National Security Threat Environment
Foreign Actor Interference

Federal Policing National Security

September 28, 2020

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

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.

Overview

Topics to be covered:

- What is Foreign Actor Interference?
- The Importance of Foreign Actor Interference
- Role of Law Enforcement
- Overview of RCMP Investigations
- Challenges associated with FAI Investigations
- Importance of Operational Security
- Considerations
- Way Forward

Objectives

At the end of this session, you will be able to:

- Define Foreign Actor Interference (FAI)
- Understand the RCMP's mandate to investigate FAI
- Understand the importance of maintaining operational security when involved in these types of investigations

UNCLASSIFIED

FAI as a National Concern

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

5

WU5
WU11

Is the RCMP Mandated to Investigate Foreign Interference Crimes?

Slide 6

WU5	New Slide - As per L&D's feedback, included a slide with a question to increase learner participation Windows User; 2/3/2020 11:06:55 AM
WU11	Meets the need Windows User; 2/6/2020 11:12:43 AM

UNCLASSIFIED

RCMP Mandate

WU6

- The RCMP's National Security Program investigates threats to the security of Canada by upholding various laws for the purpose of preventing offences from happening 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.

Slide 7

WU6 New Slide created with information from the FAI Handout to elaborate on the RCMP's mandate to investigate FAI.
Windows User; 2/3/2020 11:08:23 AM

WU7
WU12

UNCLASSIFIED

RCMP Mandate

- Section 2, ***Canadian Security Intelligence Service (CSIS) Act***: threats to the security of Canada means:

  (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

- Unlawful release of sensitive or classified information contrary to section 6 of the ***Security of Information Act (SOIA)***

- An unlawful act affecting critical infrastructure

RCMP Sensitive and International Investigations (SII) and RCMP CyberCrime units also conduct FAI investigations

Slide 8

WU7	Enhanced the speaking notes by adding the various legislation options identified in the FAI Handout. Windows User; 2/3/2020 11:12:36 AM
WU12	helps with presention. Windows User; 2/6/2020 11:14:45 AM

What is Foreign Actor Interference?

Foreign Actor Interference

- Illegal activity conducted, or directed, by a foreign actor that constitutes a threat to Canada's national security.
- Advance a foreign entity's own strategic interests to the detriment of Canada.
- Covert and/or coercive.
- Conducted by intelligence, judicial representatives, police agents or proxies.

FAI does not include legitimate foreign influence activity conducted by states, such as police, diplomatic or cultural engagement.

WU8
WWU18

UNCLASSIFIED

Foreign Actor Interference

What is it really?

- Information was taken without authorization
- Someone was compelled to do or not to do something at the direction or benefit of a foreign state

Slide 11

WU8	In the speaking notes, included examples. Pulled information from the FAI Handout (page 1) Windows User; 2/3/2020 11:15:07 AM
WU13	noted and meets need Windows User; 2/6/2020 11:15:24 AM
WU18	NOTE: Removed OR between both bullets. Both can happen, not just one or the other. Windows User; 2/20/2020 12:13:13 PM

UNCLASSIFIED

Foreign Actor Interference Activities

Intimidation and Harassment

Gathering information & reporting on individuals

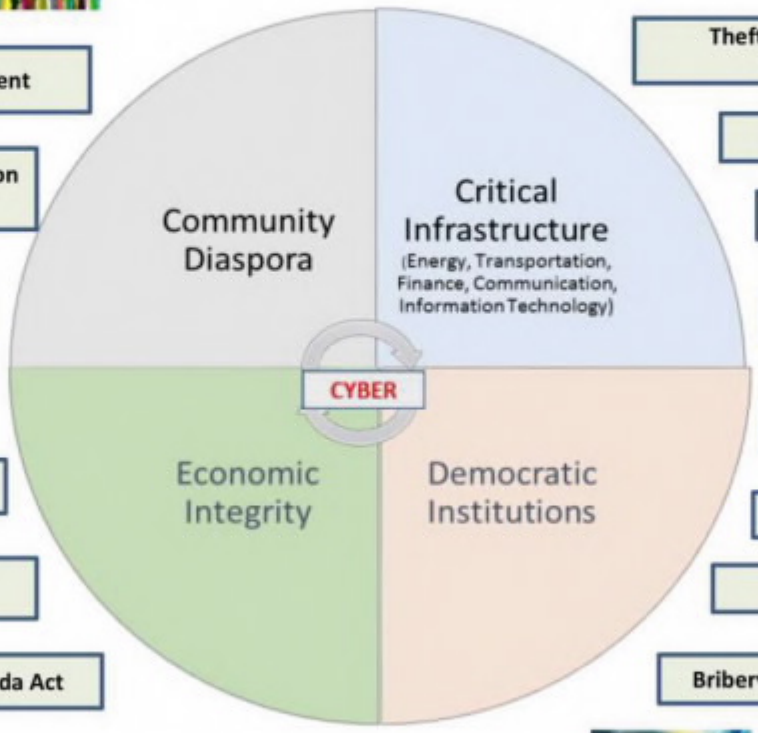
Bribery/Blackmail

Theft/Selling of Technology or Intellectual Property

Insider Threat

Physical Attacks

Hacktivism



Theft/ Selling Military Secrets

Theft/Selling of Technology or Intellectual Property

SECRET

Investment Canada Act

Electoral Interference

Disinformation Campaigns

Political Infiltration

Bribery/Blackmail

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

10

Role of Law Enforcement in Addressing FAI

RCMP Response

- The RCMP has a clear mandate to investigate FAI under the *Security Offences Act*, as a threat to the security of Canada *(CSIS Act)*
- Engaging domestic and international partners
- Critical infrastructure and cyber initiatives
- Reviewing legislative and regulatory regime; existing operational capability and capacity; and the role of law enforcement in addressing the threat

UNCLASSIFIED

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
  - Have the necessary relationships that will enable community members to report intimidation tactics
- **Identifying, disrupting and reporting cases**
  - Reporting possible incidents of espionage, sabotage, and other activities detrimental to Canada interests and national security

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

Engagement with Non-Traditional Partners

Non-Traditional Partners

- Critical Infrastructure Owners and Operators
- Canadian private industry
- Academia

Challenges

- Secure a formal complaint - industry is reticent to report possible security breaches due to reputational risk
- Difficult to assess the 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

Various Types of FAI Investigations

Can anyone give me an example of a type of FAI activity?

Slide 18

WU1 New Slide - As per L&D's feedback, included a slide with a question to increase learner participation
Windows User; 1/31/2020 3:20:03 PM

Insider Threat

An individual with insider access and/or knowledge of a company, organization, or enterprise can exploit its vulnerabilities and intentionally misuse their access in a manner which negatively impacts the organization's information.

Intimidation

Commit forms of illegal intimidation to compel Canadian citizens in Canada or abroad and/or individuals residing in Canada to do or not to do something at the benefit or the support of a foreign entity.

Intimidation

What is Criminal Intimidation?

- Criminal harassment
- Intimidation:
  - Unauthorized use of a computer
  - Interception of private communications

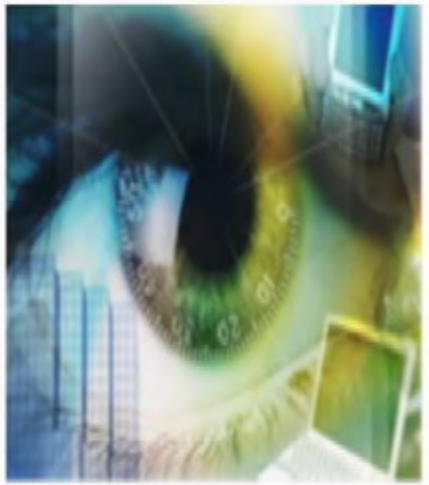
Intimidation

Who is involved in intimidation activities in Canada?

- Foreign Police
- Prosecutors
- Proxies

Theft of Technology

Agents of a foreign entity who, in support of a foreign entity, illegally obtain or the attempt to obtain technology that is safeguarded, protected by the Government of Canada, a Province/Territory or a trade secret for a purpose of increasing the capacity of the foreign entity.



Can anyone tell me if there has been a FAI investigation conducted in Canada?

WU2

Slide 24

WU2	New Slide - As per L&D's feedback, included a slide with a question to increase learner participation Windows User; 1/31/2020 3:22:44 PM

WU2

Case Studies

Slide 25

WU2 Slide use to read "Various Types of FAI Investigations

Windows User; 1/31/2020 3:22:44 PM

Case Study – Insider Threat

Project STOIQUE

- In 2007, Sub-Lieutenant Jeffrey Paul DELISLE in the Royal Canadian Navy walked into the Russian Embassy in Ottawa and offered to sell top secret allied intelligence to the Russian military intelligence service
- In 2012, he pled guilty and was sentenced to 20 years in prison
- Charges include:
  - Two counts of passing secret information to a foreign entity (*Security of Information Act*)

Case Study – Theft of Technology

Project SENTIMENTAL – Dr. Klaus NIELSEN

- World-renowned Canadian scientist; considered an expert in the field of animal brucellosis
- Employed by the Canadian Food Inspection Agency (CFIA) as a Research Scientist, in charge of a brucellosis lab overseeing several technicians
- Dr. NIELSEN was a critical and exclusive human resource, well-travelled and many publications - **He was a target**

Case Study – Theft of Technology

Project SENTIMENTAL – Ms. Weiling YU

- Sought to and ultimately worked at CFIA under the supervision of Dr. NIELSEN
- Established a biotechnical development and consultation company, the Peace River Biotechnology Company (PRBTC), owning 99% of its shares
- Close proximity to Dr. NIELSEN developed into Psychological control/dependence takes time
- Gradual change in relationship - friendship

Slide 28

WU17 Modifications made to last bullet on slide
Windows User; 2/20/2020 12:12:06 PM

Case Study – Theft of Technology

Project SENTIMENTAL – Outcomes

- In January 2011, NEILSEN and YU were both terminated from employment (with cause) at the CFIA.
- In March 2011, the CFIA laid a complaint with the RCMP.
- In 2014, RCMP conducted a controlled arrest of NIELSON. Vials of dead bacteria were found in a suitcase.
- In August 2014, NIELSEN pled guilty to all charges.
- In March 2017, he was sentenced to two years in prison.
- Ms. YU is the subject of a Canada-wide Warrant for Breach of Trust by Public Officer (*Criminal Code*).

Case Study – Theft of Technology

Project SENTIMENTAL – Charges

- Breach of Trust by Public Officer - Sec. 122, Criminal Code
- Wanton or Reckless Breach of Duty - Sec. 6 and Sec. 55 Human Pathogens and Toxins Act
- Failure to Inform Minister of an Activity - Sec. 70 and Sec. 55 Human Pathogens and Toxins Act
- Failure to Comply Sec. 33 Transportation of Dangerous Goods Act
- Attempt to Export a Good listed on an Export Control List - Sec. 13 and Sec 19 Export and Import Permits Act

UNCLASSIFIED

Case Study – Intimidation

Turkey and the GULEN Movement

- The Turkish Government has labeled Muhammed GULEN as a "terrorist" and the "GULEN Movement" or "Hismet Movement" a terrorist organization.

- Turkish communities members who support the GULEN Movement throughout the world, including Canada, have been victims of forms of intimidation and physical assaults by reported members of the Turkish government or their proxies who support the ruling party of Turkey and it's objectives to eliminate the GULEN Movement.

UNCLASSIFIED

Case Study – Intimidation

WU10
WU14
WU15
WU16

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

40

Slide 32

WU10	New slide - media clip depicting violent clash between protecters and supporters of Turkey's President Erdogan outside the Turkish ambassador's residence in Washington DC in May 2017 Windows User; 2/3/2020 11:34:12 AM
WU14	This is great. Windows User; 2/6/2020 11:18:54 AM
WU15	does the Windows User; 2/6/2020 11:19:26 AM
WU16	Added additonal link to deck in case Windows User; 2/6/2020 11:42:43 AM

UNCLASSIFIED

FOX HUNT Activities

"Fox Hunt" is an international initiative of the People's Republic of China (PRC) to repatriate and prosecute alleged economic fugitives in support of the Communist Party of China's anti-corruption efforts.

INTERPOL

RED NOTICE

The individuals may be associated to illegal economic crimes equitable to criminal offences in Canada or may be fleeing political persecution that is not equitable to a criminal or any other legislative Canadian offence.

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Consequence Management

- Maintaining Operational Security
  - Who could be watching or listening?
  - Sensitive information handling
  - Use of secure devices
- Safety of victims, witnesses and third parties
- Loss or destruction of evidence / information
- International relations
- Police independence while seeking to mitigate larger issues

Challenges

- Identifying a complaint / complainant
- Ensuring police of jurisdiction identify Fox Hunt activities and refer them to the RCMP's national security enforcement teams
- Maintaining the cooperation of the complainant
- Obtaining sufficient evidence to support criminal charges
- Language/Translation and technology translation

Way Forward

- Encouraging early identification of threats through cooperation between municipal police forces and the RCMP
- Broader interaction with other individuals, units, government agencies and/or states
- Proactively identifying Fox Hunt activities in Canada
- Educating RCMP national security enforcement teams
- Maintenance of security processes

WU9

Overview

Recap:

- What is Foreign Actor Interference (FAI)?
- The RCMP's mandate to investigate FAI
- The importance of maintaining operational security when involved in these types of investigations

Slide 37

WU9 New slide: Provides review of the objectives of the presentation (recommendation made by Learning and Development)
Windows User; 2/3/2020 11:20:51 AM

Questions

Slide Notes

Slide 5:
Foreign Actor Interference (FAI) has become an ever increasing concern to the people and Government of Canada. Now is a time that Law Enforcement can renew awareness of what Foreign Actor Interference is and what are some of our recent lessons learned in responding to those investigations. The illegal acts which define FAI may occur in any community and while the RCMP is mandated to investigate FAI investigations all law enforcement have a responsibility and role to respond to the threat posed. There is an expectation that FAI investigations will increase in the immediate future.

Slide 6:
Answer: YES - We are mandated to investigate foreign interference crimes

Slide 7:
The nexus of an FAI offence falling within the National Security mandate is not obvious.

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 8:
RCMP must accept that public safety, rather than charges/prosecution, should be 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);
Security of Information Act (SOIA): Includes numerous offences and sections in relation to FI, 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.
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 Sect 423 or Mischief Sec 430. Other provisions, such as bribery, or harassment, could also be used to disrupt FI.
Investment Canada Act (ICA): The RCMP is prescribed as an investigative body, mandating the RCMP to participate in the review of foreign investment to determine if there is any possible injury.
Immigration and Refugee Protection Act (IRPA): Working with partners, IRCC may cancel, refuse to issue, or revoke a passport. Security screening tools may provide IRCC with the reasonable ground to suspect that an individual has ties with a hostile state, and intends to conduct malicious activities on behalf of said state.

FPNS investigators must be aware that there are other units within the RCMP who have an Foreign Interference Mandate such as RCMP CYBERCRIME and RCMP SII. - Understanding that others within the RCMP may have or conduct investigation which may be pertinent FPNS investigations.

Slide 10:

Foreign Actor Interference is defined as an activity conducted or supported by a foreign state/actor that is detrimental to Canadian national interest and is clandestine deceptive or involves a threat to a person. For law enforcement officer Foreign Actor Interference investigations are basically cases of individuals taking something without permission or intimidating people to do or not to do something to the benefit or the direction of a foreign state. They are criminal or illegal acts.

Targets Canadian interests, or interferes in Canadian society.

Impact on economic integrity

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

Slide 11:

The RCMP has investigated several Foreign Actor Investigations across Canada. The most prevalent foreign government reported to be associated to these investigations is the People's Republic of China; however, there are other states who have been reported to be involved in FAI investigations such as Russia, These states have sought to benefit from illegal acts undertaken in Canada and or against Canadians.

Provide examples:
FAI can involve threats to Canadians at home or abroad via media posting and or personal interactions, critical infrastructure disruption, espionage and intellectual property (IP) theft. Foreign actors may seek to steal: proprietary software, business plans, customer information or product information (ex. designs, formulas, schematics) to increase the capacity of the foreign entity. Businesses and institutions with valuable information are often the targets for IP or information theft. FAI can be successful because the illegal acts are not identified or perceived to have been undertaken in support of a foreign actor - failure to identify the reasons the offence(s) have taken place enables the foreign actors to be successful.

Slide 12:

Understanding what Foreign Actor Interference is will aid in not only responding to various complaints police receive; but, it will aid in understanding what may be the consequences of undertaking such investigations.

Slide 14:

Federal Policing National Security – Investigation of threats to Canada National Security
Federal Policing National Division Cybercrime Team (NCDT)- NDCT investigations can lead to charges in Canada or a foreign jurisdiction, or for strategic disruptions involving FAI
Public Engagement Unit and Outreach
Necessary relationships that will enable community members to report intimidation tactics
National Intelligence Coordination Centre (NICC)
Identifying emerging threats, operational opportunities, and intelligence gaps
National Security Investigation FAI Team and - Multi-functional team to provide governance, analyse and assist in the investigation of acts of FAI by INSET/NSES.
National Critical Infrastructure Team (NCIT)
Identifies physical and cyber threats to critical infrastructure in Canada, conducts assessments, and has established partnerships with owners and operators of Canadian critical infrastructure which enables reporting of theft of technology, Intellectual Property (IP) and proprietary information, or other suspicious behaviour.

Slide 15:

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

Grooming complainant – unified front

Disclosure – joint effort

Slide 16:

Targeting Canadian Industry and Non-Traditional Partners
Companies leading in innovation, research & development, and cutting edge technology are attractive targets
Covertly obtaining sensitive technology or information from another organization can cause significant damage to Canadian interests
Canadian owners and operators of Critical Infrastructure, Academia and other private industry stakeholders are attractive targets for FAI activities due to the information they have in their holdings or their access to sensitive and classified information.

Challenges for Law Enforcement
1) Company losses may not only be financial; it might affect reputation (embarrassment for breach, no longer viewed at the forefront of innovation, which affects a company's confidence and relationship with clients), time lost for research, loss of confidence by board of directors.

Approach: LE needs to build trust and explain the process, next steps, protection of information, agency mandate and jurisdiction.

2) Not always able to provide a full picture of what was stolen or reproduced. When reporting suspected insider threat or FAI to law enforcement, it is important for industry to explain what information was stolen and its significance (what the loss or theft of this information or technology could mean) so that law enforcement can provide an appropriate response. Even when a breach is discovered, the scope or extent of loss may not be known.

For example, was the technology stolen?
Could it be used for nefarious purposes?
Does it pose a risk to public safety in the wrong hands?
What is the risk to industry as a whole? (e.g. if it is happening at one company or university, it is likely to happen to others)

Approach: Industry must take time to understand what happened, what was stolen and its significance. Identifying when and how a breach goes from an internal matter to the criminal space, and then to National Security space.

3) An ongoing internal investigation (i.e. administrative process and regulatory policies) can be done in tandem with a criminal investigation. Sometimes, industry will hire a private company to do an initial investigation. This should not hinder engagement with LE.

Approach: Early reporting and engagement between Corporate (HR, Security Officer), LE and S&I community is key.

Slide 18:
Answer:
Insider Threat
Intimidation
Theft of Technology
Theft of Knowledge / Intellectual Property
Electoral Interference
Mischief concerning computer data (i.e. hacking)

Presenter can refer the audience to the FAI Handout and review the document with the participants.

Slide 19:
What we know.....
Espionage is not new; it is one of the oldest methods used to obtain secret or confidential information without the permission of the holder of the information.

Historically, espionage has been associated with the military, and one of the most tried and true, or effective ways to obtain data and information about an enemy is by infiltrating the enemy's ranks. If used figuratively, 'infiltrating the enemy's ranks' is happening often to Canadian companies in the form of 'insider threat'.

Espionage that targets companies is known as 'industrial' or 'economic' espionage and this has become a significant concern and threat worldwide, including to Canada. Foreign interference in Canada constitutes a threat to the security of Canada.

An individual with insider access and/or knowledge of a company, organization, or enterprise can exploit its vulnerabilities and intentionally misuse their access in a manner which negatively impacts the company.

Typically, the insider threat is someone who (as the name suggests) is inside a company and has access to sensitive information. This can also extend well beyond traditional borders or walls of a network, to vendors, suppliers, contractors and sub-contractors.

Targeting Canadian Industry

Companies leading in innovation, research & development, and cutting edge technology are attractive targets
Insider threats can weaken or destroy public trust in a company, threatening its financial foundation
Covertly obtaining sensitive technology or information from another organization can cause significant damage to Canadian interests

Motivation
When an individual makes the decision to use their access in ways other than intended – abusing privileges with malicious intent towards the organization – that individual becomes an insider threat.

Often, warning signs are present but may go unreported for years because colleagues of these individuals are unwilling or hesitant to accept the idea that a trusted co-worker could be engaged in insider activity. Businesses are built on teamwork and require counterparts to trust and support one another, making it difficult for colleagues to acknowledge warning signs and red flags when they are present.

This further complicates the challenges that exist in successfully defending against insider threats.

Canadian companies, particularly those leading in the areas of innovation, research and development, technology, as well as companies working in natural resources, such as energy and mineral resources, are attractive targets to those who wish to engage in economic espionage.

The progress and innovation Canadian companies have achieved can be significantly marred by individuals or groups covertly obtaining sensitive technology, intellectual property, or other corporate information.

It is estimated that Canada loses up to $20 billion annually from economic espionage, a marked loss to the Canadian economy.

Slide 20:
Foreign Actor Interference investigations also involve incidents where agents of a foreign entity, who at the direction of or for the benefit of the foreign entity, commit forms of illegal intimidation or harassment to compel persons in Canada or Canadian Citizens abroad to do or not to do something.

An example of unique FAI investigation is when Canadian police receive a report that a Canadian Citizen who has been seriously assaulted or their life has been threatened for a political reason at the direction or the benefit of a foreign state while in another country. The criminal code allows for an extra territorial investigation to be undertaken abroad, if the illegal act is completed by an individual for a political, ideological or religious reason; if the attack is reported to be at the direction and support of a political entity then the investigation may fall within the purview of the Canadian Police to investigate. However, the consequences of undertaking such investigations would by necessity the need or process to describe a foreign entity was conducting "terrorism activity". Such titles of offences and associated to other countries may cause severe consequences politically to Canada and or its Canadian citizens.

Slide 21:

criminal offences of Intimidation and or Criminal harassment against a person outside of Canada may violate s. 465(1)(b) CCC – Conspiracy.

465 (1) Except where otherwise expressly provided by law, the following provisions apply in respect of conspiracy:

[…]

(b) every one who conspires with any one to prosecute a person for an alleged offence, knowing that he did not commit that offence, is guilty of an indictable offence […]

Conspiracy to commit offences

(3) Everyone who, while in Canada, conspires with anyone to do anything referred to in subsection (1) in a place outside Canada that is an offence under the laws of that place shall be deemed to have conspired to do that thing in Canada.

Idem

(4) Everyone who, while in a place outside Canada, conspires with anyone to do anything referred to in subsection (1) in Canada shall be deemed to have conspired in Canada to do that thing.

[…]

Note: Section 465 (1) is not an "offence" recognized under Part VI – Invasion of Privacy (s. 183) of the CCC.

Slide 22:
Give examples:

PRC MPS Police officers
PRC MPS Prosecutors.
Proxies those acting for the above – example a permanent resident of Canada told and complying with directions from a foreign police officer, prosecutor or other government official.

Slide 23:
Theft of information / Technology is a type of Foreign Actor Interference investigation which are incidents of agents or proxies of a foreign entity illegally obtaining or the attempting to obtain information or technology that is protected by the government of Canada or is a trade secret and that obtainment is for a purpose of increasing the capacity of the foreign entity.

Examples of police investigations which the RCMP National Security Program have monitored for a foreign entity involvement was a report of a theft of students and professor's passwords from a university data base; and the theft of protected data by a contracted employees working at a government facility.
The thefts may be at the direction or in support of a foreign state because the data taken may have:
provided access points to obtain other protected data,
provided highly valued research information not publically accessible,
access to information may which may be of dual use meaning the information taken may be used to creating or advancing weapons.
In those cases the investigations did not determine an association to a foreign state but both the Police of Jurisdiction and the RCMP completed and assessment of the matter.

Slide 24:
Answer: YES
And there has been successful prosecutions of the same.

Slide 26:
In July 2007, DELISLE walked into the Russian Embassy in Ottawa and offered to sell secret information to the Russian military intelligence service (known as the GRU).

DELISLE's activities were particularly damaging due to his access to a database of intelligence shared between Canada, the United States, the United Kingdom, Australia and New Zealand.

In July 2007, DELISLE walked into the Russian Embassy in Ottawa and offered to sell secret information to the Russian military intelligence service (known as the GRU).

DELISLE's activities were particularly damaging due to his access to a database of intelligence shared between Canada, the United States, the United Kingdom, Australia and New Zealand. Espionage and insider activity can weaken or destroy public trust in a Canadian company, or even damage Canada's working relations with its allies.

DELISLE blamed his espionage activities on his marital problems, rather than financial need.

Charges include:
Two counts of passing secret information to a foreign entity (Security of Information Act)

In 2012, DELISLE pled guilty and was sentenced to 20 years in prison less the time he had already served in custody awaiting trial. He was also stripped of his commission, service decorations and was dishonourably discharged.

In March 2019, DELISLE was granted full parole after serving one-third of his sentence.

Slide 27:

Dr. Klaus NIELSEN was a world-renowned scientist who focused much of his research on the bacteria brucellosis. In particular, Dr. NIELSEN was considered a subject matter expert in the field of animal brucellosis, a highly contagious and chronic infectious disease affecting many species of animals which can also be transmitted to humans. Dr. NIELSEN was employed by the Government of Canada since 1979 and spent a considerable length of his career at the Canadian Food Inspection Agency (CFIA) as a Research Scientist.

The CFIA had a collaborative research agreement with DIACHEMIX, providing the company with worldwide commercialization rights to all joint patents arising from the agreement. Intellectual property was deemed to be the joint property of DIACHEMIX and the CFIA, and would be treated as confidential by both parties.

In the 1990s, Dr. NIELSEN and a scientist from DIACHEMIX, Michael Jolley, developed an antigen used in Fluorescence Polarisation (FP) testing kits for brucellosis. This antigen became the subject of a US patent in 1999, and again in 2003.

DIACHEMIX, a private company with a collaborative research agreement (CRA) the Canadian Food Inspection Agency (CFIA) developed diagnostic tests for animal diseases and food safety.

In and around 2005, Dr. NIELSEN's professional behaviours began to change. These behaviours were noticed by coworkers, but not acted upon.
They include: violating the Material Transfer Agreement policy; not fully declaring his conflict of interest working with a foreign company; requesting a "twinning project" with a foreign company (declined); travelling to the People's Republic of China (PRC) and not liaising with the CFIA PRC point of contact; and, requesting the CFIA's "Conflict of Interest Guidelines".

During this period, equipment and material also went missing from the lab.
Another noted change was that Dr. NIELSEN reduced the size of his lab from eight to ten, down to two or three, although brucellosis is a reportable disease and it would be considered normal to have a larger staff.

In April 2010, the CFIA reported to, that two DIACHEMIX employees (Dr. NIELSEN and Ms. Weiling YU) were manufacturing brucellosis diagnostic kits contrary to the CRA through a company called the Peace River Biotechnology Company (PRBTC).

Beginning in 2011, Dr. NIELSEN was investigated for illegally obtaining research information protected by the government of Canada at CFIA and was patently protected by a US company collaborating with the CFIA. Dr. NIELSEN and fellow CFIA researcher from China, Ms. Weiling YU illegally obtained protected information and attempted moved samples of pathogens for the purpose of illegally patenting a manufacturing process in China. The benefits were monetary to NIELSEN and his accomplice; but, the illegal act also provided China with years of expensive and very unique research for a very low cost. It is an investigative belief that Dr. NIELSEN was targeted by YU who currently resides in China and has an outstanding warrant for her arrest for same offences as Dr. NIELSEN.

Slide 28:
As part of his work responsibilities at the CFIA, Dr. NIELSEN was in charge of a brucellosis lab overseeing several lab technicians.
In 2001, Weiling YU began employment with the CFIA under the supervision of Dr. NIELSEN.
Ms. YU was born in Heilongjiang, China and had worked in the Immunology Department of the Harbin Medical University in Harbin, China.

In 2005, Ms. YU became a Canadian citizen in 2005.

In March 2006, Ms. YU established the Peace River Biotechnology Company (PRBTC), specializing in biotechnical development and consultation.
Ms. YU was a junior technician from a suspect foreign power, emplaced close to Dr. NIELSEN.
After three years as a functionary-type lab technician, Ms. YU began to move up rapidly, although she did not have the required expertise or knowledge.
Dr. NIELSEN began to travel to the PRC with Ms. YU and, similarly, Ms. YU would accompany Dr. NIELSEN on trips; they appeared inseparable.

Slide 29:
Both Ms. YU and Dr. NIELSEN were terminated from employment by CFIA in 2011.

During the RCMP OINSET investigation, Dr. NIELSEN acknowledged that unauthorized shipments were made to China (via the PRBTC) and that he was an unpaid consultant to the company.

He further stated that he was trying to help the company start itself up and offered a less expensive alternative to brucellosis testing to certain markets.

Ms. YU denied everything, stating that the shipments were not made to PRBTC, but to PhD students in China. She denied any involvement in the company and denied everything that linked her to the company.

During the course of the investigation, classic tradecraft methodology was identified. It became apparent that proximity is key to isolating and co-opting the target subject; psychological control/dependence takes time to develop; there is a gradual change in agent/target relationship; and, an emplacement was not accidental.

In this case, Dr. NIELSEN was a critical and exclusive human asset; he was a person with an international profile, well-travelled and published, making him a valuable target.

He was convicted of Breach of Trust and 10 counts relating to the offences under the Human Pathogens and Toxins Act, the Export and Import Permits Act, and the Transportation of Dangerous Goods Act.

Charges include:
Breach of Trust by Public Officer (Criminal Code)
Wanton or Reckless Breach of Duty (Human Pathogens and Toxins Act)
Failure to Inform Minister of an Activity (Human Pathogens and Toxins Act)
Failure to Comply (Transportation of Dangerous Goods Act)
Attempt to Export a Good listed on an Export Control List (Export & Import Permits Act.)

The RCMP investigation enabled CFIA to fully understand what had actually happened and what damage had been done.

The RCMP investigation used a covert posture to undo the conspiracy, which included the use of Part VI, covert entries, surreptitious entries and undercover operations.

If insider activity is suspected, it is beneficial to engage law enforcement as they have the legal authority and mandate to use more investigative techniques than a company itself, undertaking an internal investigation on their own, even with the assistance from a private investigation company.

Slide 30:
He was convicted of Breach of Trust and 10 counts relating to the offences under the Human Pathogens and Toxins Act, the Export and Import Permits Act, and the Transportation of Dangerous Goods Act.

Charges include:
Beach of Trust by Public Officer (Criminal Code)
Wanton or Reckless Breach of Duty (Human Pathogens and Toxins Act)
Failure to Inform Minister of an Activity (Human Pathogens and Toxins Act)
Failure to Comply (Transportation of Dangerous Goods Act)
Attempt to Export a Good listed on an Export Control List (Export & Import Permits Act.)

The RCMP investigation enabled CFIA to fully understand what had actually happened and what damage had been done.

The RCMP investigation used a covert posture to undo the conspiracy, which included the use of Part VI, covert entries, surreptitious entries and undercover operations.

If insider activity is suspected, it is beneficial to engage law enforcement as they have the legal authority and mandate to use more investigative techniques than a company itself, undertaking an internal investigation on their own, even with the assistance from a private investigation company.

Slide 31:

The Turkish President Recep Tayyip ERDOGAN and Muhammed Fethullah GULEN have been long time political rivals in Turkey. Recently, President ERDOGAN's government has blamed GULEN for masterminding the unsuccessful coup d'état that took place on July 15, 2016, a charge that GULEN denies. No evidence has been provided thus far to support this claim. GULEN has been in living in exile since 1999 in Saylorsburg, Pennsylvania. GULEN has a large following in Turkey and around the world including Canada. While GULEN's followers do not have any official membership status, they are recognized as supporters of "The GULEN Movement", also known as the "The Hizmet Movement". The Turkish Government feels that its authority is undermined by GULEN followers. This has led to a very polarized and deeply divided Turkish diaspora in Canada and around the world. Following the coup d'état attempt on July 15, 2016, there have been numerous media reports suggesting that GULEN followers are being targeted throughout Europe and North America by the agents of the Turkish Government. Since the Turkish Government blames the 2016 coup on GULEN, their government has been seeking extradition of GULEN supporters from the US government, a request that the US has declined thus far, citing lack of evidence provided by the Turkish Government for GULEN role in the coup. The Turkish Government has labeled GULEN a "terrorist" and his "GULEN Movement" also known as "Hismet Movement" a terrorist organization.

There have been incidents of concern in the Turkish communities in the GTA about profiling and targeting by Turkish members who support the current ruling party of Turkey.

People linked with the Turkish Government are reported to be spying on GULEN supporters and reporting information back to the Turkish Government. This makes situation difficult for the relatives of those Turkish Canadians who live in Turkey.

Reports of Turkish representatives visiting different Mosques stating the a negative view of GULEN supporters, and calling them all "terrorists". They allege that the actions of the representatives have resulted in individuals being banned from some Turkish community events and community Mosques.

During a Turkish community event in Ottawa, alleged Turkish Government supporters came to demonstrate against the community event, calling them supporters of GULEN. While no physical violence was reported; photographs of organizers were taken and posted on Facebook. This caused fear for those Turkish Canadians who have families in Turkey, or wish to travel to Turkey to visit families.

Two violent occurrences were been reported have been reported of GULEN supporters being assaulted on was assaulted coming out of a local Home Depot store and other was assaulted near his residence after trying to video individuals who had come to their home. It is alleged that the accused were supporters of the Turkish government. Incidents were apparently reported to the local police of jurisdiction. Charges were not laid in each matter.

Those residing in Canada who come forward have their concerns were acknowledged, however discussions lend to insure that reports of such events fits with the RCMP's authority INSET/NSES or the police of jurisdiction. However, any victims or witness's of criminal activities should be reported to the police of jurisdiction immediately.

It was stressed to the community leader's that incidents of harassment, intimidation and threats need to be reported by the victims directly to the police and not through hearsay and other means of representation. They were advised that future incidents could be deterred if the community reported the incidents to police.

It was explained that law enforcement in Canada does not have a reach beyond criminal activity in society. Suggestions were made to file civil libel lawsuits especially in the cases where slander against members of the community caused financial loss, for example being labeled a 'terrorist' caused a person to lose their job.

Slide 32:

Violent clashes broke out between protesters and supporters of Turkey's President Tayyip Erdogan outside the Turkish ambassador's residence in May 2017, in Washington.

Despite that the incident took place in the United States, this depicts a good example of intimidation – the video shows men in suits charging past police to kick and punch protesters.

One would interpret this incident as an attach on peaceful protesters. The Turkish embassy, however, said that the demonstrators had aggressively provoked Turkish-Americans gathering to greet the President and the bodyguards had responded in self-defence.

LINK TO VIDEO (duration 1:55 minutes)

https://www.haaretz.com/middle-east-news/turkey/erdogan-trump-turkey-washington-bodyguards-1.8101174
(Source: BBC, US summons Turkey envoy for embassy brawl, May 18, 2017 https://www.bbc.com/news/world-us-canada-39969965)
LINK TO VIDEO BBC video May 17, 2017 https://www.youtube.com/watch?v=PLzgtpd5D3s (1:06 minutes).

Slide 33:
INTERPOL Red Notices and the MING PAO Daily News

RCMP assesses that there are PRC emissaries residing in or visiting Canada who are carrying out criminal activities in support of Project Fox Hunt – violation of domestic law and international obligations.

The investigation of these matters is within the mandate of the RCMP National Security Program.

Another example of FAI investigations in Canada are incidents related to Project Fox Hunt or Skynet activities undertaken in Canada. These are terms publically available and describe activities related to an international initiative of the People's Republic of China to target and prosecute fugitives from China who are sought after for political or criminal matters. Those fleeing China may be associated to illegal activities similar to criminal offences in Canada others may be fleeing political persecution for which there is no equitable criminal or legislative offence. PRC may use traditional police to police requests for assistance to have the fugitives return to China an international arrest warrant and a request for extradition may be sought. When these authorized police to police government to government requests for assistance fail, PRC prosecutors or police officers travel to Canada to directly contact or use proxies to contact individuals and to illegally compel individuals to return to China. The process used by the PRC operatives may to intimidate person via threats of violence such as suggestion that suicide is an option if they do not return, restricting other family members' access to travel or state resources, or by criminal harassment by way of following besetting an individual in order to compel them to return to China.

The unique issues arise in these cases:
The individual may feel that they cannot report these incidents to police as they are suspected to be a criminal and are not subject to protection of Canadian law enforcement. Thus criminal actions are being undertaken in Canada and the victim is complaint to the request of the PRC representatives.
Others within the Chinese community in Canada may feel compelled to aid PRC operatives out of necessity because they are told or are aware of China's recently legislated National Security Law that compels all Chinese citizens regardless of their location to aid PRC agents in their request for assistance.
There have been very high profile examples of senior members of the Chinese government officials being returned to Canada without consequence to China.

RED NOTICE Interpol Ottawa report of a man wanted in China for Bribery and Embezzlement for which PRC Law Enforcement had obtained and currently maintains an active Red Notice - first issued in 2005. China actions to support the return of the man from Canada were not successful. However China remains committed to having the man returned to China by placing adds in local community papers.

"Ming Pao Daily" is a daily Chinese language publication printed in Toronto and Vancouver which is owned by Ming Pao of Hong Kong. Open media assessments of Ming Pao indicate it is a pro-government of China publication.

Another example of publicly reported possible PRC foreign interference is China's interaction with of Uyhgurs and Tibetans and pro-democracy supporters living in Canada. (Three of the five poisons.) It has been reported in the media that the PRC government may use operatives or proxies to influence and at times threaten member of these minority groups to stop making statements that run contrary to the PRC objectives.

Some such examples were never reported to Canadian police for fear of retribution or lack of trust in Canadian Law enforcement other times complaints are reported to the RCMP or police of jurisdiction. When such complaints are received assessments are made as to which law enforcement agency RCMP / POJ is best able to respond to the threats and mitigate the issue. However, the police must be aware of false reporting however rare they may be. For example, a member of a minority group reported to their family that they were forced to return to China and not to report the matter to the police. The police became involved and after an extensive joint RCMP POJ investigation the report kidnapping abduction was proven to be hidden travel to enable an extramarital affair.

Slide 34:
The security of FAI investigations is imperative to mitigate consequences of investigations.

There will be consequences of FAI investigation and investigators must make all attempts to minimise threats to the investigation they can control.

The security of the investigation is most important to:
most importantly ensure the safety of victims, witnesses and possibly unknown third party individuals,
international relations,
police independence,
Determining how to handle sensitive information that if disclosed could be reasonably be expected to cause serious injury to the national interest.

Which then must include the cost and maintenance of operational security, (responding to who could be watching or listening?. These cases do not involve just individual or criminal group but rather nation states that have the person and equipment with capability to obtain and possibly interfere with the police investigation.
Following that is sensitive information handling techniques and using secure devices to retain and transmit data or information is necessary.

Slide 35:
Challenges for Law Enforcement:

Not getting the full picture of what was stolen or reproduced. When reporting suspected insider threat to law enforcement, it is important to explain what information was stolen and its significance (what the loss or theft of this information or technology could mean) so that law enforcement can provide an appropriate response. For example, was the technology stolen considered dual-use? Could it be used for nefarious purposes? Does it pose a risk to public safety in the wrong hands?

LE need to build trust and explain the process, next steps, protection of information, agency mandate and jurisdiction

Industry may take time to understand what happens, what was stolen and its significance. Not getting the full picture of what was stolen or reproduced. When reporting suspected insider threat to law enforcement, it is important to explain what information was stolen and its significance (what the loss or theft of this information or technology could mean) so that law enforcement can provide an appropriate response. For example, was the technology stolen considered dual-use? Could it be used for nefarious purposes? Does it pose a risk to public safety in the wrong hands?

Identifying when and how a breach goes from an internal matter to the criminal space, and then to National Security space.

Make sure agency on board so one process

WHEN DEALING WITH INSIDER AND FAI, fulsome assessment will benefit everyone. We may not know what the end use is, attribution, is it FAI, or corporate espionage… Partners needs to be reassured, who is best placed to do so. Nothing stops us from talking among each others…

Witness statements taken by RCMP can be provided back to the company or organization to take any action, if required (ie. Termination of employment)

GOLD STANDARD IS NOT PROSECUTION but threat mitigation and disruption – PUBLIC SAFETY

Slide 36:
Identifying the FAI component be aware of the - mosaic effect - a situation in which information in isolation may not pose a risk but when combined with other available information could pose such a risk

FAI NS investigations – broad range of implications
Safety of victims and witnesses is parmanout
Must take into account Foreign relations and International implications

Slide 37:
RECAP – Review the objectives of the module with the course participants

What is FAI:
Illegal activity conducted, or directed, by a foreign actor that constitutes a threat to Canada's national security.
Advance a foreign entity's own strategic interests to the detriment of Canada.
Covert and/or coercive.
Conducted by intelligence, judicial representatives, police agents or proxies.

RCMP's mandate to investigate FAI:
Section 2, Canadian Security Intelligence Service (CSIS) Act: threats to the security of Canada means:
(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
Unlawful release of sensitive or classified information contrary to section 6 of the Security of Information Act (SOIA)

Consequence Management
The security of FAI investigations is imperative to mitigate consequences of investigations.

There will be consequences of FAI investigation and investigators must make all attempts to minimise threats to the investigation they can control.