

# FOREIGN INFLUENCED ACTIVITIES IN CANADA

BRIEFING FOR PARLIAMENTARIANS

UNCLASSIFIED



Canada 

For Public Release

# WHAT IS FOREIGN INFLUENCED ACTIVITY?

## A THREAT TO NATIONAL SECURITY

CONFIDENTIAL

In the *CSIS Act*, foreign influenced activities are defined as any activities within or relating to Canada that:

- are detrimental to the interests of Canada, and
- clandestine or deceptive or involve a threat to any person.

FI activity differs from normal diplomatic conduct or acceptable foreign state-actor lobbying.

Lawful advocacy and dissent is a healthy part of democracy. Clandestine or deceptive foreign interference is not.

# FOREIGN INFLUENCED ACTIVITY IN CANADA

## CANADA IS A TARGET OF FI

UNCLASSIFIED

Foreign states continue to engage in extensive and aggressive foreign influenced activities against Canadians and Canadian institutions.

States conduct FI activity to further their own strategic national interests.

The main goals of foreign interference are:

- strategic and economic gain;
- regime preservation; and
- discrediting liberal-democratic institutions.

FI and espionage constitute the greatest threats to Canada's long-term prosperity and security.

# THREAT TO DEMOCRATIC INSTITUTIONS

## PROTECTING OUR DEMOCRACY

UNCLASSIFIED

Canada is a target of foreign state efforts to interfere with or damage our democratic process and institutions.

Foreign states target voters, parties, candidates, elected officials and their staff, as well as electoral processes.

- FI activities have been observed at all levels of government in Canada.

FI poses a threat to the integrity of our political system, Canada's democratic institutions, and the rights and freedoms of Canadians.

Ahead of the 2019 election, FI activities will likely intensify.

# FOREIGN INFLUENCE TECHNIQUES

## A COMPLEX THREAT

UNCLASSIFIED

Foreign states employ a variety of tactics to target Canada:

- Foreign language and mainstream media in Canada have been used to promote foreign agendas and challenge Canadian interests.
- Communities in Canada are targeted by foreign states who try to silence dissent or use them as tools to support their FI activities.
- Spear phishing and other malicious cyber intrusions are used to gain access to private information to leverage for FI.

Person-to-person FI activities remain common, conducted by:

- Foreign diplomats;
- Intelligence officers; and
- Proxies and co-optees (both witting and unwitting).

Government and elected officials are targeted because of their access to privileged information, contacts and decision-makers.

# THE CYBER THREAT

## CYBER INFLUENCE ACTIVITIES

UNCLASSIFIED

Foreign cyber actors use different techniques for influence activities:

- Cyber threat actors use cyber tools to target the websites, e-mail, social media accounts, and the networks and devices of political parties, candidates, and their staff.
- Cyber threat actors could attempt to undermine trust in our elections or suppress voter turnout by altering content on websites, social media accounts, and networks and devices used by Elections Canada.
- Cyber threat actors manipulate online information, often on social media using cyber tools, in order to influence voters' opinions and behaviour.

# THE TARGETING OF INDIVIDUALS

## TARGETING

UNCLASSIFIED

Foreign governments may target you, directly or indirectly, because:

- You possess information they want;
- You have access to information they want; or
- You are in a position to influence government policy.

Techniques employed – both in Canada and overseas, can include:

- Elicitation;
- Cultivation;
- Intrusion;
- The 'Honey Trap'; and
- Eavesdropping.

Foreign governments may also seek to discredit you to further their strategic agendas.

# STEPS TO PROTECT YOURSELF AND YOUR INFORMATION

## THREAT MITIGATION

**UNCLASSIFIED**

### Be Prepared

- Exercise care in carrying information; classified information should only be carried in a secure briefcase.
- Send information through secure channels in advance of travel.
- Travelling with clean electronics minimizes the loss and risk if a device is lost, stolen, hacked or copied.

### Be Cyber Safe

- Employ good cyber hygiene practices: use strong passwords for devices, enable two-factor authentication, secure mobile devices with passcodes or other identification (fingerprint or face recognition).
- Regularly patch devices and computers.
- Avoid using public wifi and, when travelling, assume that telecommunications may be monitored.

### Remain Vigilant

- Use discretion and assume that conversations in public places may be overheard.
- Be wary of gifts, especially electronic ones that can plug into your computer.
- Never click on links or open attachments unless you are certain you know who sent them and why.
- Be wary of approaches from strangers, particularly when their interest pertains to your work or area of interest. Even seemingly benign information can be of interest to foreign intelligence agencies.



# ADDRESSING THE THREAT

UNCLASSIFIED

## WHAT IS BEING DONE?

### Enhancing Awareness

- New resources for digital, news and civic literacy programming.
- Canadian Centre for Cyber Security has released resources, including an updated assessment of Cyber Threats to Canada's Democratic Process. The website [cyber.gc.ca/democracy](http://cyber.gc.ca/democracy) provides practical ways for Parliamentarians, parties and candidates to protect against cyber threats.

### Detecting and Assessing Threats

- Security and Intelligence Threats to Elections (SITE) Task Force established to build awareness of threats and support assessment and response.

### Responding to Threats

- G7 Rapid Response Mechanism Coordination Unit coordinates information sharing and threat analysis among G7 partners to better identify and respond to threats.
- Critical Election Incident Public Protocol provides a simple, non-partisan process for informing Canadians if series incidents threaten the integrity of the 2019 General Election.

# SECURITY AND INTELLIGENCE THREATS TO ELECTIONS TASK FORCE

## THE ROLES OF SITE PARTNERS

UNCLASSIFIED

UNCLASSIFIED FOR OFFICIAL USE ONLY





Security and Intelligence Threats to Elections Task Force - Partner Roles Leading to Election 2019



### SECURITY AND INTELLIGENCE THREATS TO ELECTIONS TASK FORCE

#### WHAT ARE WE TALKING ABOUT?

Covert, clandestine, or criminal activities interfering with or influencing electoral processes in Canada

	MANDATE/ROLE	ACTIVITIES
 <b>CSE</b> Communications Security Establishment	<b>Information Technology Security</b> <ul style="list-style-type: none"> <li>Providing advice, guidance, and services to help ensure the protection of electronic information and of systems of importance</li> </ul> <b>Foreign Intelligence</b> <ul style="list-style-type: none"> <li>Collection of foreign intelligence for Government of Canada on threat actors</li> </ul> Supporting CSIS and RCMP <ul style="list-style-type: none"> <li>Providing assistance on technical operations</li> </ul>	<ul style="list-style-type: none"> <li>Providing intelligence and cyber assessments on the intentions, activities, and capabilities of foreign threat actors</li> <li>Protecting Government systems and networks related to elections through cyber defence measures</li> <li>Providing cyber security advice and guidance to political parties, provinces and other institutions involved in democratic processes</li> </ul>
 <b>CSIS</b> Canadian Security Intelligence Service	<b>Intelligence and Threat Reduction</b> <ul style="list-style-type: none"> <li>Collection of information about foreign influenced activities that are detrimental to the interest of Canada and are clandestine or deceptive or involve a threat to any person</li> <li>Countering such activities through threat reduction measures</li> </ul> <b>Intelligence Assessment</b> <ul style="list-style-type: none"> <li>Providing advice, intelligence reporting and intelligence assessments to Government of Canada about foreign influenced activities</li> </ul>	<ul style="list-style-type: none"> <li>Providing threat briefings and intelligence reporting to Elections Canada and the Commissioner of Elections</li> <li>Providing an assessment of hostile state activity methodologies and capabilities to Government of Canada decision makers</li> </ul>
 <b>GAC</b> Global Affairs Canada	<b>G7 Rapid Response Mechanism</b> <ul style="list-style-type: none"> <li>Open source research on global trends and data on threats to democracy</li> <li>Partnership with G7 countries to share information and coordinate responses to threats as appropriate</li> </ul>	<ul style="list-style-type: none"> <li>Providing research on disinformation campaigns targeting Canada by foreign actors</li> <li>Reporting on global trends, metrics, and incidents</li> <li>Coordinating attribution of incidents</li> </ul>
 <b>RCMP</b> Royal Canadian Mounted Police	<b>National Security</b> <ul style="list-style-type: none"> <li>The primary responsibility for preventing, detecting, denying and responding to national security-related criminal threats in Canada</li> <li>Investigates criminal offences arising from terrorism, espionage, cyber attacks, and foreign influenced activities</li> <li>The key investigatory body for Elections Canada if criminal activity is suspected</li> </ul>	<ul style="list-style-type: none"> <li>Investigates any criminal activity related to interference or influence of Canada's electoral process</li> <li>Works closely in partnership with intelligence, law enforcement and regulatory agencies</li> </ul>

# CONCLUSION

## THREAT AWARENESS IS KEY

UNCLASSIFIED

- Foreign states continue to engage in aggressive FI activities in Canada to advance their own strategic interests.
- Canada's political system is the principal target of foreign states seeking to advance their political, economic and security agendas by influencing government policies and decisions.
- Individuals with perceived access or influence over decision-making, at the federal, provincial and municipal levels, may be targeted.
- FI activity may be conducted by individuals in Canada operating on behalf of a foreign state through person-to-person contact.
- Cyber tools provide another powerful means to influence the electorate, political outcomes and even, potentially, the electoral process.
- Preparation, vigilance, discretion and robust cyber security are important steps to mitigate against the threat.

/// PAGE 11

## Slide Notes

### Slide 7:

Any of the methods described here may be done via personal exchanges or through cyber space.

### Slide 8:

The best way to secure information or assets when you travel is to send classified information to your destination via classified email/mail before your departure. Never carry classified documentation.

Using clean electronics ensures that if lost, stolen, hacked, or copied, the loss of information is known, contained, and risk can be accurately assessed.

Pay special attention to security considerations when communicating over non-secure means of communications. Seemingly innocuous details can become intelligence information. Adversaries pay close attention to observables to deduce critical information about your projects, programs, and activities.

Ex: A CBC/Radio Canada investigation was just released regarding the compromise of NDP MP Matthew DUBE's cellphone, who volunteered for the experiment - discussions and geolocation.

Situational awareness

### Slide 9:

The Government of Canada recently announced its plan to protect Canada's democracy, including the 2019 Federal Election, from cyber and other threats