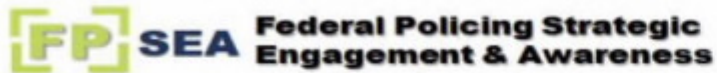


UNCLASSIFIED | NON CLASSIFIÉ



Foreign Actor Interference





CAVEAT

This document is the property of the Royal Canadian Mounted Police (RCMP), Federal Policing National Security. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the Director General, Federal Policing National Security, RCMP.

UNCLASSIFIED | NON CLASSIFIÉ

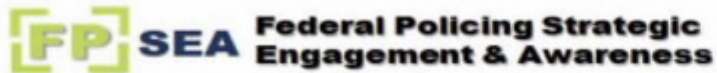


PIFI - Canada Release 034 - August 12, 2024

WHAT IS FOREIGN ACTOR INTERFERENCE (FAI)?

For Public Release

CAN024152






WHAT IS FAI?

Foreign Actor Interference **is defined as an illegal activity** conducted or supported by a foreign state / actor that is detrimental to Canadian national interests and is clandestine or deceptive or involves a threat to any person.

- FAI may be conducted by state representatives or their proxies.
- FAI does not include legitimate foreign state activities, such as policing, diplomatic or cultural engagements.



States engage in FAI activities to **further their national interests**, including:

-  Regime protection
-  Projection of power
-  To gain economic, geopolitical, military and strategic influence and advantage

WHO ENGAGES IN FAI?

CSIS Annual Report 2022 – States of concern:

- People's Republic of China (PRC)
- Islamic Republic of Iran
- Russian Federation
- Any other country projecting power





WHO ENGAGES IN FAI?

Community Groups	Students	Research Scientists	Journalists and Media	Co-optees	Employees
<ul style="list-style-type: none"> Infiltrate culturally / linguistically diverse communities 	<ul style="list-style-type: none"> Gain access to academia Recruit students working in targeted fields Silence opposition 	<ul style="list-style-type: none"> Influence research agendas Influence peer review process Illegal acquirement of technology, private and public 	<ul style="list-style-type: none"> Influence public opinion State sponsored disinformation /misinformation campaigns Stifle freedom of speech 	<ul style="list-style-type: none"> An individual such as an Embassy employee who collaborates with their country's intelligence agency to undertake minor assignments 	<ul style="list-style-type: none"> Insider threat Illegal acquirement of technology

CAN024152

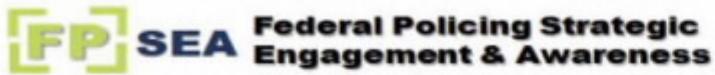
For Public Release



FAI - INDICATORS

- **Elicitation:** Actors attempt to manipulate a person into sharing valuable information
- **Cultivation:** Exploitation of long-standing relationships in order to manipulate a person with access to valuable information
- **Blackmail** and threats: Can be used to gain cooperation from a targeted person, or to silence dissent
- **Debt traps:** When a targeted person's financial situation is used as leverage to manipulate them
- **Cyber attacks:** Phishing, spear-phishing, malware
- **Acquirement:** acquirement of information or technology to the detriment of Canada or Canadians

Who benefits from these actions? Is it a foreign state? This could be foreign actor interference!



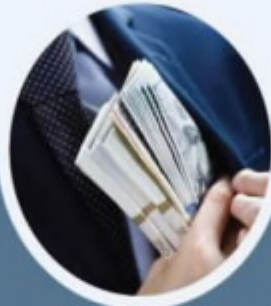
WHAT DOES FAI LOOK LIKE?



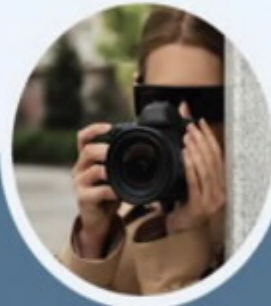
- Community harassment
- Physical/online harassment
- Intimidation
- Surveillance/following



- Threats to critical infrastructure
- State-backed cyber attacks
- Insider threats
- Compromised facilities



- Threats to democracy
- Electoral interference
- Bribery/corruption
- Voter intimidation



- Foreign intelligence
- Theft of secret information
- Blackmail/compromise
- Cultivating sources



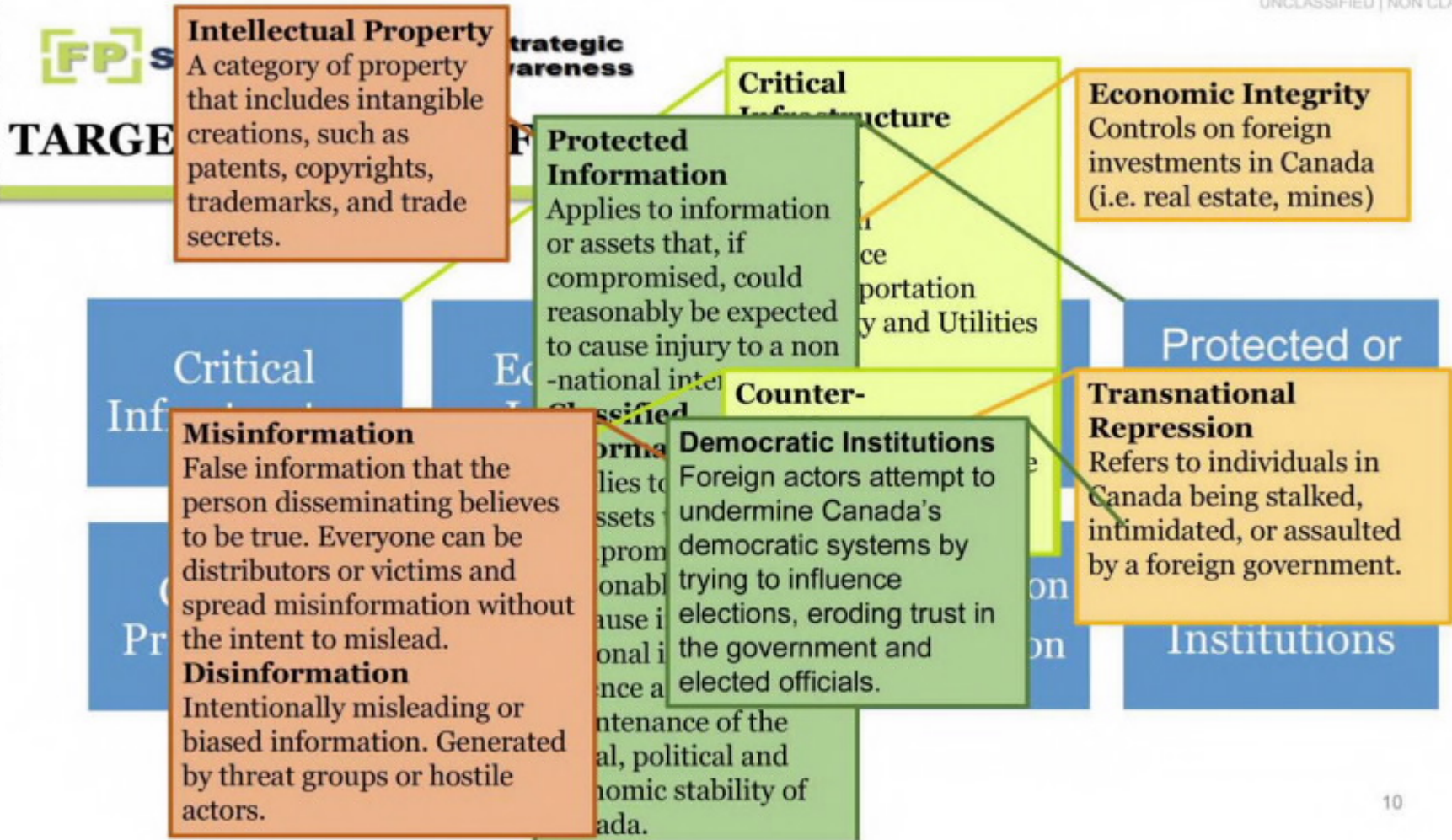
- Economic threat
- Theft of sensitive technology
- Theft of research data
- Attempts to gain control of sensitive resources

UNCLASSIFIED | NON CLASSIFIÉ

PIFI - Canada Release 034 - August 12, 2024

CAN024152

For Public Release





FAI IMPACTS

Benefits the foreign actor:

- Theft of trade secrets to undercut competition, to the detriment of the Canadian economy
- Manipulate public perception in favour of the actor and / or against the target
- Project power
- Gain economic, political and military strategic influence and advantage

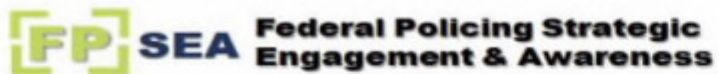
Undermines Canadian interests:

- Damage trust in Canadian democratic systems
- Erode trust in credible journalism
- Amplify societal differences to create / increase social unrest

Intimidates/harms/coerces culturally and linguistically diverse communities

- Silence criticism of the hostile state's regime
- Force cooperation with hostile states to advance their interests

UNCLASSIFIED | NON CLASSIFIÉ



PIFI - Canada Release 034 - August 12, 2024

IS THE RCMP MANDATED TO ENFORCE FAI?

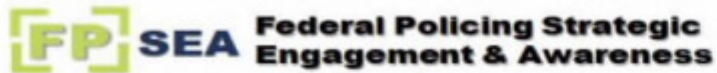
For Public Release

CAN024152



RCMP MANDATE

- By legislation the RCMP is Canada’s primary law enforcement body to investigate threats to the security of Canada
- The RCMP’s National Security Program investigates threats to the security of Canada by upholding various laws for the purpose of preventing offences and bringing to justice those who contravene Canadian legislation.
- The RCMP, and the broader Canadian law enforcement community, have a clear role to play in protecting Canada and Canadians from foreign actor interference.



RCMP ENFORCEMENT OF MANDATE

- **Criminal Code of Canada**- broad range of offences can be brought to bear against foreign interference.
- ***Security of Information Act (SOIA)*** - unlawful release of sensitive or classified information
 - ***Includes threats to persons***
- ***Other examples: Export Act, Pathogens Act, Public Servants Inventions Act....***

UNCLASSIFIED | NON CLASSIFIÉ

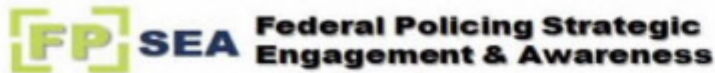


PIFI - Canada Release 034 - August 12, 2024

ROLE OF LAW ENFORCEMENT IN ADDRESSING FAI

For Public Release

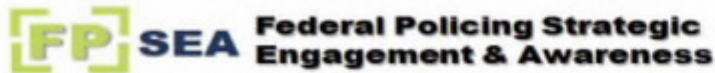
CAN024152



RCMP RESPONSE

- Investigate FAI as a threat to the security of Canada
- Collaborate with domestic and international partners
- Identify and engage in critical infrastructure and cyber initiatives
- Review legislative and regulatory regime, existing operational capability and capacity, and the role of law enforcement in addressing the threat





POLICE OF JURISDICTION

➤ **Eyes and ears on the ground**

- First to hear about harassment or receive complaints related to foreign intimidation tactics

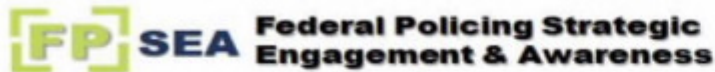
➤ **Robust community network**

- Public engagement and outreach initiatives
- Maintain strong relationships that enable community members to report intimidation tactics

➤ **Identify, disrupt and report cases**

- Report possible incidents of espionage, sabotage, and other activities detrimental to Canadian interests and national security

We cannot address this threat alone. We need to work together with our partners.



RCMP ENGAGEMENT WITH NON-TRADITIONAL PARTNERS

Non-Traditional Partners

- Critical infrastructure owners and operators
- Canadian private industry
- Academia

Challenges

- Securing a formal complaint - reticence to report possible security breaches due to reputational risk
- Difficult to assess loss or injury - may take time and assessment may change from initial reporting
- Alignment with corporate security processes (internal investigations, administrative procedures) and criminal investigation



INSIDER THREATS

Any person or group who has or had authorized access to assets and uses their access either knowingly or inadvertently in a way that could negatively affect their organization.

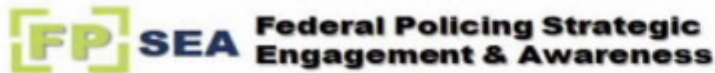
Includes employees, contractors, volunteers, or employees from another agency on assignment.

Types of Insider Threats

- Intentional
- Unintentional
 - negligent or accidental

Indicators

- Disgruntlement
- Difficulty accepting Feedback
- Anger Management
- Disengagement
- Disregard for authority
- Poor performance
- Confrontational Behaviour
- Personal Issues
- Self-Centeredness
- Lack of Dependability
- Absenteeism/Unusual Hours



FAI AND CYBERCRIME

Think before you click

- Emails, links, attachments

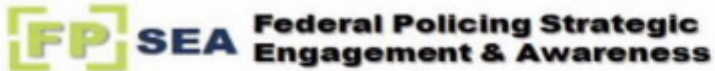
USBs, media and mobile devices

- Don't use gifted USBs or other electronic devices
- Don't connect any device to work computers or systems unless authorized

Follow good cyber practices

- Use strong passwords – 12+ characters with numbers, symbols, upper and lower case letters
- Install reputable antivirus and malware software; use network firewalls; secure your router
- Use multi-factor authentication
- Avoid opening emails from unknown addresses or clicking links embedded in them
- Regularly update software to protect against the latest vulnerabilities. Follow instructions from software provider
- Create backup copies on at least 2 different devices with 1 backup stored in a separate location





UNCLASSIFIED | NON CLASSIFIÉ

FAI – HOW TO HARDEN INFRASTRUCTURE

Prevent ransomware

- Email and web – block spam and access to malicious links
- Server – protect servers from exploitable vulnerabilities
- Network and endpoint – prevent ransomware from spreading and running on endpoint

Physical Security

- Cameras
- Passcodes
- Locking screens and doors



21



UNCLASSIFIED | NON CLASSIFIÉ

REAL LIFE EXAMPLES

Iranian dissidents in Canada say they're being watched and under threat from the regime in Iran

Dissidents of the Turkish government are living in fear in Canada

India among top actors for foreign interference in Canada: national security adviser

Russian cyber threat to Canada worse than previously reported: CSE



USEFUL RESOURCES

UNCLASSIFIED | NON CLASSIFIÉ



Canada



Canada



Canada



Canada



Canada



Canada

CAN024152

For Public Release

Slide Notes

Slide 4:

Foreign interference is distinct from normal diplomatic conduct or acceptable foreign state lobbying.

It is purposely covert, malign, and deceptive.

States cross a line anytime they go beyond diplomacy to conduct activities that attempt to threaten our citizens, residents and institutions, or to compromise our way of life, undermine our democratic processes, or damage our economic prosperity.

**Can ask the audience "Do you know what a proxy is?" - a person authorized to act on behalf of someone else to conduct illegal activity.

FAI can be conducted by representatives of the state (e.g. intelligence or police agents) or by proxies (e.g. individuals or groups of people) who are directed to conduct illegal activity.

Source: Foreign Interference and You – Canadian Security Intelligence Service.

Slide 5:

Foreign governments engage in foreign interference activities in Canada and target Canadians to advance their interests, sometimes at our expense, in an effort to achieve geopolitical, economic, military and strategic advantage.

They seek to sow discord, disrupt our economy, bias policy development and decision-making, and to influence public opinion. In many cases, clandestine influence operations are meant to support foreign political agendas or to deceptively influence the targeted country's policies, officials, research institutions or democratic processes

Slide 6:

As highlighted by CSIS annual report, states of concern regarding FAI activities in Canada include: People's Republic of China (PRC), Iran and Russia. Any other country that project's power can also be of concern.

As an advanced economy and an open and free democracy, Canada has long been targeted by hostile states seeking to acquire information, intelligence and influence to advance their own interests.

Slide 7:

FAI can also involve non-state entities attempting to infiltrate targeted groups in order to influence Canadians.

Infiltrated groups can be directed, inspired, or unwitting participants in FAI.

* Community Groups: In 2017, the PRC passed a National Security Law that requires Chinese organizations to assist with state intelligence work

Slide 8:

Foreign Interference and You - Canada.ca

Slide 9:

Suggest having charges that police would look at for each example.

1) 264CC Harassment

423 CC Intimidation

Section 20 and 21 SOIA

S 322 (1) CC Theft, s. 342.1 CC [unauthorized use of computer]

Elections act violation fed or prov.

Intimidation

Theft intimidation

Theft, unauthorized use of a computer, S122 CC Breach of Trust of a Public Officer

Misinformation: 5G conspiracies circulating online that 5G frequencies in new cell towers are the cause of COVID-19. The belief in these conspiracies led to acts of vandalism against cell towers in Canada.

Slide 10:

Critical infrastructure: Exploiting vulnerabilities across all sectors of Canada's critical infrastructure, including Canada's energy sector and information and communication technologies.

Vulnerability: cyber attacks, supply chains

Economic integrity: Leveraging Canada's open economy to gain influence or advantage over strategic resources, research, technologies and industries leads to economic erosion, loss of competitive advantage.

Vulnerability: export investments, knowledge, and licenses

Intellectual property: Efforts to gain commercial, academic, scientific and military information, goods and technologies from GoC or private companies, research and academic institutions, undermines Canada's global competitive edge and prosperity.

Vulnerability: academic espionage, innovative technologies

Protected information: Targeted acquisition of information secured from the public, or bound by confidentiality agreements, threatens Canada's national security & economic integrity.

Vulnerability: Security of Information Act (SOIA) and insider threats, trade secrets, classified information

Counter-proliferation: Efforts to procure sensitive, restricted and dual-use technologies and goods, bolster the State actor's military capabilities and strategic advantage impact global peace and security.

Vulnerability: weapons of mass destruction, violations of sanctions

Transnational repression: Monitoring, and intimidating Canadian diaspora communities to force cooperation or mute criticisms of regime policies, threatens Canada's sovereignty and the safety of Canadians.

Vulnerability: assassination, coercion, threats, intimidation, harassment, misuse of Interpol, renditions and forced repatriations

Misinformation/disinformation: State-sponsored manipulation of information and use of misinformation seeking to influence or to discredit and erode confidence in Canada's democratic institutions, policies and values.

Vulnerability: use of online platforms and community spaces, influence narratives, targeting of elected officials

Democratic institutions: Interfering in and influencing Canada's democratic processes erodes public confidence in Canada's democracy and impacts social cohesion.

Vulnerability: corruption of elected officials, cultivation of relationships with key demographics, election interference, placement of individuals in positions of influence

Slide 13:

The nexus of an FAI offence falling within the National Security mandate is not obvious.

*****Section 6(1) Security Offences Act

RCMP Operational Manual National Security: 12 2. 2. Mandate

2. 2. 1. The National Security Program retains primary responsibility in the investigation of the following national security offences:

2. 2. 1. 2. duties assigned to police officers under sec. 6(1), Security Offences Act;

Section 6 (1) explains that Members of the RCMP who are peace officers have the primary responsibility to perform the duties that are assigned to peace officers in relation to any offence referred to in section 2 or the apprehension of the commission of such an offence. Section 2 of the SOA explains that notwithstanding any other Act of Parliament, the Attorney General of Canada may conduct proceedings in respect of an offence under any law of Canada where (a) the alleged offence arises out of conduct constituting a threat to the security of Canada within the meaning of the Canadian Security Intelligence Service (CSIS) Act.

2. 2. 1. 3. threats to the security of Canada as defined in

sec. 2, CSIS Act to mean:

(a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,

(b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,

(c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and

d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,

2. 2. 1. 5. unlawful, unauthorized or intentional communication to a foreign entity of any national security criminal information that is safeguarded by the Canadian government, or by a province, that could constitute a breach of the Security of Information Act or other similar provisions in other federal laws and the CC;

2. 2. 1. 6. any other federal statute or Criminal Code offence that may have a national security dimension

Slide 14:

RCMP must accept that public safety, rather than charges/prosecution, is the gold standard.

Legislation:

Security Offences Act: Section 6(1) designates the RCMP as the primary enforcement body in relation to national security, as defined by the Canadian Security Intelligence Service Act, including acts of foreign interference (FI);

Criminal Code: There are a broad range of offences that can be brought to bear against foreign interference. For instance, offences such as Breach of Trust Sec. 122 Criminal Harassment Sec 264.01, unauthorized use of a computer Sec. 342.1 or Intimidation Sec. 423 or Mischief Sec. 430. Other provisions, such as bribery, or harassment, could also be used to disrupt FI.

Security of Information Act (SOIA): Includes numerous offences and sections in relation to FAI, including economic espionage, the release of classified information, and foreign influenced threats or violence. SOIA offences have severe penalties, many involving life in prison sentences. Includes threats to persons.

Enforcement to response to threats to persons yet the title does not indicate such inclusion.

Foreign-influenced or Terrorist influenced Threats or Violence

Threats or violence

20 (1) Every person commits an offence who, at the direction of, for the benefit of or in association with a foreign entity or a terrorist group, induces or attempts to induce, by threat, accusation, menace or violence, any person to do anything or to cause anything to be done

- (a) that is for the purpose of increasing the capacity of a foreign entity or a terrorist group to harm Canadian interests; or
- (b) that is reasonably likely to harm Canadian interests.

Export Act, Pathogens Act,
Public Servants Inventions Act....

4 (1) Every public servant who makes an invention
(a) shall inform the appropriate minister of the invention and shall provide the minister with such information and documents with respect thereto as the minister requires;
(b) shall not file outside Canada an application for a patent in respect of the invention without the written consent of the appropriate minister; and
(c) shall, in any application in Canada for a patent in respect of the invention, disclose in his application that he is a public servant.

Slide 16:

Foreign actor interference is considered a threat to the security of Canada and is investigated by RCMP Integrated National Security Enforcement Teams (INSET). The RCMP INSET will prevent, detect, disrupt and respond to national security related criminal threats in Canada in partnership with intelligence and other law enforcement agencies. FPNS provides oversight to these investigations.

The RCMP will collaborate with domestic and international law enforcement and intelligence partners, as well as private companies, to investigate suspected foreign actor interference.

FPIIP oversees the RCMP's intelligence analysts and various international programs, such as the analysts deployed abroad, the international liaison and coordination centre, and Interpol Ottawa. These programs are essential in working with international partners on all types of investigations.

FPCO provides oversight and governance on serious and organized crime, financial crime, Sanction Violations and cybercrime investigations. This include the Canadian Anti-Fraud Centre (CAFC) which receives all kinds of fraud reports. Cybercrime and fraud go hand in hand, and these are areas that foreign actors could exploit to gain access to Canadians.

FP-SEA provides support to RCMP Federal Policing through strategic engagement with key national and international stakeholders, and raise awareness of federal priority enforcement areas through crime prevention and reporting initiatives. The overall goal is to reduce federal crime victimization, and to increase reporting to police and partners on possible illicit activity that might otherwise go uninvestigated.

Slide 17:

Similar to any other type of investigation – need to work jointly and have a united front

Slide 18:

For Example, the Federal Policing Strategic Engagement and Awareness (FP-SEA) unit supports RCMP Federal Policing through strategic engagement with key national an international stakeholders, and raises awareness of federal priority enforcement areas through crime prevention and reporting initiatives.

Initiatives:

FP-SEA holds information sessions where law enforcement and other partner agencies present on their mandates and operations in order to share information on best practices, current challenges and a variety of other topics. The information sessions promote information sharing and bring awareness to law enforcement agencies and the organizations we work with on potential threats.

FP-SEA also has a large network of law enforcement and other strategically selected partners that it disseminates bulletins and information to. The distribution lists are tailored to each product and helps to raise awareness of current and emerging threats and issues.

Slide 19:

Unintentional insider threats are when an individual accidentally puts information or assets at risk. This would be losing a USB key with sensitive information, losing a laptop or work phone can pose risks as well.

An intentional insider threat is when an individual chooses to engage in activities that cause harm, or expose sensitive material for personal gain or on behalf of a malicious third party.

The insider threat could be motivated by selfish reasons or could be in a situation where they are being coerced. Certain risk factors put an individual at risk of being exploited for their privileged position.

The Critical Pathway to Insider Risk (in most cases follows this order but all don't need to be present):

Personal Predisposition (e.g. medical, psychiatric, personality issues, previous rule violations)

Stressors precede insider acts: stressors become triggers (e.g. unmet expectations, marriage/divorce, relocation, loss, leadership failures, restructuring, public health crisis, etc.)

Concerning Behaviours (e.g. declining performance, usual working hours, personal/workplace conflict, mishandling sensitive information, unexplained travel)

Maladaptive Organization Response (management keeps problem going by not addressing issue, ignoring/promoting/moving the employee rather than dealing with the issue)

Plans, Recruitment, Insider Attack, Op Sec Action

Insider Threat - Infoweb (rcmp-grc.gc.ca)

Insider Threat Mitigation Guide (cisa.gov)

Slide 20:

Think before you click: How to spot phishing and malware attacks - Infoweb (rcmp-grc.gc.ca)

Fact sheet: Phishing - Get Cyber Safe

USB storage devices – What you need to know - Infoweb (rcmp-grc.gc.ca)

Prevent ransomware | Royal Canadian Mounted Police (rcmp-grc.gc.ca)

Slide 21:

Prevent ransomware | Royal Canadian Mounted Police (rcmp-grc.gc.ca)

Slide 22:

Iranian dissidents in Canada say they're being watched and under threat from the regime in Iran | CBC News

In November 2022, CBC reported on Iranian dissidents that were being watched and threatened in Canada. Iranian activists in Canada reported having to cut ties with their friends and family in Iran in order to keep them safe as the Islamic Revolutionary Guard, a branch of the Iranian forces designated as a terrorist organization in the US, were using their connections in Iran to intimidate them.

Dissidents of the Turkish government are living in fear in Canada (theconversation.com)

An October 2020 article discussing Turkey's espionage activities against dissidents living in Canada. According to this article, Turkey is engaging in propaganda activities in order to discredit opposition groups, is involved in intelligence gathering and espionage activities and is intimidating, threatening and abducting individuals that disagree with their regime.

India among top actors for foreign interference in Canada: national security adviser | CTV News

A June 6, 2023 article confirms that Canada's national security advisor says that India is among the top sources of foreign interference in Canada

Russian cyber threat to Canada worse than previously reported: CSE | National Post

An article from July 2022 indicates that CSE issued a threat bulleting saying "the scope and severity of cyber operations related to the Russian invasion of Ukraine has almost certainly been more sophisticated and widespread than has been reported in open sources." Just prior to Russia's invasion of Ukraine, the CSE warned Russia could target Canadian critical infrastructure. It said since then, its cybersecurity centre has reached out to critical infrastructure sectors in Canada to "reinforce the need to enhance vigilance and follow Cyber Centre advice."

Slide 23:

Resources:

Foreign Interference and You, 2022: CSIS Publication: <https://www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-and-you/foreign-interference-and-you-list.html>

Foreign Interference Threats to Canada's Democratic Process, 2021: CSIS Publication: <https://www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-threat-to-canadas-democratic-process.html>

Foreign Actor Interference – Recognise it, reject and report it!: RCMP Bulletin: <http://infoweb.rcmp-grc.gc.ca/fp-pf/fpsea-esspf/index-eng.htm> (external partners can request by contacting the Federal Policing Strategic Engagement and Awareness (FP-SEA) team at: FP-SEA_ESS-PF@rcmp-grc.gc.ca)

Insider Risk: RCMP Publication: <http://infoweb.rcmp-grc.gc.ca/fp-pf/fpsea-esspf/index-eng.htm> (external partners can request by contacting the Federal Policing Strategic Engagement and Awareness (FP-SEA) team at: FP-SEA_ESS-PF@rcmp-grc.gc.ca)

National Cyber Threat Assessment 2023-2024 - Canadian Centre for Cyber Security