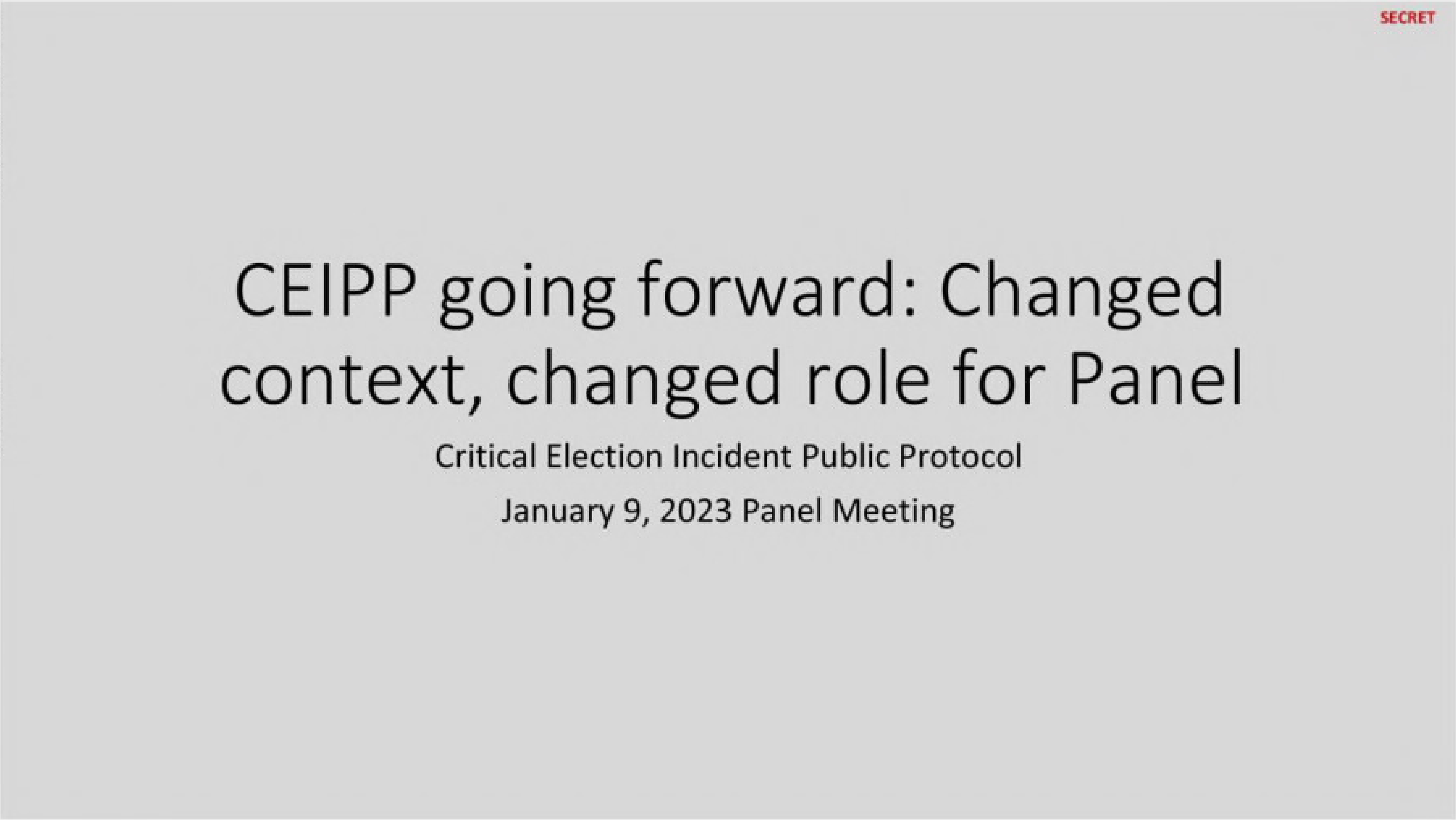


SECRET

CEIPP going forward: Changed context, changed role for Panel

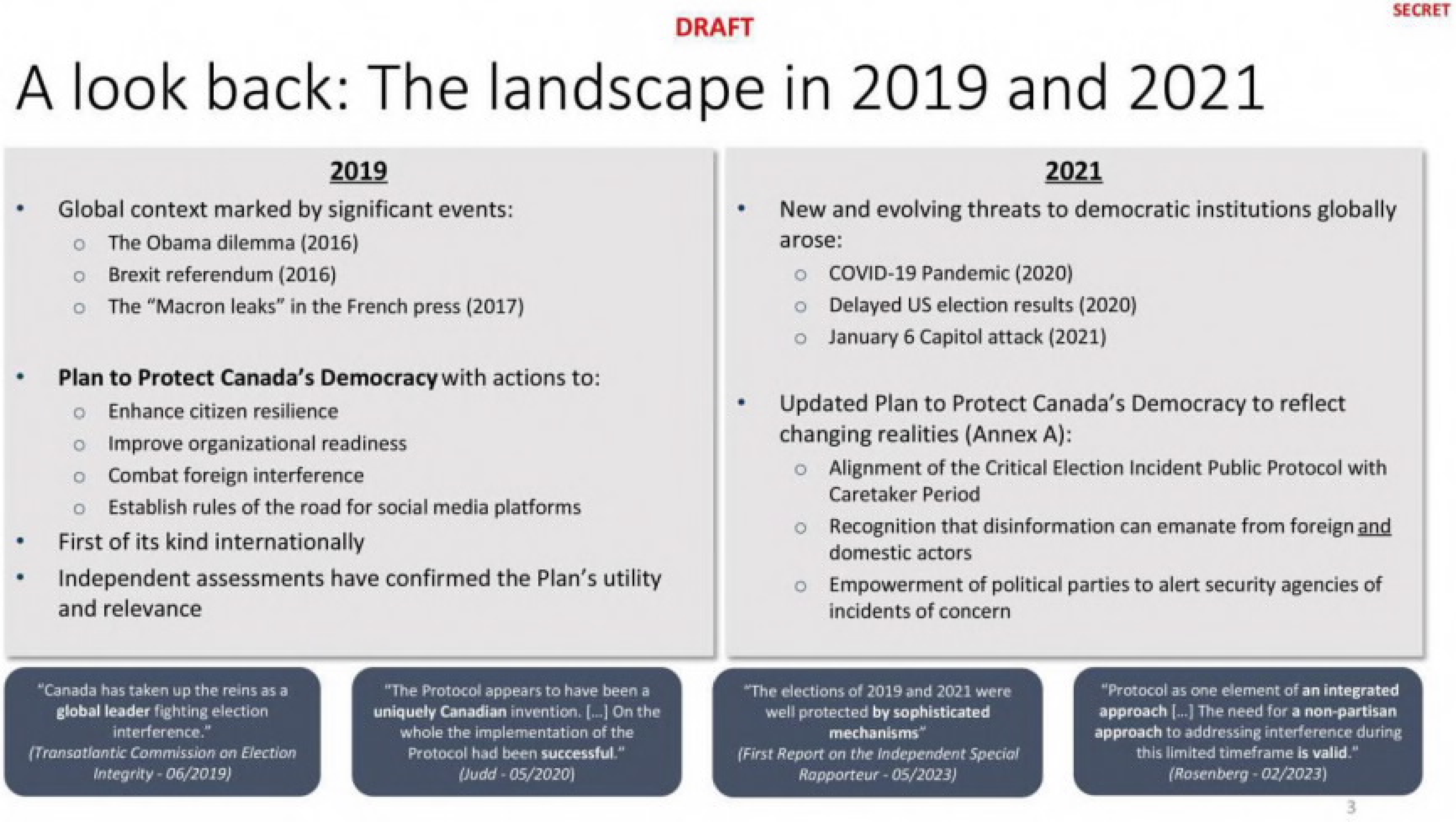
Critical Election Incident Public Protocol

January 9, 2023 Panel Meeting

SECRET

CEIPP: how the context has evolved

- The Critical Election Incident Public Protocol and the Panel have been in place for two general elections (2019 and 2021)
- Attention on the Panel in 2019 and 2021 was not particularly significant – media, political parties treated it as one element of Canada's election ecosystem
- The Canadian and global contexts have changed considerably since 2021 when the Panel was last active, including through evolving methods used by adversaries
    - o Since Russia's invasion of Ukraine in February 2022, efforts by NATO members, including Canada, to aggressively call out Russian disinformation operations
- Since late 2022, there has been increased Parliamentary interest in the role of the Panel and SITE Task Force. It will also likely be raised in the various ongoing reviews on foreign interference (ie. NSICOP, NSIRA, PROC, Public Inquiry).
    - o Growing expectation that Canadians will be informed of events and information affecting Canada's national security, including efforts to interfere



DRAFT

SECRET

A look back: The landscape in 2019 and 2021

2019

- Global context marked by significant events:
  - The Obama dilemma (2016)
  - Brexit referendum (2016)
  - The "Macron leaks" in the French press (2017)
- **Plan to Protect Canada's Democracy** with actions to:
  - Enhance citizen resilience
  - Improve organizational readiness
  - Combat foreign interference
  - Establish rules of the road for social media platforms
- First of its kind internationally
- Independent assessments have confirmed the Plan's utility and relevance

2021

- New and evolving threats to democratic institutions globally arose:
  - COVID-19 Pandemic (2020)
  - Delayed US election results (2020)
  - January 6 Capitol attack (2021)
- Updated Plan to Protect Canada's Democracy to reflect changing realities (Annex A):
  - Alignment of the Critical Election Incident Public Protocol with Caretaker Period
  - Recognition that disinformation can emanate from foreign and domestic actors
  - Empowerment of political parties to alert security agencies of incidents of concern

"Canada has taken up the reins as a **global leader** fighting election interference."
(Transatlantic Commission on Election Integrity - 06/2019)

"The Protocol appears to have been a **uniquely Canadian** invention. [...] On the whole the implementation of the Protocol had been **successful**."
(Judd - 05/2020)

"The elections of 2019 and 2021 were well protected **by sophisticated mechanisms**"
(First Report on the Independent Special Rapporteur - 05/2023)

"Protocol as one element of **an integrated approach** [...] The need for **a non-partisan approach** to addressing interference during this limited timeframe **is valid**."
(Rosenberg - 02/2023)

DRAFT

SECRET

Escalation and heightened attention: 2022 and 2023

2022

- Rapid escalation of disinformation narratives, melding foreign and domestic
  - Russia's invasion of Ukraine
  - Aftermath of COVID-19 pandemic
  - Convoy 2022 and Public Order Emergency Commission

- New investments in 2022 to:
  - Renew Rapid Response Mechanism, to monitor and respond to foreign state actors
  - Renew Digital Citizen Initiative to build citizen digital literacy and resilience
  - Create the Protecting Democracy Unit at the Privy Council Office
  - Build capacity in civil society by establishing the Canadian Digital Media Research Network

2023

- Increased attention on foreign interference
  - Media coverage since late 2022, based in part on leaked intelligence documents (Fife & Chase; Cooper)
  - Parliamentary reviews
  - Independent Special Rapporteur & Public Inquiry into Foreign Interference Federal Electoral Processes and Democratic Institutions

- Further signals to combat foreign interference and disinformation:
  - LeBlanc-Charette report, April 2023
  - Activation of the Security and Intelligence Threats to Elections (SITE) Task Force for by-elections
  - Public statements bringing transparency to information operations affecting Parliamentarians
  - Creation of disinformation and foreign interference toolkits, as well as a guidebook for public servants

DRAFT

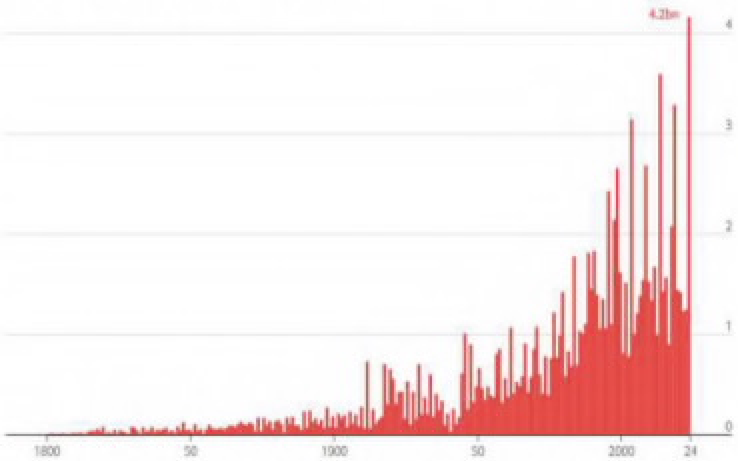
SECRET

The Panel is operating in a new context ...

2024 is the biggest election year in history

- The Economist, November 2023

People in countries with an election that year, bn



*Includes legislative, presidential and EU elections, as well as nationwide elections at the municipal or regional level in 2024 and in 1950-23 for countries of over 100m people

Geopolitical conflicts

- Increase in disinformation in the Canadian information ecosystem and potential impact on social cohesion
- Higher impact on diaspora communities
- Disinformation as a tool in conflict

Rapidly developing artificial intelligence (AI)

- More sophisticated disinformation at lower cost
- Improved and widely available techniques
- Capability to produce convincing material

Changes amongst platforms

- Platforms loosening approach to standards
- Less predictability in platform response (X/Twitter and others)
- Increasingly challenging to engage with platforms at national level

Increased attention on foreign interference

- Some 70 elections, including US, India and EU, expected in 2024
- Impact of foreign interference and disinformation in elections abroad impacts domestic trust in electoral processes
- Increased parliamentary and media attention to issues related to foreign interference

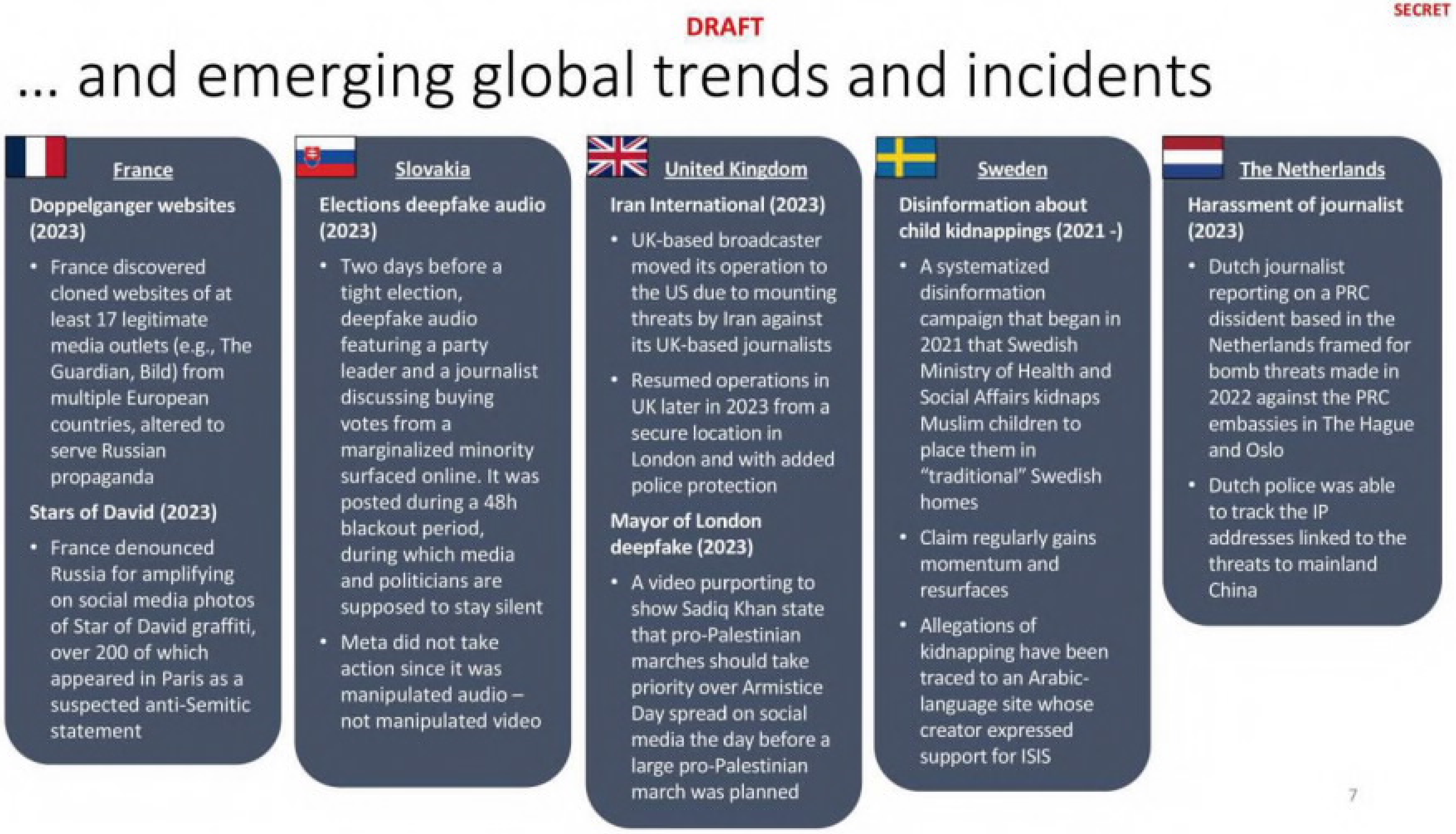
Critical that GoC learns from the Year of Democracy

SECRET

DRAFT

… which includes recent Canadian incidents …

Incident	Context	Lessons learned
Targeting of Member of Parliament Michael Chong through a WeChat information operation, featuring "highly probable" involvement from PRC	• GC detected the information operation through Rapid Response Mechanism Canada, which, as a member of the SITE Task Force, was monitoring by-elections for interference for the first time • GC issued public statement and briefed MP Chong	• Incident only found because SITE was active for by-elections • There is no established GC process to determine when/how to make findings public • Reaction to the decision to make findings public was factual, robust and in some cases actively complementary of GC's efforts
Targeting of Canadian Parliamentarians by likely PRC-linked 'spamouflage' campaign	• GC became aware of spamouflage campaign through information received from [redacted] • Spamouflage refers to a network of new or hijacked social media accounts that posts and increases the number of propaganda messages across multiple social media platforms • GC issued public statement and sent letters to affected MPs	• GC relied on international partners for detection • Civil society played key role in detection and response • GC response built on MP Chong process for determination of whether and how to go public • Reaction to the decision to make findings public was largely similar to MP Chong/WeChat report
Disinformation about Canada-India relations following PM's September 18, 2023, statement in the House of Commons	• Indian media was rife with disinformation about Canada-India relations, some of which spilled over to Canadian media • Diaspora communities specifically exposed to such disinformation	• Determination of when and how to respond by GC was made on ad hoc basis in the absence of an established response framework



SECRET

DRAFT

… and emerging global trends and incidents

France

Doppelganger websites (2023)

- France discovered cloned websites of at least 17 legitimate media outlets (e.g., The Guardian, Bild) from multiple European countries, altered to serve Russian propaganda

Stars of David (2023)

- France denounced Russia for amplifying on social media photos of Star of David graffiti, over 200 of which appeared in Paris as a suspected anti-Semitic statement

Slovakia

Elections deepfake audio (2023)

- Two days before a tight election, deepfake audio featuring a party leader and a journalist discussing buying votes from a marginalized minority surfaced online. It was posted during a 48h blackout period, during which media and politicians are supposed to stay silent
- Meta did not take action since it was manipulated audio – not manipulated video

United Kingdom

Iran International (2023)

- UK-based broadcaster moved its operation to the US due to mounting threats by Iran against its UK-based journalists
- Resumed operations in UK later in 2023 from a secure location in London and with added police protection

Mayor of London deepfake (2023)

- A video purporting to show Sadiq Khan state that pro-Palestinian marches should take priority over Armistice Day spread on social media the day before a large pro-Palestinian march was planned

Sweden

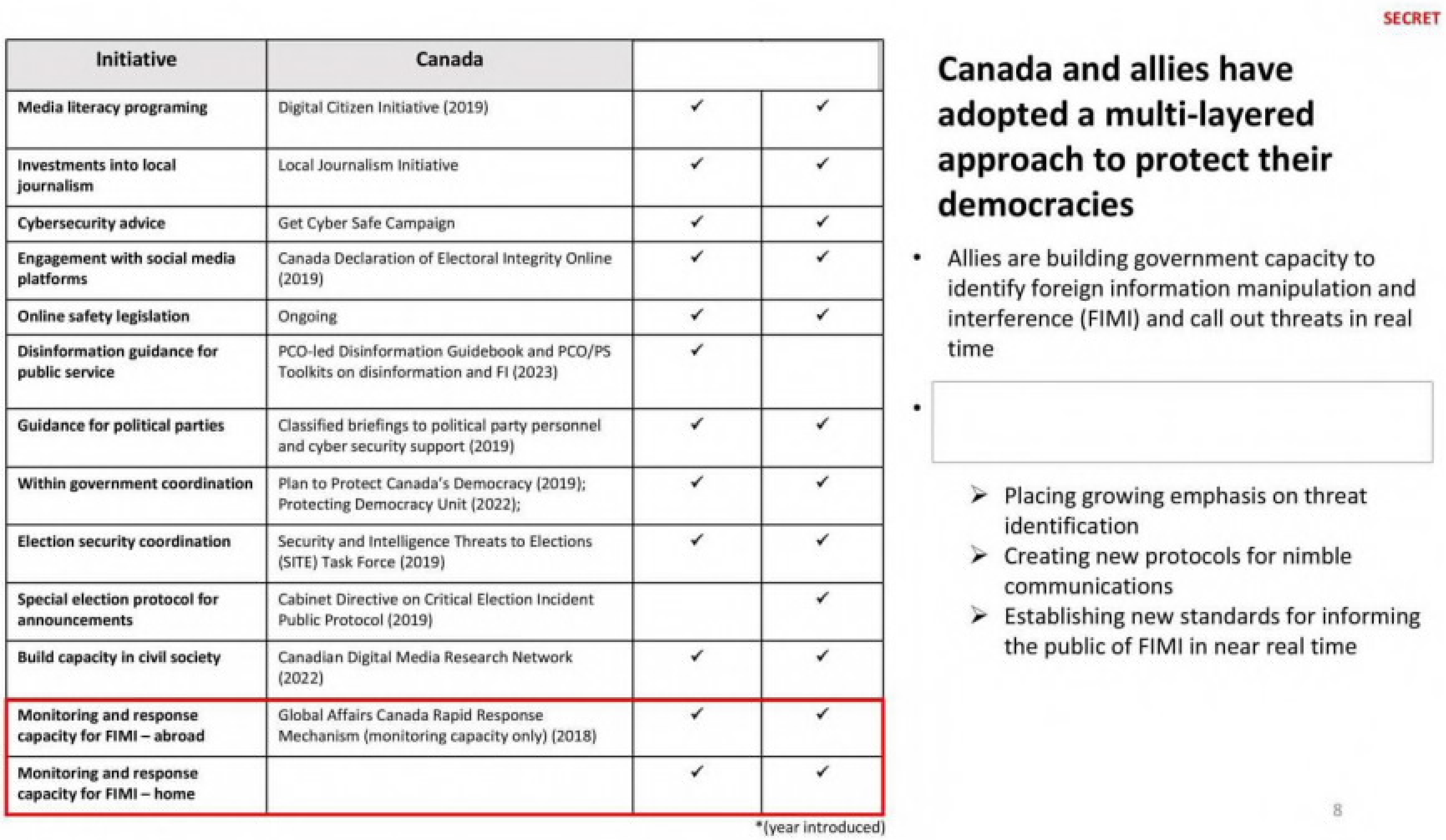
Disinformation about child kidnappings (2021 -)

- A systematized disinformation campaign that began in 2021 that Swedish Ministry of Health and Social Affairs kidnaps Muslim children to place them in "traditional" Swedish homes
- Claim regularly gains momentum and resurfaces
- Allegations of kidnapping have been traced to an Arabic-language site whose creator expressed support for ISIS

The Netherlands

Harassment of journalist (2023)

- Dutch journalist reporting on a PRC dissident based in the Netherlands framed for bomb threats made in 2022 against the PRC embassies in The Hague and Oslo
- Dutch police was able to track the IP addresses linked to the threats to mainland China



SECRET

Initiative	Canada	[redacted]	
Media literacy programing	Digital Citizen Initiative (2019)	✓	✓
Investments into local journalism	Local Journalism Initiative	✓	✓
Cybersecurity advice	Get Cyber Safe Campaign	✓	✓
Engagement with social media platforms	Canada Declaration of Electoral Integrity Online (2019)	✓	✓
Online safety legislation	Ongoing	✓	✓
Disinformation guidance for public service	PCO-led Disinformation Guidebook and PCO/PS Toolkits on disinformation and FI (2023)	✓	
Guidance for political parties	Classified briefings to political party personnel and cyber security support (2019)	✓	✓
Within government coordination	Plan to Protect Canada's Democracy (2019); Protecting Democracy Unit (2022);	✓	✓
Election security coordination	Security and Intelligence Threats to Elections (SITE) Task Force (2019)	✓	✓
Special election protocol for announcements	Cabinet Directive on Critical Election Incident Public Protocol (2019)		✓
Build capacity in civil society	Canadian Digital Media Research Network (2022)	✓	✓
Monitoring and response capacity for FIMI – abroad	Global Affairs Canada Rapid Response Mechanism (monitoring capacity only) (2018)	✓	✓
Monitoring and response capacity for FIMI – home		✓	✓

*(year introduced)

Canada and allies have adopted a multi-layered approach to protect their democracies

- Allies are building government capacity to identify foreign information manipulation and interference (FIMI) and call out threats in real time
- [redacted]
  - ➢ Placing growing emphasis on threat identification
  - ➢ Creating new protocols for nimble communications
  - ➢ Establishing new standards for informing the public of FIMI in near real time

SECRET

Looking ahead: Applying the CEIPP in 2024/2025

The threat remains constant and evolving

- "...increased tensions or antagonism between Canada and a hostile state is very likely to result in cyber threat actors aligned with that state targeting Canada's democratic processes or disrupting Canada's online information ecosystem ahead of a national election." (CSE, 2023)
- "We assess it very likely that cyber threat actors are increasingly using obfuscation techniques and/or are outsourcing their cyber activities in order to hide their identities or links to foreign governments" (CSE, 2023)
- "...the greatest strategic challenges to Canada's sovereignty and democracy are the threats of foreign interference or transnational repression and state sponsored foreign espionage." (CSIS Director Vigneault, 2023)
- "There is no doubt that foreign governments are attempting to influence candidates and voters [...] This is a growing threat to our democratic system..." (Independent Special Rapporteur, 2023)

During the next election, the Panel must be prepared to apply the Protocol in the context of:

➢ Heightened interest from Canadians, media, and Parliamentarians in foreign interference in Canada's elections

➢ New expectations by Canadians and precedent by GC to share information about FI threats, including through public reports

FOR DISCUSSION

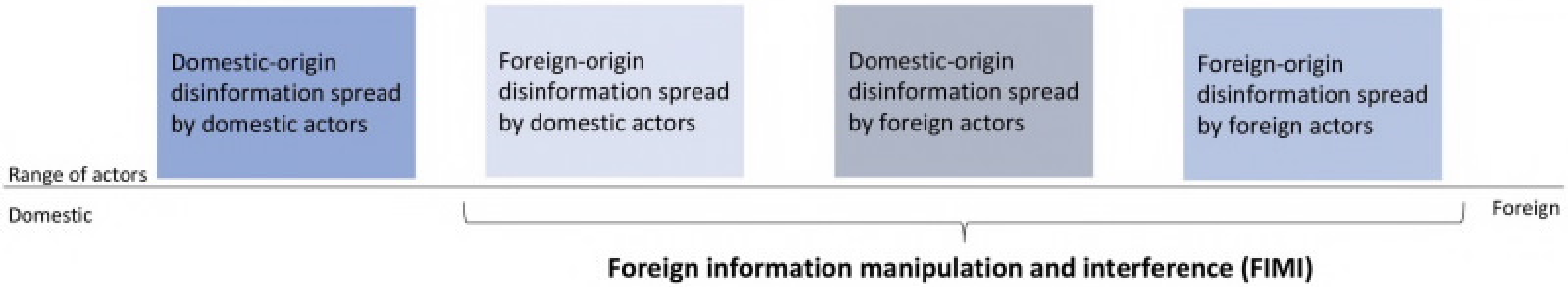
SECRET

Looking ahead: Applying the CEIPP in 2024/2025

- Allies' efforts to call out disinformation are increasingly based on uncovering the mechanisms behind a message without weighing in on the accuracy of its contents
  - Such a "networks not narratives approach" focuses on identifying how disinformation is being shared, and where possible, by what type of actor

- While challenges remain with attribution, disinformation campaigns may feature characteristics corresponding to known actors in the space
  - In its October 2023 statement, short of attributing the 'spamouflage' campaign to PRC with certainty, GAC highlighted that spamouflage as a tactic has been tied by experts to the PRC and concluded it "probable" that PRC was behind the campaign

> "The majority of cyber threat activity targeting elections is unattributed […] In 2022, 85% of cyber threat activity targeting elections was unattributed, meaning that these cyber incidents are not ascribed or credited to a state-sponsored cyber threat actor." (CSE, 2023)



Domestic-origin disinformation spread by domestic actors

Foreign-origin disinformation spread by domestic actors

Domestic-origin disinformation spread by foreign actors

Foreign-origin disinformation spread by foreign actors

Range of actors

Domestic

Foreign

Foreign information manipulation and interference (FIMI)