

Disinformation

(TS//SI) Russia seeks to influence Canadians by damaging the foundations of trust in our free and open society, such as by degrading public belief in government institutions and news media. The use of targeted disinformation campaigns in the manner ultimately poses a threat to democracy itself. The PRC disinformation campaigns unfold principally in cyberspace, where falsified information intended to manipulate, sow confusion, or guide people in the wrong direction is propagated at the scale and speed of technology.

(TS//SI) Russia is employing disinformation to confront Western nations while ensuring protection and stability of its regime.

(TS//SI) Canada is often impacted through the collateral effects of Russia's disinformation efforts targeting other Western democracies, NATO, and the US.

People's Republic of China's (PRC)

(TS//SI) The PRC employs active cyber operations to disrupt Canadian and allied equities to pursue foreign policy and statecraft objectives. The PRC is a highly sophisticated cyber threat actors

Disinformation

(TS//SI) The PRC seeks to influence Canadians by damaging the foundations of trust in our free and open society, such as by degrading public belief in government institutions and news media. The use of targeted disinformation campaigns in the manner ultimately poses a threat to democracy itself. The PRC disinformation campaigns unfold principally in cyberspace, where falsified information intended to manipulate, sow confusion, or guide people in the wrong direction is propagated at the scale and speed of technology.

(TS//SI) The PRC uses disinformation as a tool to control the global information environment and advance its core strategic goals, including: projecting a positive image abroad; countering narratives that are not in the PRC's interest;

Other Actors

Violent Extremism

(TS//SI) The expansion of the digital world poses new threat given the ability for threat actors to exploit online platforms for borderless recruitment and radicalization. Cyberspace expands the tools, platforms and reach of violent extremist actors, enabling them to sow and grow grievances and narratives in relative anonymity

through various tactics, which include mis/disinformation.

(TS//SI) Canada's population continues to grow, become more diverse and connected to the rest of the world, and is, through modern technologies and social media, exposed to radical political views promoted by foreign and domestic actors. The Government of Canada should consider if and how these realities factor into a growing risk of violent extremism, including at home.

India

(TS//SI) India is using disinformation to project a positive image globally, while targeting specific adversaries. This includes countering activities it considers as "anti-India" including the Khalistan movement. influence the Canadian diaspora and Canadian decision-making

CSE's Cyber Operations

(S//CEO) CSE's teams received a wide variety of which have served to:

- Disrupt and interfere with malware and ransomware threats to Canadians and Canadian organizations;
- Counter Russian disinformation following Russia's invasion of Ukraine; and
- Disrupt

(S//CEO) Intelligence was used for strategic (e.g., senior executive briefings, operational and tactical purposes With respect to interactions that have facilitated this success, CSE's teams work very closely with CSE groups This includes regular meetings to discuss requirements and priorities and share findings amongst the community.

(U//OUO) See Annexes A and B for recent operational examples and successes.

(TS//SI) CSE and DND/CAF participate in

(TS//SI) CSE provides cyber support to CAF missions abroad, including **Op UNIFIER**.

Cyber Authorizations, Legislative and Regulatory Instruments

CSE Act of 2019

(U) Ss. 18 and 19 of the *CSE Act* of 2019 authorizes CSE to conduct active and defensive cyber operations. CSE is authorized to carry out activities on or through the global information infrastructure to help protect federal institutions' electronic information and information infrastructures and electronic information and information infrastructures of importance to the Government of Canada. CSE is also authorized to conduct activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security.

(U) Under s. 29 of the *CSE Act* of 2019, the Minister of National Defence may issue Defensive Cyber Operations Authorizations that authorize CSE to carry out defensive cyber operations. The Minister of National Defence must consult with the Minister of Foreign Affairs before issuing an Authorization.

(U) Under s. 30 of the *CSE Act* of 2019, the Minister of National Defence may issue Active Cyber Operations Authorizations that may authorize CSE to carry out active cyber operations. The Minister of National Defence must consult with the Minister of Foreign Affairs before issuing an Authorization and must obtain written consent as soon as feasible.

(U) Under s. 32 of the *CSE Act* of 2019, CSE is prohibited from carrying out any activity that causes, intentionally or by criminal negligence, death or bodily harm to an individual or wilfully attempts in any matter to obstruct, pervert or defeat the course of justice or democracy.

(S) With the consent of the Minister of Foreign Affairs, the Minister of National Defence can authorize and direct CSE to conduct cyber activities to address the threat

CSE's Cyber Operations Partnership Initiatives

Limitations and Prohibitions

(S) Due to the drafting of the *CSE Act*, CSE cannot conduct activities activities that result in the "detention", "seizure", or "forfeiture" of funds rendered inaccessible.

Policy Discussion

s. 39 - Cabinet Confidence

Status Quo: Current Capacity

(S//CEO) Since the 2019 *CSE Act*, CSE has leveraged Budget 2022 funds to

(S//CEO) Within 15 years,

Enhanced Target Investment (RECOMMENDED//RATIFIED)

GCdocs # [APG]

Canada

(S//CEO) Within 15 years,

Substantial Long-Term Investment

(S//CEO) Substantial long-term investments would enable Canada

(S//CEO) Within 15 years,

National Cyber Security Strategy

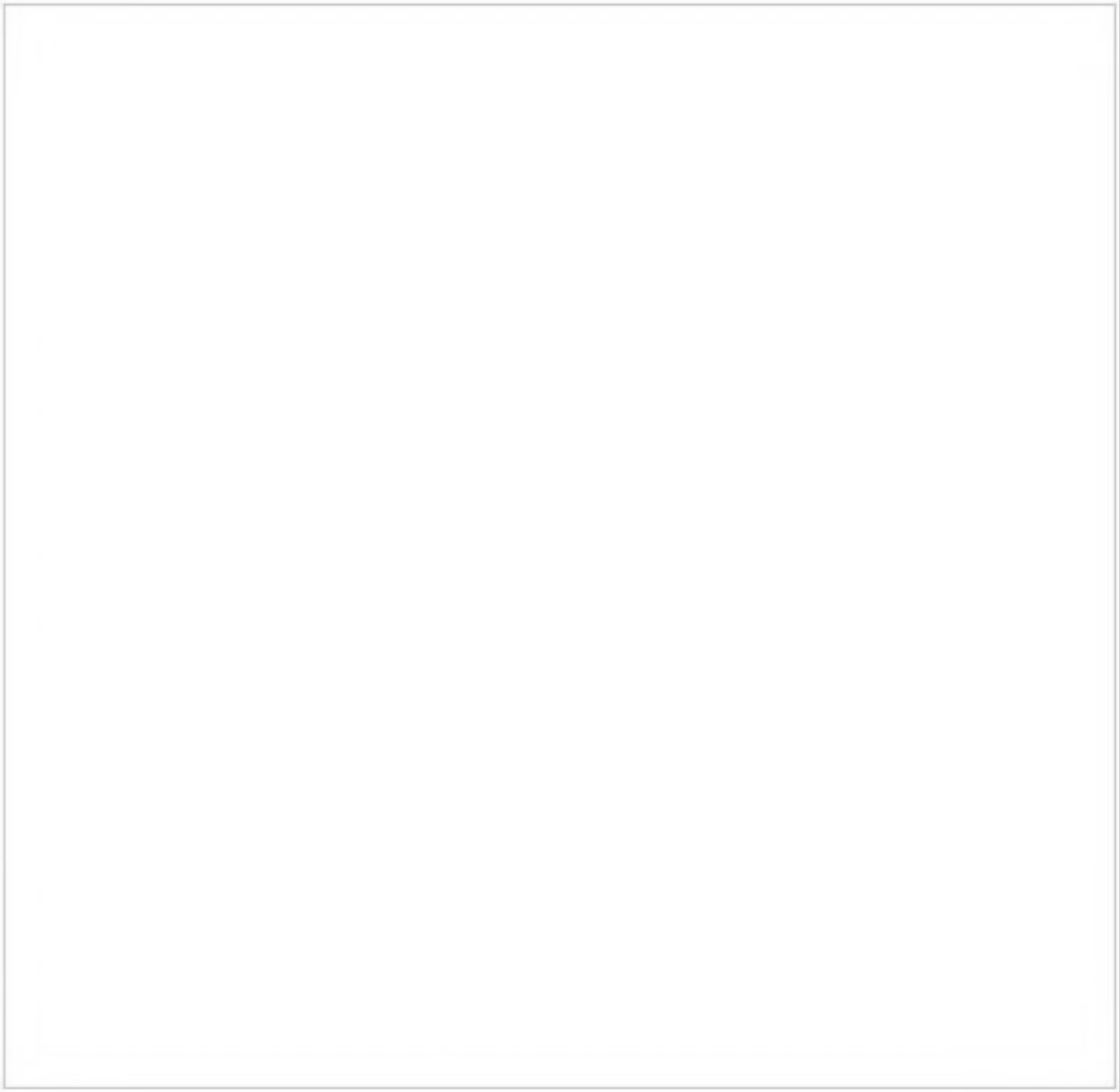
s. 39 - Cabinet Confidence

Annex A – Operational Successes

(S//CEO) CSE's teams received a wide variety of which have served to:

- Disrupt and interfere with malware and ransomware threats to Canadians and Canadian organizations;
- Counter Russian disinformation following the invasion of Ukraine; and
- Disrupt

(S//CEO) Intelligence was used for strategic (e.g., senior executive briefings, operational and tactical purposes With respect to interactions that have facilitated this success, CSE's teams work very closely with CSE groups . This includes regular meetings to discuss requirements and priorities and share findings amongst the community.



Annex B – Recent Operations

GCdocs # [APG]

Canada