CANADIAN CENTRE FOR CYBER SECURITY

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

2024-01-25

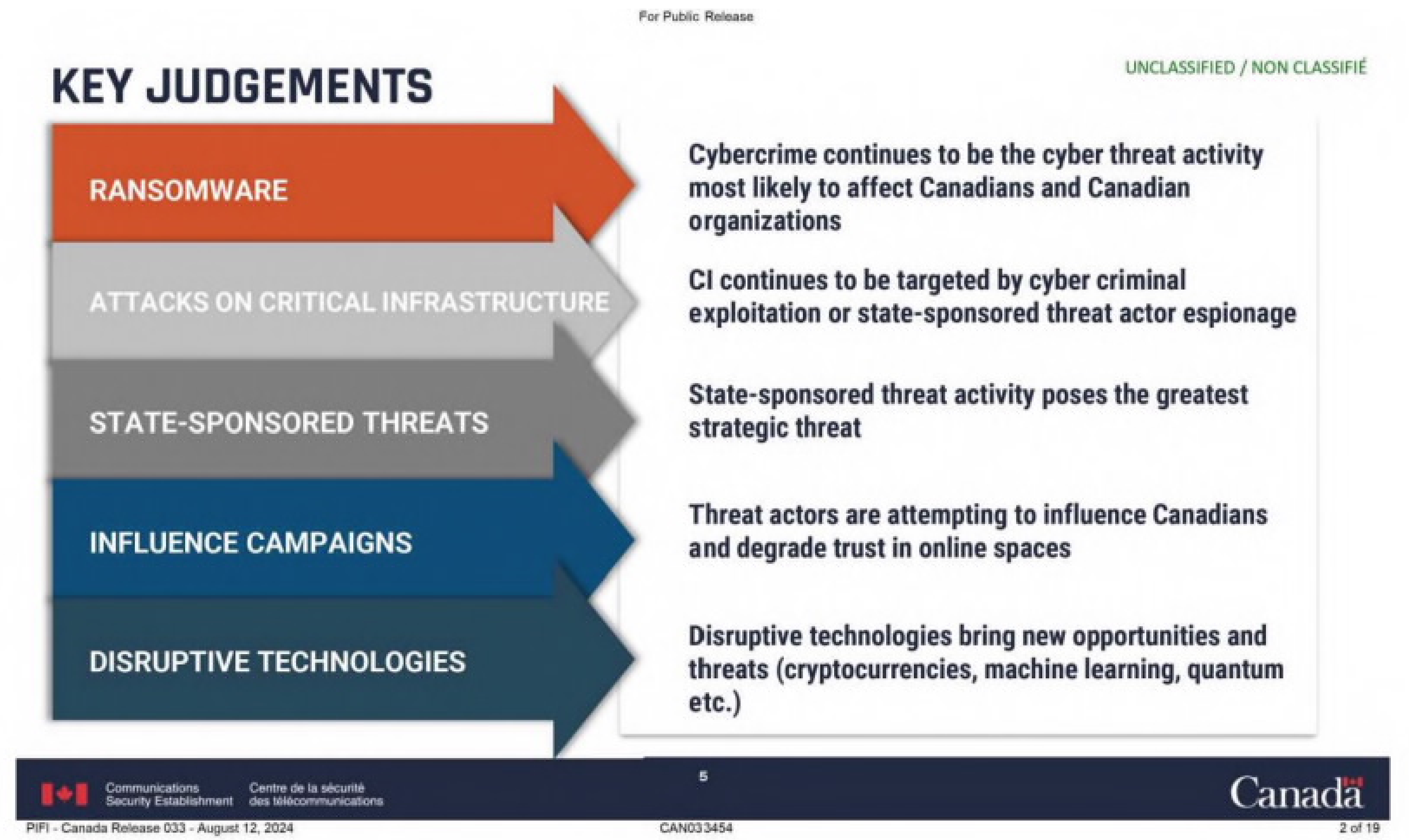
The National Cyber Threat Assessment

2023-2024

Communications Security Establishment
Centre de la sécurité des télécommunications

GCdocs 15333161

Canada



For Public Release

UNCLASSIFIED / NON CLASSIFIÉ

KEY JUDGEMENTS

RANSOMWARE

Cybercrime continues to be the cyber threat activity most likely to affect Canadians and Canadian organizations

ATTACKS ON CRITICAL INFRASTRUCTURE

CI continues to be targeted by cyber criminal exploitation or state-sponsored threat actor espionage

STATE-SPONSORED THREATS

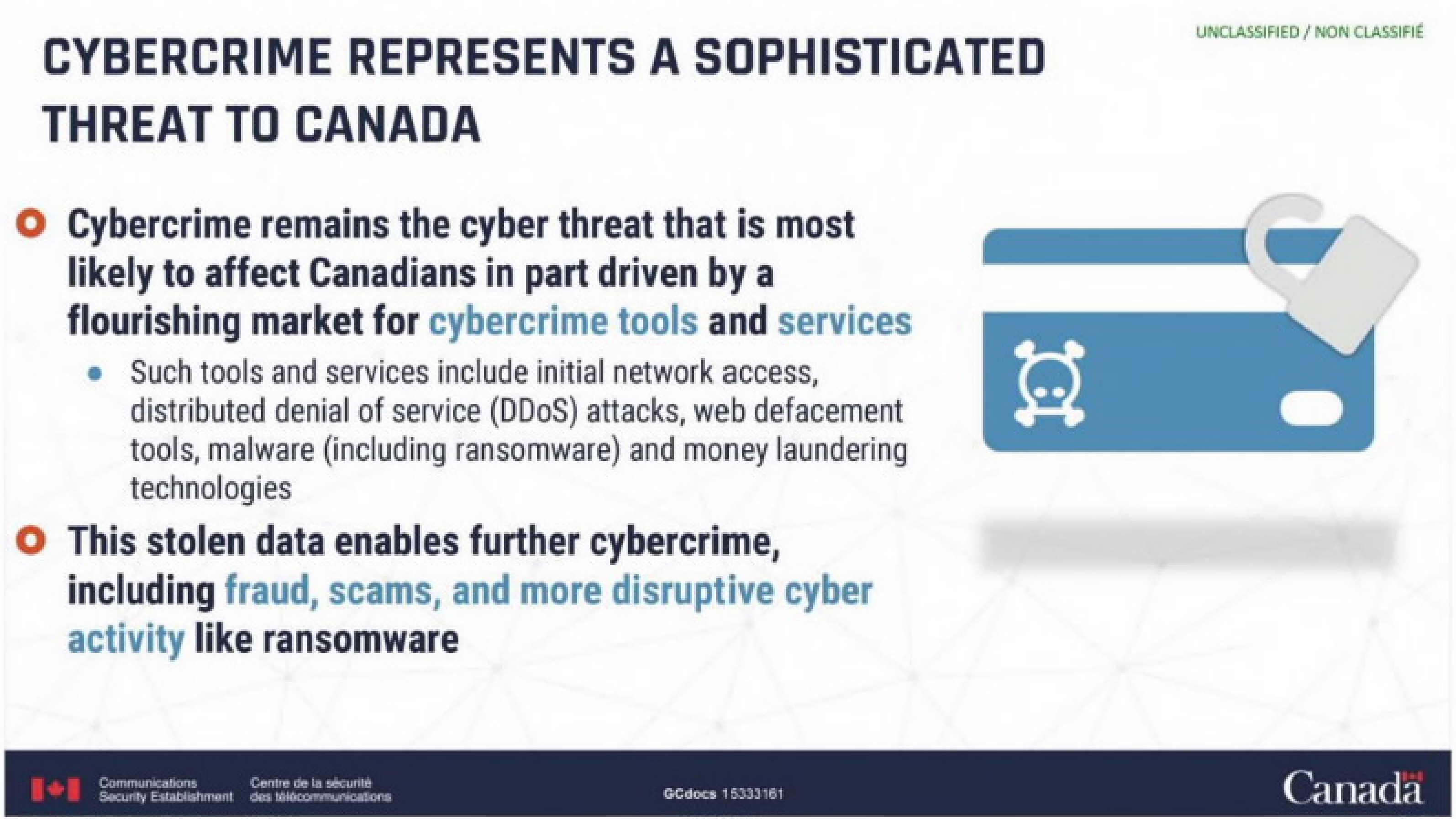
State-sponsored threat activity poses the greatest strategic threat

INFLUENCE CAMPAIGNS

Threat actors are attempting to influence Canadians and degrade trust in online spaces

DISRUPTIVE TECHNOLOGIES

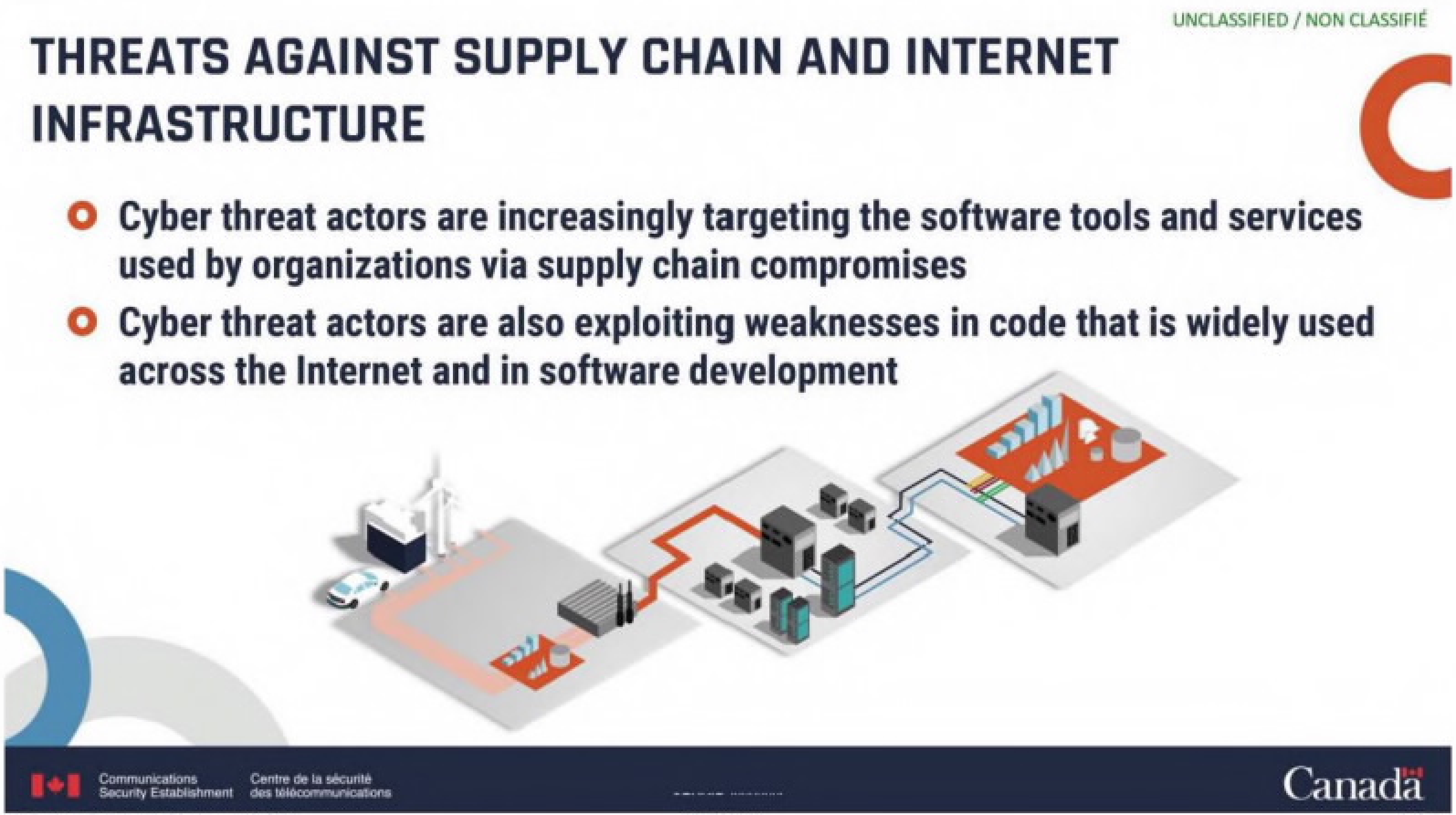
Disruptive technologies bring new opportunities and threats (cryptocurrencies, machine learning, quantum etc.)



CYBERCRIME REPRESENTS A SOPHISTICATED THREAT TO CANADA

- **Cybercrime remains the cyber threat that is most likely to affect Canadians in part driven by a flourishing market for cybercrime tools and services**
  - Such tools and services include initial network access, distributed denial of service (DDoS) attacks, web defacement tools, malware (including ransomware) and money laundering technologies
- **This stolen data enables further cybercrime, including fraud, scams, and more disruptive cyber activity like ransomware**

For Public Release



UNCLASSIFIED / NON CLASSIFIÉ

THREATS AGAINST SUPPLY CHAIN AND INTERNET INFRASTRUCTURE

- Cyber threat actors are increasingly targeting the software tools and services used by organizations via supply chain compromises
- Cyber threat actors are also exploiting weaknesses in code that is widely used across the Internet and in software development

Communications Security Establishment

Centre de la sécurité des télécommunications

Canada

For Public Release

UNCLASSIFIED / NON CLASSIFIÉ

GEOPOLITICAL COMPETITION IN CYBERSPACE

- Nation states use malicious cyber activity as a tactic for subversion and power projection to achieve their geopolitical goals
- Canadian critical infrastructure is almost certainly targeted by malicious cyber activity from nation state-backed cyber actors

Communications Security Establishment

Centre de la sécurité des télécommunications

GCdocs 15333161

Canada

UNCLASSIFIED / NON CLASSIFIÉ

GLOBAL INTERNET CONTINUES DIVERGING

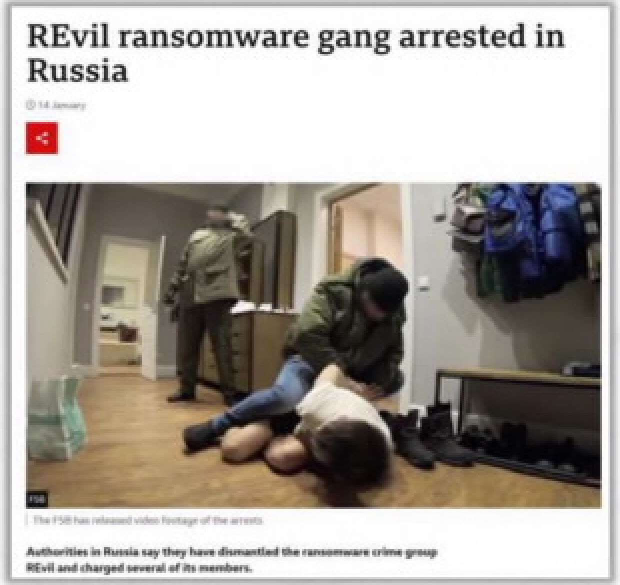
Over the next two years, it is very likely that the divergence between an open and transparent Internet and an Internet based on state sovereignty will continue to grow

Example - Russia and China have invested in their own Internet infrastructure and are advocating for information and communications technology standards - allowing more state-led control of the Internet in their respective countries.

While Internet governance may appear abstract and quite removed from daily life, we judge that competing technological ecosystems and disparate information environments inhibit the free flow of information, build distrust, and make it more difficult to combat misinformation and disinformation.

RANSOMWARE

- Cybercrime continues to be the cyber threat activity most likely to affect Canadians and Canadian organizations
- Due to its impact on an organization's ability to function, ransomware is almost certainly the most disruptive form of cybercrime facing Canadians
  - Example – after Russia's arrest of 14 members of a ransomware gang in early 2022, cyber security researchers observed the ransomware group back in operation within weeks



REvil ransomware gang arrested in Russia

14 January

FSB

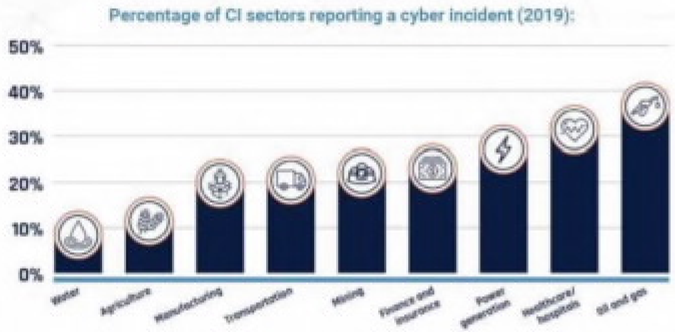
The FSB has released video footage of the arrests

Authorities in Russia say they have dismantled the ransomware crime group REvil and charged several of its members.

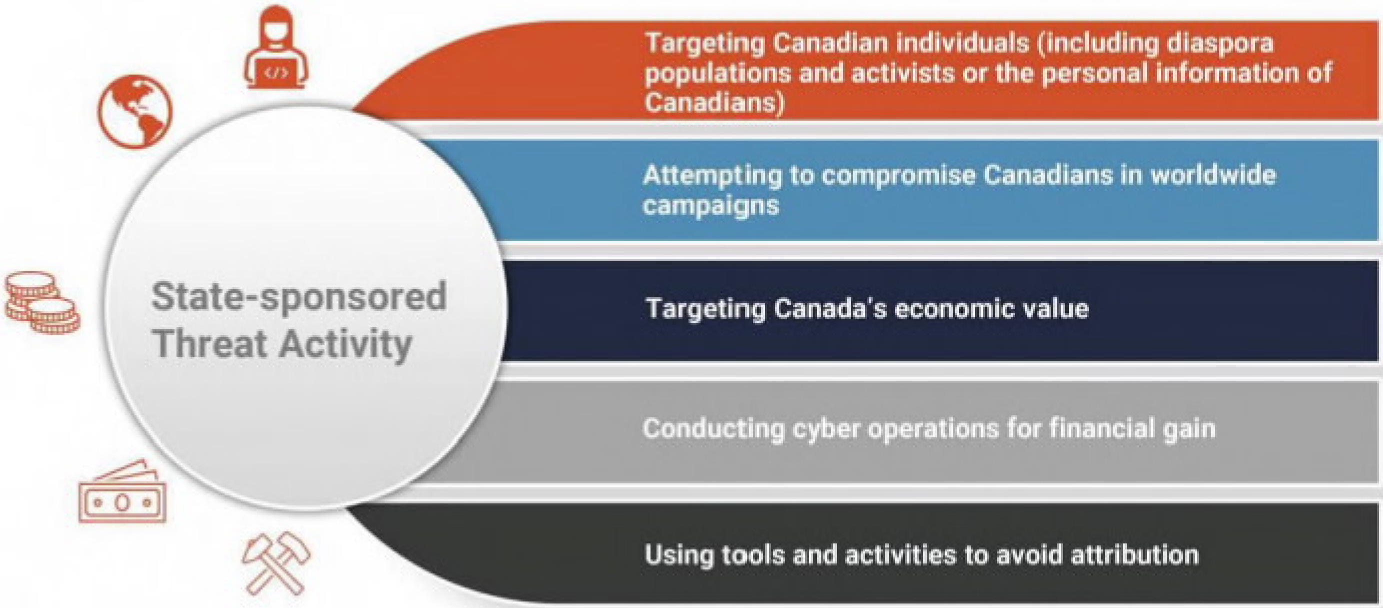
Source: BBC

THREATS TO CRITICAL INFRASTRUCTURE

- Critical infrastructure is increasingly at risk from cyber threat activity
- Opportunities for critical infrastructure disruption expand as operators increasingly expose the operational technology (OT) underpinning industrial processes to the Internet


Percentage of CI sectors reporting a cyber incident (2019):

STATE SPONSORED CYBER THREATS



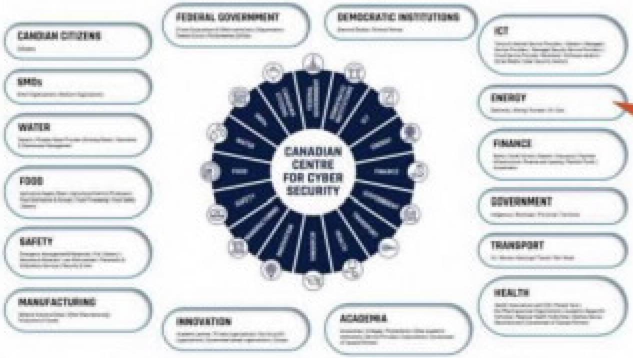
State-sponsored Threat Activity

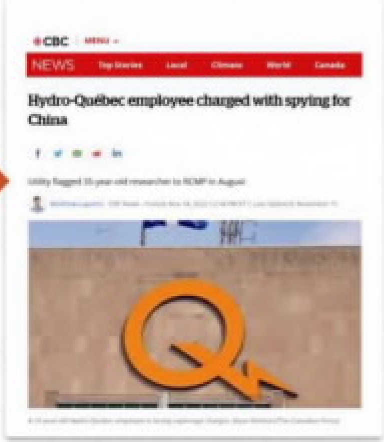
- Targeting Canadian individuals (including diaspora populations and activists or the personal information of Canadians)
- Attempting to compromise Canadians in worldwide campaigns
- Targeting Canada's economic value
- Conducting cyber operations for financial gain
- Using tools and activities to avoid attribution

UNCLASSIFIED / NON CLASSIFIÉ

STATE SPONSORED THREATS TO CI

- Critical infrastructure is increasingly at risk from cyber threat activity
- We assess that the state-sponsored cyber programs of China, Russia, Iran, and North Korea continue to pose the greatest strategic cyber threats to Canada. State-sponsored cyber threat activity against Canada is a constant, ongoing threat that is often a subset of larger, global campaigns undertaken by these specific states.





Hydro-Québec employee charged with spying for China

Utility flagged 35-year-old researcher to RCMP in August

Source: cbc.ca

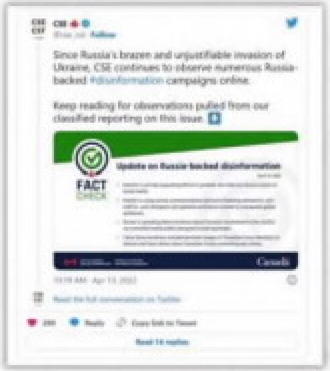
UNCLASSIFIED / NON CLASSIFIÉ

CYBER THREAT ACTOR INFLUENCE CAMPAIGNS

- Cyber threat actors exploit technology to spread MDM and deceive Canadians
- Foreign actors use MDM to influence international narratives

Photo capturing CAF members featured on forces.ca

In April 2022, CSE reported that Russia was spreading MDM about Canadian Forces members committing war crimes in Ukraine and using fake images to back up false narratives about Canada's involvement in the conflict. In one online survey of Canadian social media users, over half of the respondents reported encountering MDM relating to the Russian invasion of Ukraine on social media.

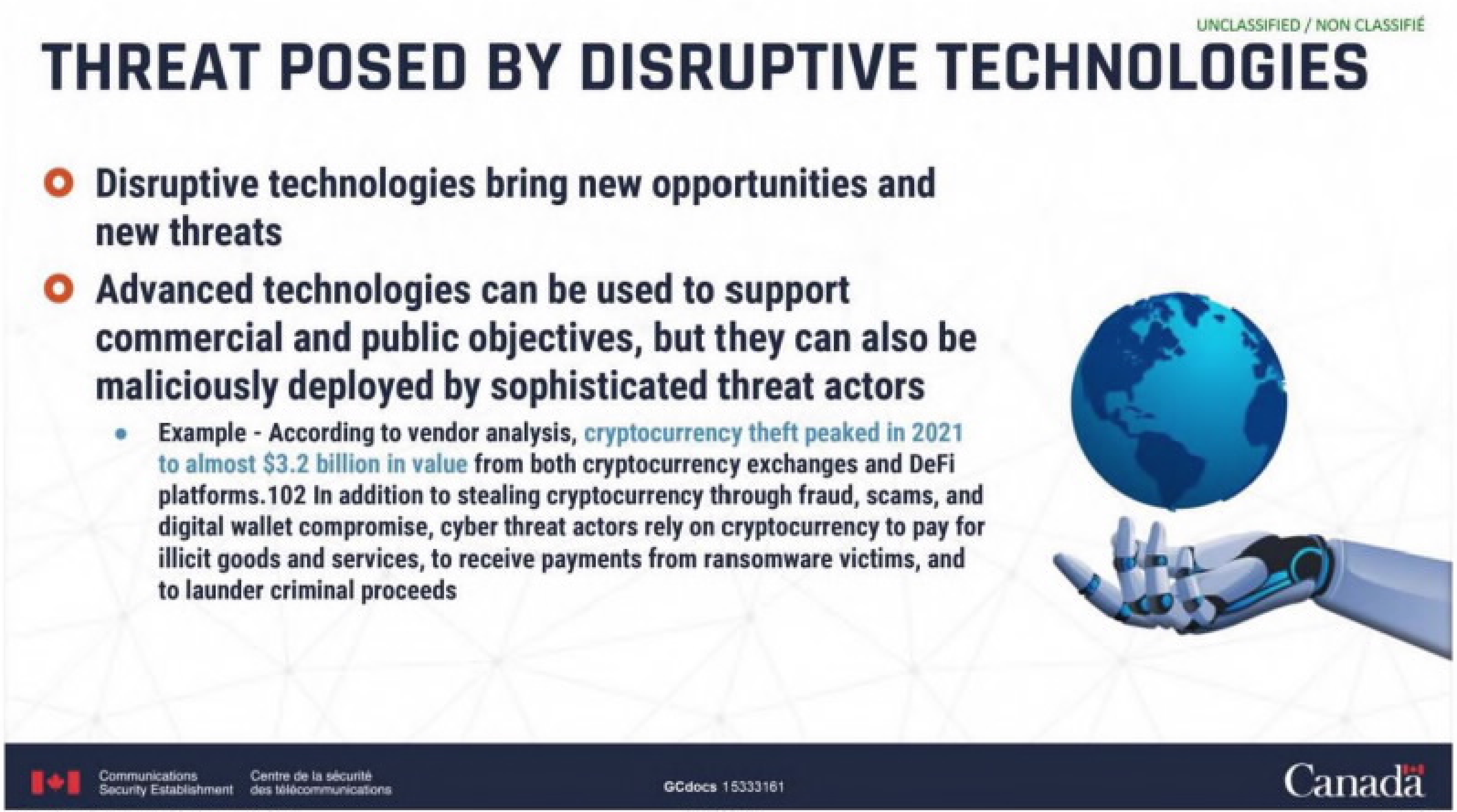


CSE

Since Russia's brazen and unjustifiable invasion of Ukraine, CSE continues to observe numerous Russia-backed #disinformation campaigns online.

Keep reading for observations pulled from our classified reporting on this issue ⬇

FACT CHECK
Update on Russia-backed disinformation
Canada
Read the full conversation on Twitter
Reply
Copy link to Tweet
Read 14 replies



UNCLASSIFIED / NON CLASSIFIÉ

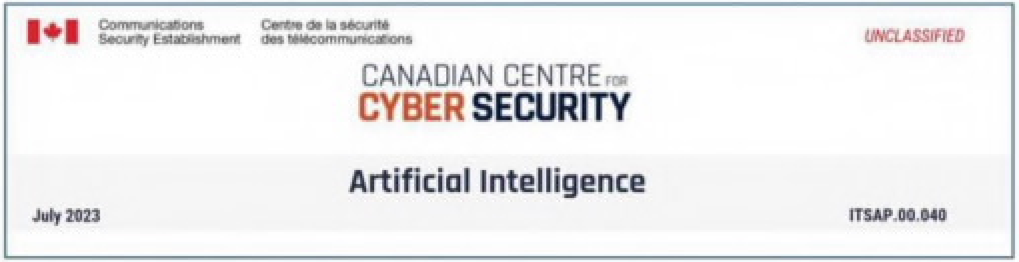
THREAT POSED BY DISRUPTIVE TECHNOLOGIES

- Disruptive technologies bring new opportunities and new threats
- Advanced technologies can be used to support commercial and public objectives, but they can also be maliciously deployed by sophisticated threat actors
  - Example - According to vendor analysis, cryptocurrency theft peaked in 2021 to almost $3.2 billion in value from both cryptocurrency exchanges and DeFi platforms.102 In addition to stealing cryptocurrency through fraud, scams, and digital wallet compromise, cyber threat actors rely on cryptocurrency to pay for illicit goods and services, to receive payments from ransomware victims, and to launder criminal proceeds

Communications Security Establishment · Centre de la sécurité des télécommunications

GCdocs 15333161

Canada



Communications Security Establishment | Centre de la sécurité des télécommunications

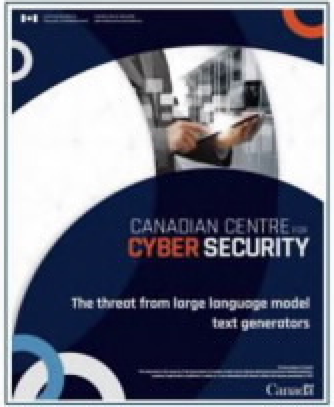
UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

Artificial Intelligence

July 2023

ITSAP.00.040

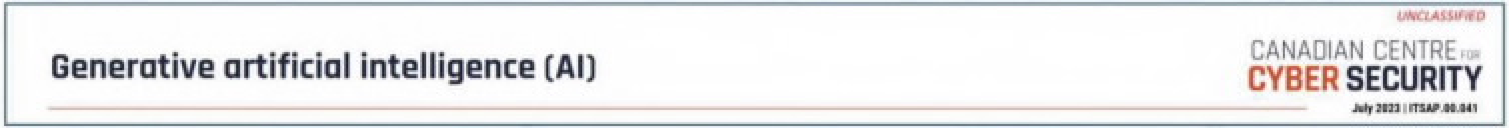


CANADIAN CENTRE FOR CYBER SECURITY

The threat from large language model text generators

Canada

Artificial Intelligence

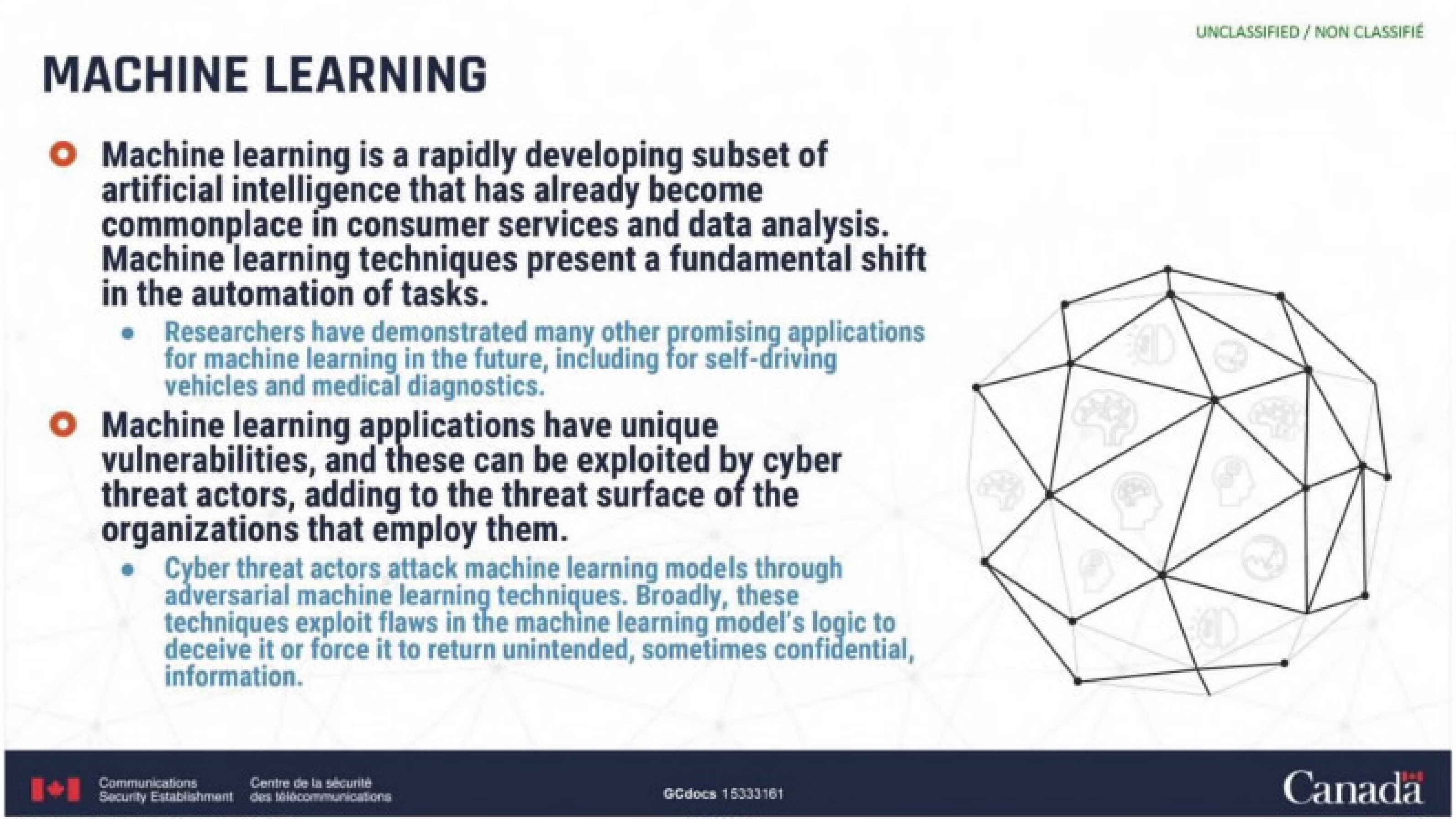


UNCLASSIFIED

Generative artificial intelligence (AI)

CANADIAN CENTRE FOR CYBER SECURITY

July 2023 | ITSAP.00.041

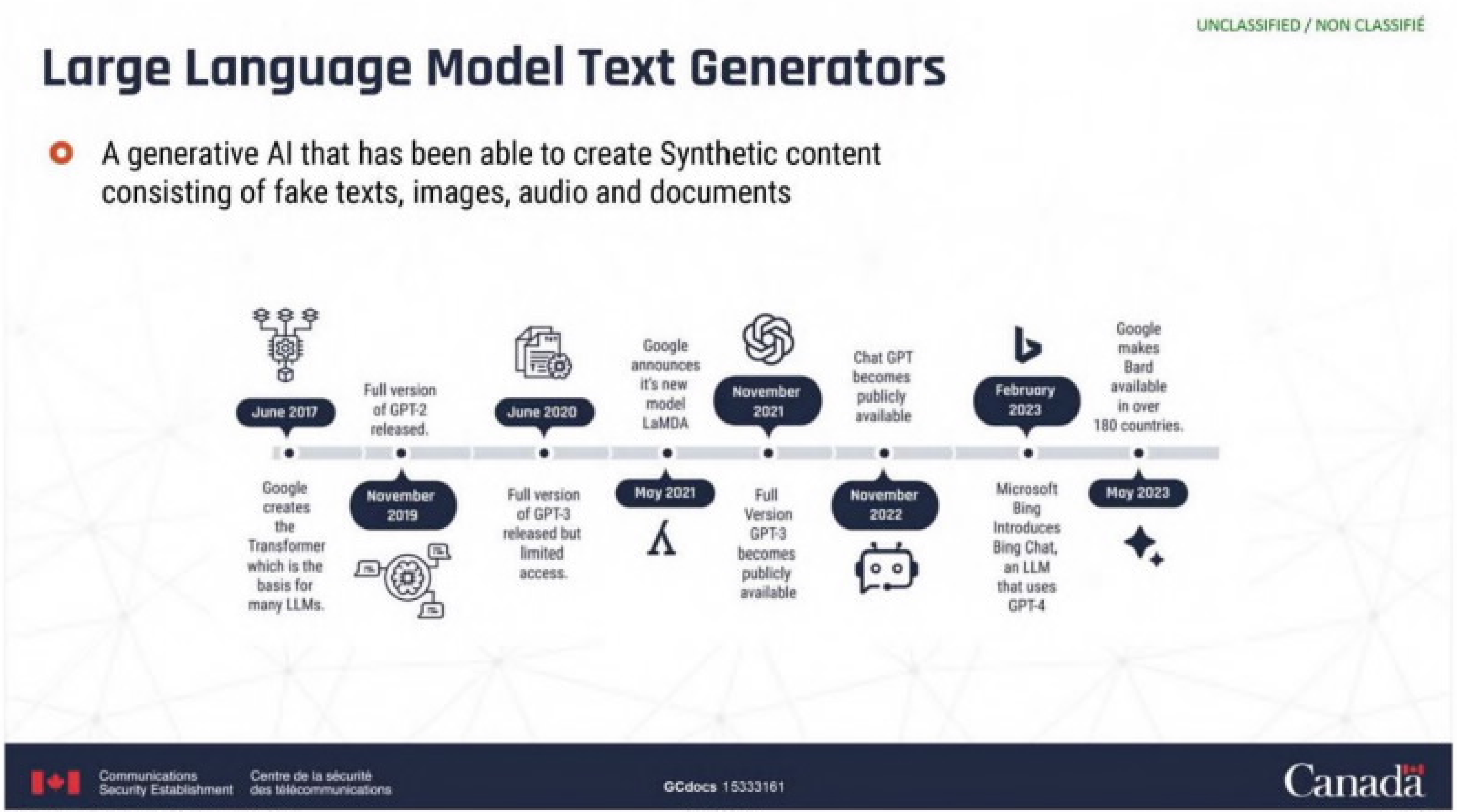


UNCLASSIFIED / NON CLASSIFIÉ

MACHINE LEARNING

- Machine learning is a rapidly developing subset of artificial intelligence that has already become commonplace in consumer services and data analysis. Machine learning techniques present a fundamental shift in the automation of tasks.
  - Researchers have demonstrated many other promising applications for machine learning in the future, including for self-driving vehicles and medical diagnostics.
- Machine learning applications have unique vulnerabilities, and these can be exploited by cyber threat actors, adding to the threat surface of the organizations that employ them.
  - Cyber threat actors attack machine learning models through adversarial machine learning techniques. Broadly, these techniques exploit flaws in the machine learning model's logic to deceive it or force it to return unintended, sometimes confidential, information.

For Public Release



UNCLASSIFIED / NON CLASSIFIÉ

Large Language Model Text Generators

- A generative AI that has been able to create Synthetic content consisting of fake texts, images, audio and documents

June 2017

Google creates the Transformer which is the basis for many LLMs.

November 2019

Full version of GPT-2 released.

June 2020

Full version of GPT-3 released but limited access.

May 2021

Google announces it's new model LaMDA

November 2021

Full Version GPT-3 becomes publicly available

November 2022

Chat GPT becomes publicly available

February 2023

Microsoft Bing Introduces Bing Chat, an LLM that uses GPT-4

May 2023

Google makes Bard available in over 180 countries.

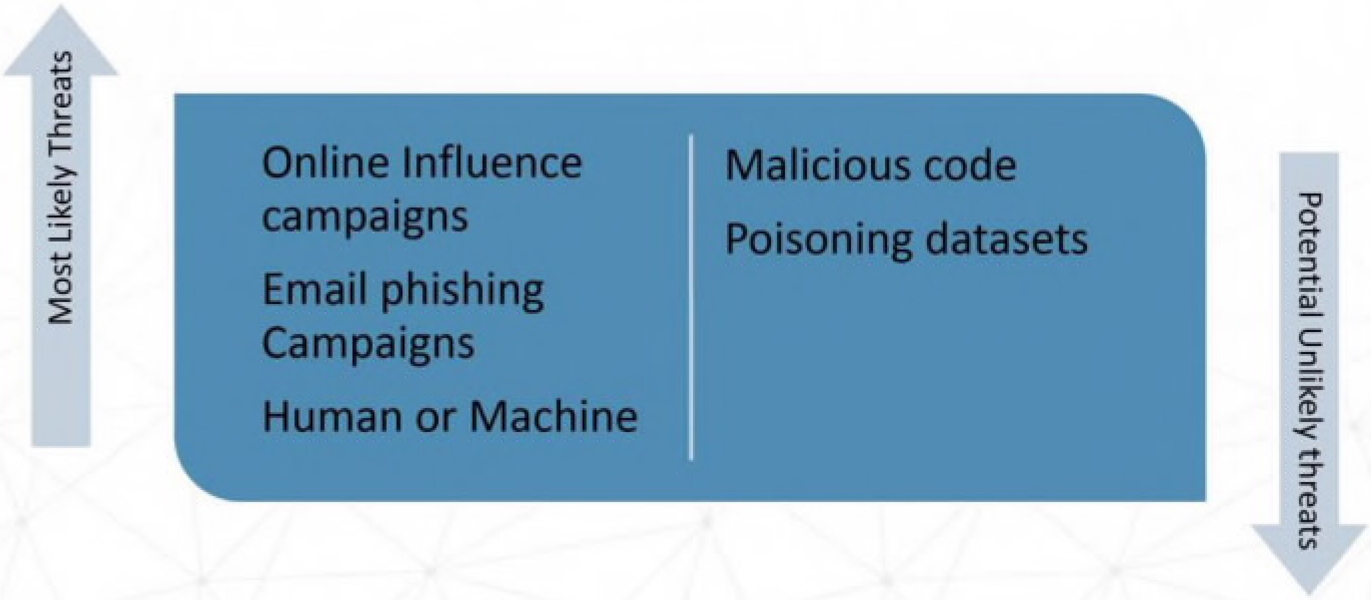
Communications Security Establishment

Centre de la sécurité des télécommunications

GCdocs 15333161

Canada

LLM Threats



Most Likely Threats

Online Influence campaigns

Email phishing Campaigns

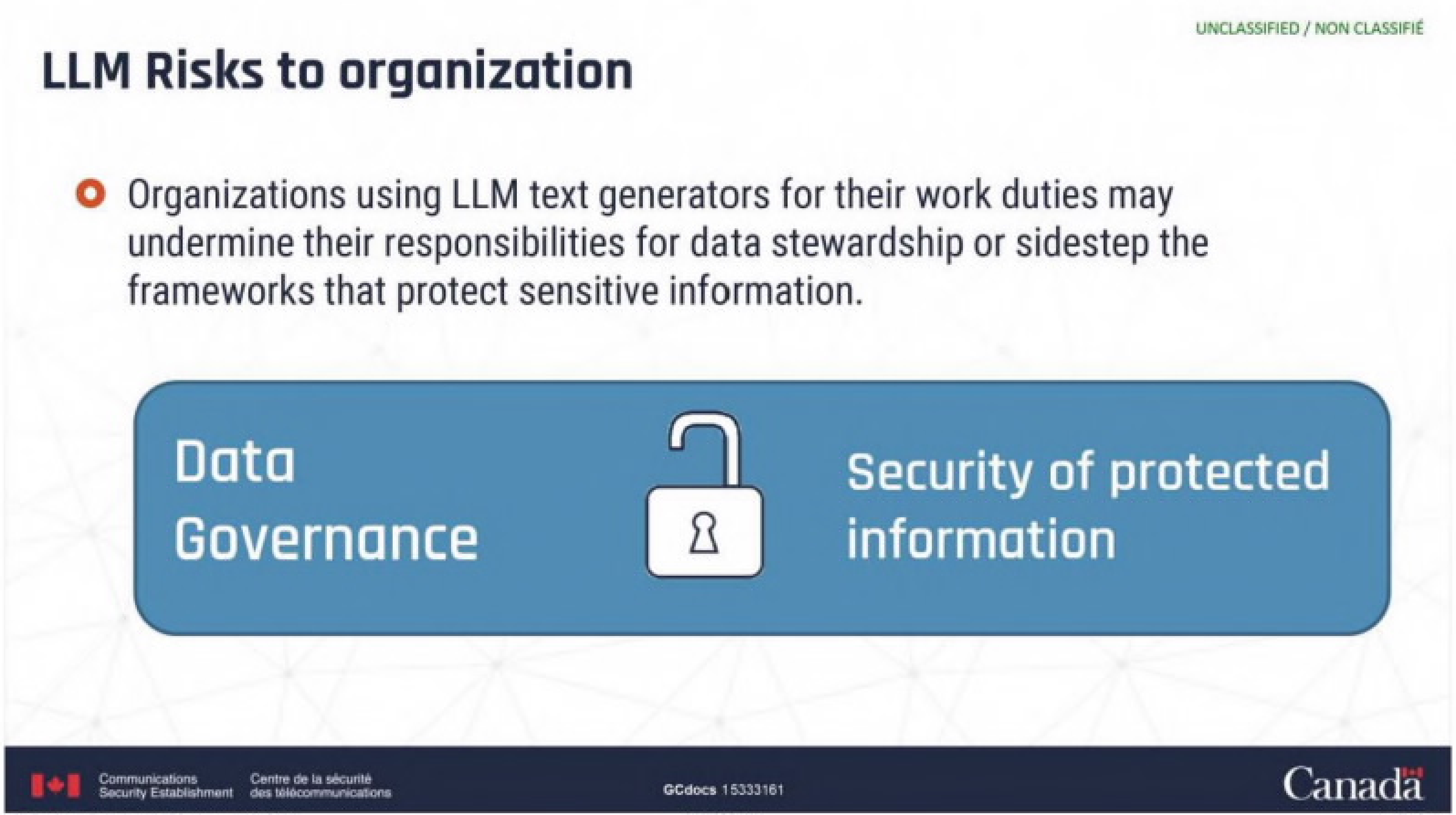
Human or Machine

Malicious code

Poisoning datasets

Potential Unlikely threats

For Public Release



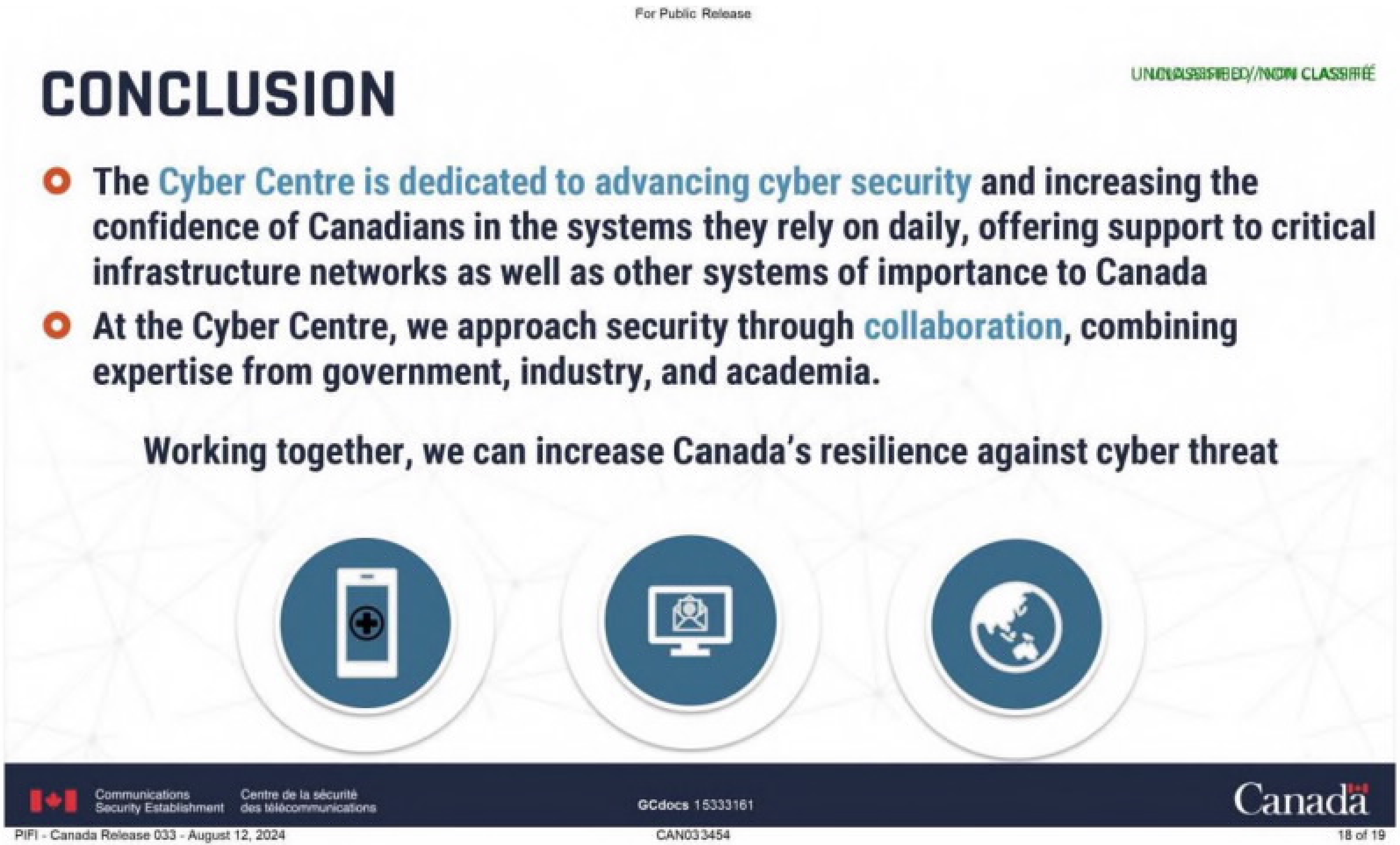
UNCLASSIFIED / NON CLASSIFIÉ

LLM Risks to organization

- Organizations using LLM text generators for their work duties may undermine their responsibilities for data stewardship or sidestep the frameworks that protect sensitive information.

Data Governance

Security of protected information



UNCLASSIFIED//NON CLASSIFIÉ

CONCLUSION

- The **Cyber Centre is dedicated to advancing cyber security** and increasing the confidence of Canadians in the systems they rely on daily, offering support to critical infrastructure networks as well as other systems of importance to Canada
- At the Cyber Centre, we approach security through **collaboration**, combining expertise from government, industry, and academia.

Working together, we can increase Canada's resilience against cyber threat

Communications Security Establishment | Centre de la sécurité des télécommunications

GCdocs 15333161

Canada

UNCLASSIFIED / NON CLASSIFIÉ

CONNECT WITH US

@cse_cst

contact@cyber.gc.ca

www.cyber.gc.ca

@cybercentre_ca

Communications Security Establishment
Centre de la sécurité des télécommunications

GCdocs 15333161

Canadä