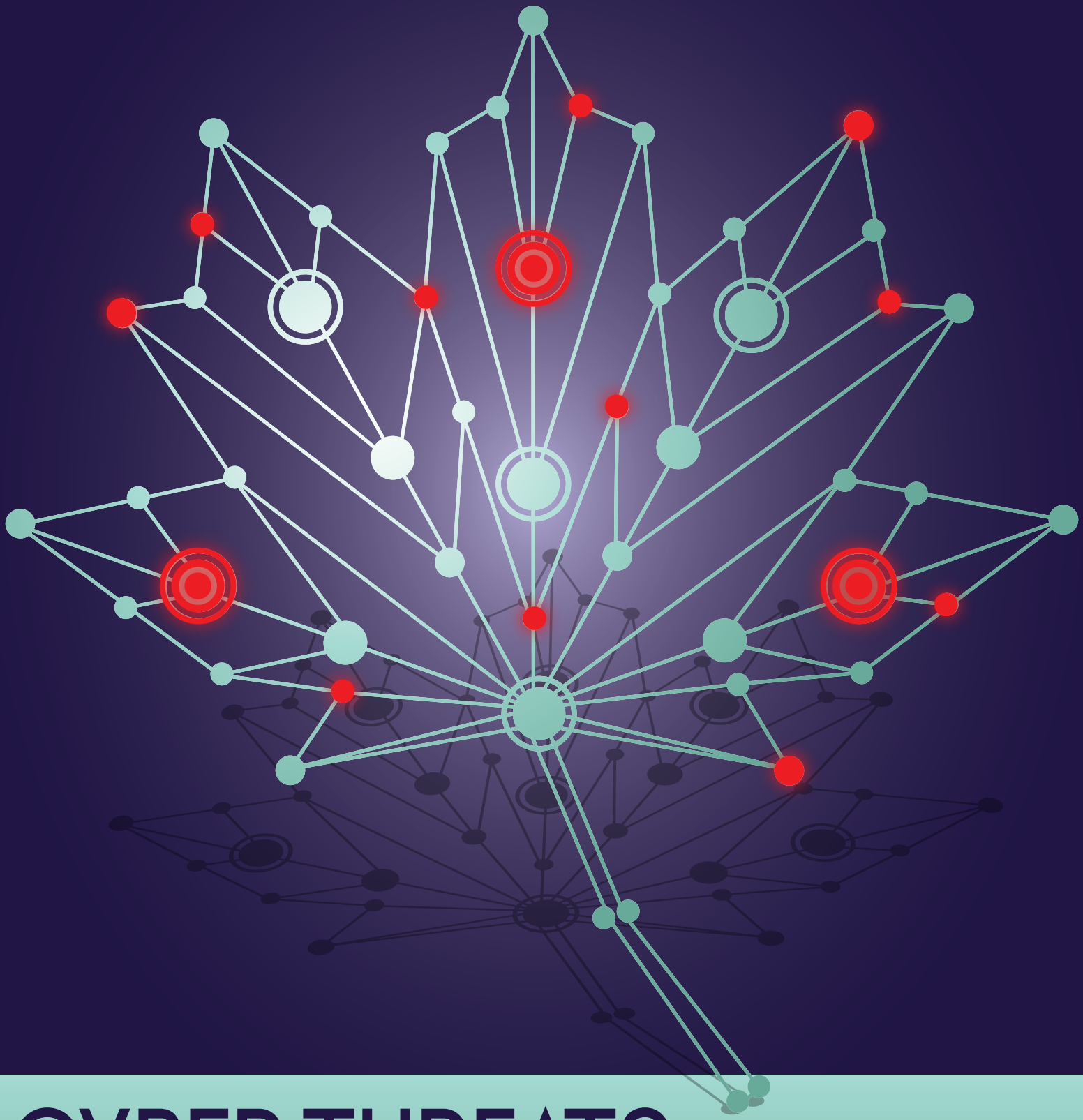
Communications Security Establishment
Centre de la sécurité des télécommunications



CYBER THREATS TO CANADA'S DEMOCRATIC PROCESS

Canada

ABOUT CSE

The Communications Security Establishment (CSE) is Canada's centre of excellence for cyber operations. As one of Canada's key security and intelligence organizations, CSE protects the computer networks and information of greatest importance to Canada and collects foreign signals intelligence. CSE also provides assistance to federal law enforcement and security organizations in their legally authorized activities, when they may need CSE's unique technical capabilities.

CSE protects computer networks and electronic information of importance to the Government of Canada, helping to thwart state-sponsored or criminal cyber threat activity on our systems. In addition, CSE's foreign signals intelligence work supports government decision-making in the fields of national security and foreign policy, providing a better understanding of global events and crises and helping to further Canada's national interests in the world.

As a result, CSE plays an integral role in helping to protect Canada and Canadians against foreign-based terrorism, foreign espionage, cyber threat activity, kidnappings of Canadians abroad, attacks on our embassies, and other serious threats with a significant foreign element, helping to ensure our nation's security, stability, and prosperity.

EXECUTIVE SUMMARY

The recent cyber threat activity against the **democratic process** in the United States and Europe has raised concerns about similar threats to Canada. In this assessment, we consider the **cyber threats** to Canada's democratic process at the federal, provincial/territorial, and municipal levels of government. We restrict our analysis of the democratic process to three important aspects that adversaries can target: elections, political parties and politicians, and the media.

To better understand the threat environment, CSE examined cyber threat activity against democratic processes both in Canada and around the world over the past ten years. In this assessment, we review cyber capabilities and how adversaries use these capabilities in sophisticated ways to influence a democratic process. We provide our assessment of cyber threat activity targeting democratic processes – both around the world and in Canada – and what we expect to see against the 2019 federal election, political parties and politicians, and the media relevant to the election.

KEY JUDGEMENTS

- Cyber threat activity against the democratic process is increasing around the world, and Canada is not immune. In 2015, during the federal election, Canada's democratic process was targeted by low-sophistication cyber threat activity.[1] It is highly probable that the perpetrators were hacktivists and cybercriminals, and the details of the most impactful incidents were reported on by several Canadian media organizations.[2]
- A small number of nation-states have undertaken the majority of the cyber activity against democratic processes worldwide, and we judge that, almost certainly, they are the most capable adversaries.
- However, to date, we have not observed nation-states using cyber capabilities with the purpose of influencing the democratic process in Canada during an election. We assess that whether this remains the case in 2019 will depend on how Canada's nation-state adversaries perceive Canada's foreign and domestic policies, and on the spectrum of policies espoused by Canadian federal candidates in 2019.
- We expect that multiple hacktivist groups will very likely deploy cyber capabilities in an attempt to influence the democratic process during the 2019 federal election. We anticipate that much of this activity will be low-sophistication, though we expect that some influence activities will be well-planned and target more than one aspect of the democratic process.
- Regarding Canada's democratic process at the federal level, we assess that, almost certainly, political parties and politicians, and the media are more vulnerable to cyber threats and related influence operations than the election activities themselves. This is because federal elections are largely paper-based and Elections Canada has a number of legal, procedural, and information technology measures in place.
- We assess that the threat to Canada's democratic process at the sub-national level (i.e. provincial/territorial and municipal) is very likely to remain at its current low level. However, some of Canada's sub-national political parties and politicians, electoral activities, and media are likely to come under increasing threat from nation-states and hacktivists.

- Over the past five years, there has been an upward trend in the amount of cyber threat activity against democratic processes globally. So far, in 2017, 13 percent of countries holding federal elections have had their democratic process targeted.
- Adversaries worldwide use cyber capabilities to target all three aspects of the democratic process (i.e. elections, political parties and politicians, and traditional and social media).
    - Against **elections**, adversaries use cyber capabilities to suppress voter turnout, tamper with election results, and steal voter information.
    - Against **political parties and politicians**, adversaries use cyber capabilities to conduct cyberespionage for the purposes of coercion and manipulation, and to publicly discredit individuals.
    - Against both **traditional and social media**, adversaries use cyber capabilities to spread disinformation and propaganda, and to shape the opinions of voters.
- We judge that it is highly probable that cyber threat activity against democratic processes worldwide will increase in quantity and sophistication over the next year, and perhaps beyond that. The reasons for this include:
    - Many effective cyber capabilities are publicly available, cheap, and easy to use.
    - The rapid growth of social media, along with the decline in longstanding authoritative sources of information, makes it easier for adversaries to use cyber capabilities and other methods to inject disinformation and propaganda into the media and influence voters.
    - Election agencies are, increasingly, using the Internet to improve services for voters. As these services move online, they become more vulnerable to cyber threats.
    - Deterring cyber threat activity is challenging because it is often difficult to detect, attribute, and respond to in a timely manner. As a result, the cost/benefit equation tends to favour those who use cyber capabilities rather than those who defend against their use.
    - Finally, there is a dynamic of success emboldening adversaries to repeat their activity, and to inspire copycat behaviour.

TABLE OF CONTENTS

ABOUT THIS DOCUMENT

In response to a request from the Minister of Democratic Institutions, this report includes a threat assessment by the Communications Security Establishment (CSE) on **cyber threats** to Canada's democratic process.

ASSESSMENT PROCESS

The goal of intelligence analysis is to provide readers with intellectually rigorous, objective, and timely products. CSE's cyber threat assessments are based on an analysis process that includes evaluation of the quality of available information, exploration of alternative explanations, mitigation of biases, and application of probabilistic approaches.

In this assessment, we distinguish between fact, assumptions, and conclusions. We use the words "we assess" or "we judge" to convey an analytic assessment or judgement made by CSE. We also use words such as "possibly", "likely", and "very likely" to convey probability (see Annex A).

SOURCES

Many of the key judgements in this assessment rely on a body of reporting from multiple sources and are based on CSE's knowledge and expertise in foreign intelligence and cybersecurity. However, this is an unclassified document and we cannot divulge classified intelligence, which would jeopardize sources and methods of intelligence collection. CSE cannot publicly reveal the full extent of our knowledge or the complete basis for our judgements.

SCOPE

This document discusses a wide range of cyber threats to Canadian political and electoral activities at the federal, provincial/territorial, and municipal levels.[3] Given the scope of the assessment, we do not look at the particular risks to and vulnerabilities of all elections, political parties and politicians, and media in Canada. Nor do we provide an exhaustive list of cyber capabilities, or the way that adversaries could deploy them, as the activities of Canada's cyber adversaries would take chapters to catalogue.[4]

As well, providing cyber threat mitigation advice is beyond the scope of this assessment. In a general sense, many of the cyber threats that we discuss throughout the assessment can be mitigated through cybersecurity (e.g. measures found in CSE's Top 10 IT Security Actions), physical security, and business-continuity best practices.

This threat assessment is based on information available as of 7 June 2017.

INTRODUCTION

The recent cyber threat activity against political institutions and personal communications of politicians around the world has raised concerns about the cybersecurity of the democratic process in Canada. In this document we assess the cyber threats facing Canada's democratic process.

To better understand the threat environment, CSE examined cyber threat activity against democratic processes, both in Canada and around the world, over the past ten years. We identify how key aspects of the democratic process (i.e. elections, political parties and politicians, and the media) are vulnerable to cyber threat activity and influence operations. We consider the democratic process at the federal, provincial/territorial, and municipal levels of government in Canada. We introduce some common cyber capabilities and how Canada's adversaries could use these capabilities to influence the democratic process. We then describe the different types of adversaries that could use these cyber capabilities and what the threat is to Canada.

Finally, by combining our knowledge of recent history and our understanding of current trends in cyber capabilities and Canada's adversaries, we assess how the cyber threats to Canada's democratic process are likely to evolve.

CANADA'S DEMOCRATIC PROCESS

In this assessment we restrict our analysis of the democratic process to three key aspects that adversaries can target: (1) elections; (2) political parties and politicians; and (3) the media (see Figure 1).

Elections are at the core of any democracy. They are the way that citizens select their representatives and their government. For an orderly and peaceful transition of power to take place, citizens must trust that the outcome of an election is valid and free from interference. This is why democratic elections must be carried out in a transparent way, in which observers can verify every step of the process.

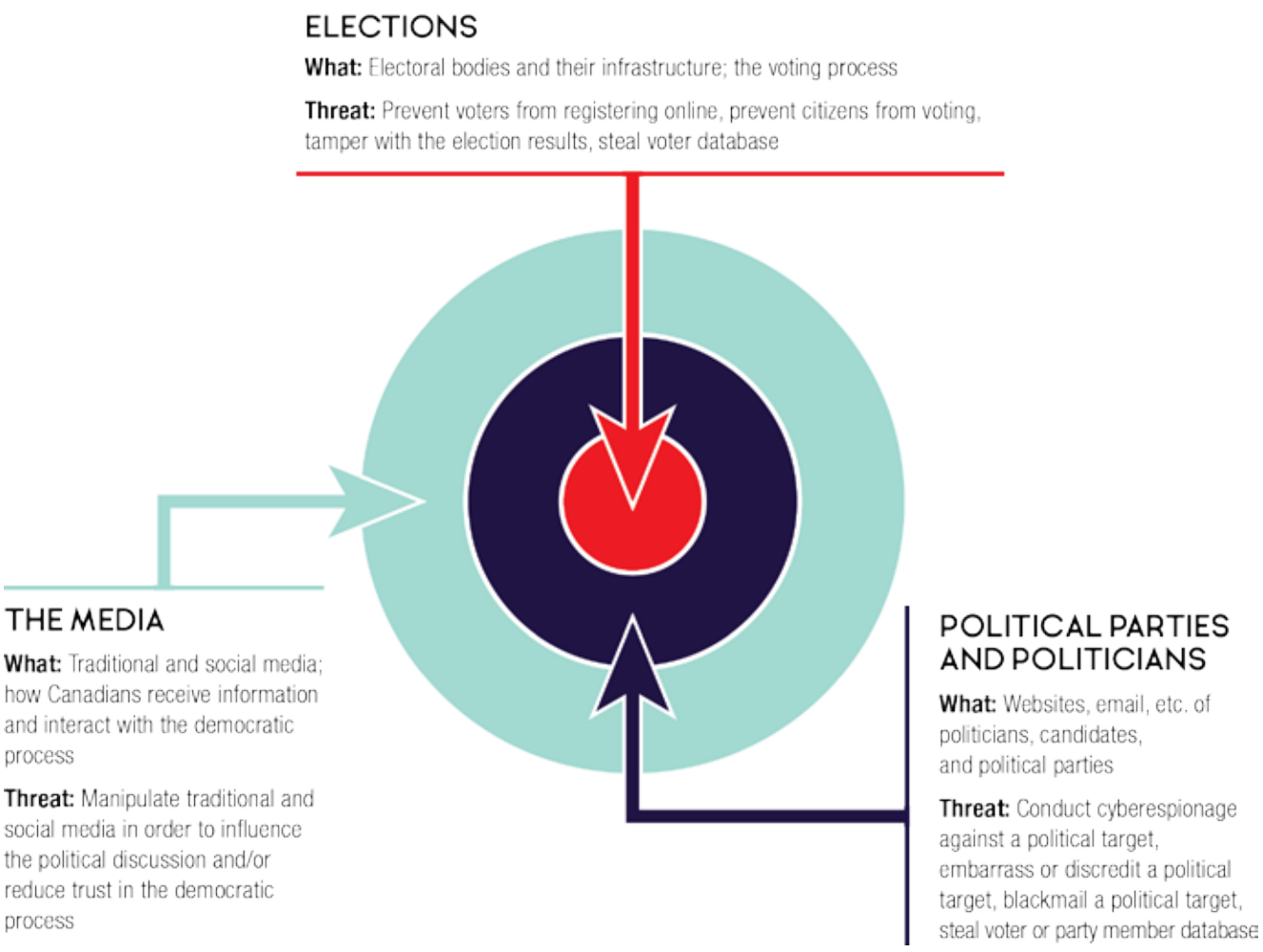
Political parties and politicians are the political institutions and individuals competing for power in an election. They represent the interests of voters and seek to generate support for domestic and foreign policies which they believe are in the best interest of Canadians.

The **media** is where discourse between politicians and voters most often occurs. By media we mean both traditional media (e.g. newspapers and television news networks) and social media.

These three aspects of the democratic process are so important that they are protected by Canada's constitution. The *Canadian Charter of Rights and Freedoms* guarantees Canadians the right to select their members of parliament in a free and fair election. The *Charter* also protects Canadians' right to freedom of expression and belief – including allowing citizens to freely engage, challenge, and propagate ideas in public. The *Charter* also specifically protects the freedom of the press.

Trust is at the core of all aspects of the democratic process. For democracy to work, citizens need to trust that the process is fair, that politicians are not beholden to foreign or criminal interests, and that the media is not influenced by foreign or criminal interests attempting to sway voters and the outcome of the democratic process.

FIGURE 1: Canada's democratic process



OVERVIEW OF CYBER THREATS

The Internet age has ushered in new threats to the democratic process. Most social discourse related to the democratic process now occurs online. This includes email, tweets, websites, databases, computer networks, and many other information technologies used by voters, electoral bodies, political parties and politicians, and the media. Canada is among a large and growing group of states that must defend against adversaries using cyber capabilities to covertly influence all three aspects of the democratic process.

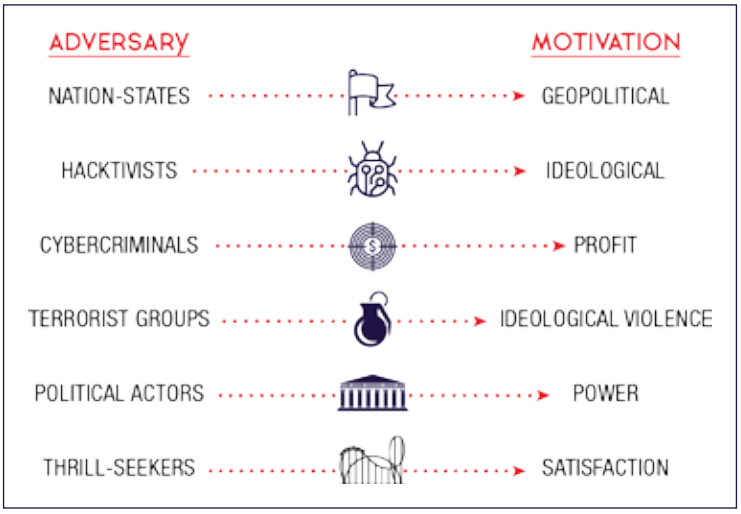
Adversaries are any states, groups, or individuals who have used or might use cyber capabilities to threaten or influence Canada's democratic process. Some adversaries intentionally set out to covertly influence a democratic process: these are **strategic threats**.

Other adversaries do not set out to influence the outcome of a democratic process, although this might occur as an unintended consequence: these are **incidental threats**. Those responsible for incidental threats are often simply casting a wide net, hoping to exploit an insecure network or database to earn some money or for the thrill of it. That their activities could affect the democratic process is simply coincidental.

To assess the cyber threats to the democratic process, CSE examined cyber threat activity against democratic processes worldwide over the past ten years. There are six types of adversaries that have undertaken activities to influence the democratic process, or have the capability to do so.

- **Nation-states** are motivated by economic, ideological, and/or geopolitical interests.
- **Hacktivists** are motivated by ideological issues.
- **Cybercriminals** are motivated by financial profit.[5]
- **Terrorist groups** are motivated by violent extremist ideologies.
- **Political actors** are motivated by winning political power domestically.
- **Thrill-seekers** are individuals seeking reputational or personal satisfaction from successful hacking.

FIGURE 2: At a glance: Adversaries targeting Canada



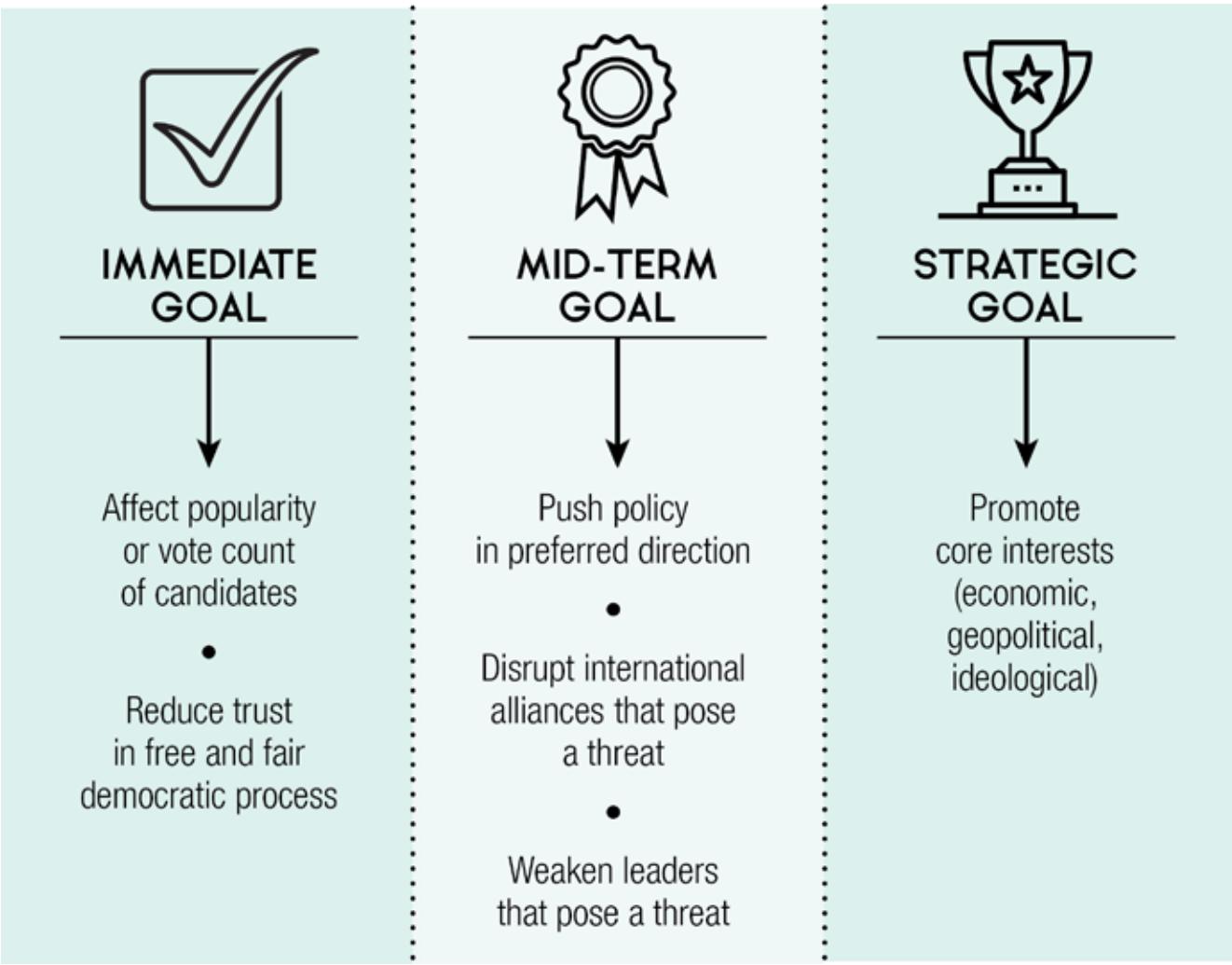
WHY TARGET CANADA'S DEMOCRATIC PROCESS?

Canada is a G7 country, a NATO member, and an influential member of the international community. As a result, the choices that the Canadian federal government makes about military deployments, trade and investment agreements, diplomatic statements, foreign aid, or immigration are influential and impactful. They can affect the decisions taken by Canada's allies, and the core interests of other countries, foreign groups, and individuals. Canada's governments at the provincial/territorial and municipal levels also create policies, direct spending, and make laws that affect tens of millions of Canadians, and in some cases (e.g. regarding resource extraction) affect foreign interests as well.

Adversaries that may target the democratic process for strategic purposes, whether at the federal, provincial/territorial, or municipal level, are attempting to further their core interests, which typically consist of national security, economic prosperity, and ideological goals. Cyber threats can also be used as a show of force to deter other nation-states.

Adversaries may seek to change Canadian election outcomes, policymakers' choices, governmental relationships with foreign and domestic partners, and Canada's reputation around the world. They may also try to delegitimize the concept of democracy and other values such as human rights and liberty, which may run contrary to their own ideological views of the world.

FIGURE 3: Why do nation-states use cyber capabilities to influence democratic processes of foreign countries?

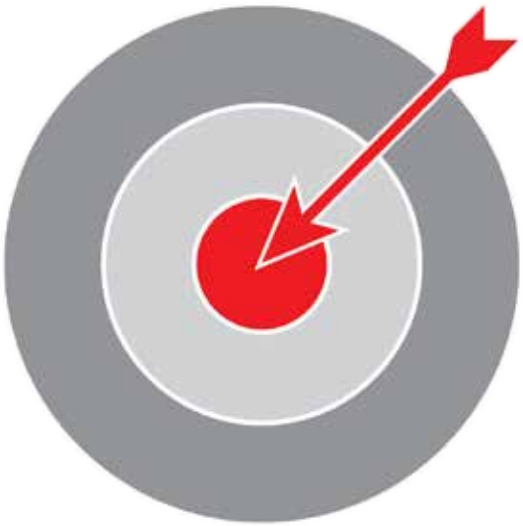


HOW THE DEMOCRATIC PROCESS IS TARGETED

This section details three key aspects of Canada's democratic process and how each is vulnerable to cyber threats.

TARGET: ELECTIONS

- **Key threat:** Prevent citizens from registering
- **Key threat:** Prevent voters from voting
- **Key threat:** Tamper with the election results
- **Key threat:** Steal voter database



Federal, provincial/territorial, and municipal election agencies carry out elections across Canada. While the activities of these agencies will vary, every election involves these essential phases:

1. **Registering voters:** Determining who is eligible to vote;
2. **Voting:** Receiving, counting, and recording the votes; and
3. **Disseminating results:** Informing the public of the election results.

Decades ago, elections were entirely paper-based. Today, as Figure 4 shows, there is a variety of both paper-based and electronic systems used to carry out elections in Canada. While we cannot consider the specifics of every electoral jurisdiction in Canada, what follows below is a general description of the three election phases and the ways in which they may be vulnerable to cyber threats.

FIGURE 4: Target: Elections

GOVERNMENT LEVEL	VOTER REGISTRY	VOTE	VOTE COUNT	DISSEMINATE RESULTS[6]
Federal				
Provincial/ Territorial	[1]		[2]	
Municipal	[3]	[4]	[5]	

LEGEND

Paper	Digital	Internet
Process is conducted using paper	Process uses electronic devices that are not regularly connected to the Internet (e.g. to scan paper ballots or to store information digitally)	Process is conducted on the Internet (e.g. online voting)

1: Online voter registration is available for Alberta, British Columbia, Northwest Territories, Prince Edward Island, and Saskatchewan.
2: New Brunswick only.
3: Some municipalities across Canada offer online voter registration.
4: Some municipalities in Nova Scotia (36%) and Ontario (22%) use Internet voting.
5: Some municipalities use machines to count paper ballots; for those that use Internet voting, the count is also online.
6: Unofficial results are provided on election night. In most cases, election results are certified (i.e. offical results) days or weeks following election night.

REGISTERING VOTERS

For every election, there is a process that determines the eligibility of voters. Only those voters meeting particular criteria (e.g. minimum age and/or residency requirements) are allowed to vote. In Canada, all levels of government maintain and update voter registration lists.[6]

If voter registration occurs online, adversaries could use cyber capabilities to pollute the database with fake voter records. They could also render the website inaccessible or have it display misleading information. Moreover, they could attempt to erase or encrypt the data and thereby make it unavailable.

All of this activity has the potential to embarrass the electoral agency and sow doubt in the minds of voters. It could also slow down voting, leading to voter frustration and/or suppression, which could impact election results. It is also possible that the voter database – potentially containing millions of personal identity records – could be stolen, resulting in a massive breach of privacy.

ARIZONA & ILLINOIS VOTER REGISTRY (2016)

In June 2016, the US state of Arizona shut down its voter registration system for nearly a week after adversaries attempted to gain access to the system. The next month, in Illinois, the state election agency took down its website for two weeks after discovering tens of thousands of voter records (e.g. names, addresses, and driver's licence numbers) were suspected to have been viewed by the adversaries.[8]

VOTING

Voting is the process by which an eligible voter casts a ballot for a candidate. Most voting occurs on Election Day but also on advance poll dates and via absentee ballots. In Canada, voters cast their votes via three main methods: paper ballot, electronic voting machine, or the Internet.[7] After the polls close, the votes are counted and the results are tabulated. Paper ballots can be counted by hand or by using a digital vote tabulation machine. Internet votes are also tabulated digitally.

Neither digital vote tabulation nor electronic voting machines are typically connected to the Internet, but sophisticated adversaries could tamper with these machines prior to their use. For example, an adversary could cause them to improperly count ballots, or wipe all data at the end of the night. Internet voting presents many more opportunities to adversaries, who can use cyber capabilities, for example, to "stuff the ballot box" or to render the voting website inaccessible.

COVERTLY CHANGING THE VOTE COUNT?

While there is a risk that cyber capabilities could be used to covertly change the vote count and lead to a different election winner, we assess that this would be very challenging for an adversary to accomplish *if* elections were conducted in a manner that includes cybersecurity best practices and paper processes that occur in parallel.[9] In general, it is likelier that adversaries would use cyber capabilities to disrupt the voting process in order to sow doubt among voters about the fairness of the election.

DISSEMINATING RESULTS

In most elections, there is more than one polling place. After the polls close, and counting at the polling stations is finished, the count totals from each polling station must be transmitted to a centralized location. In many elections, the election authority provides frequent updates of the tallies to the public via a website. The same results may be sent directly to the media. Transmitting this vote count can be done by hand, by phone, and/or by Internet. If done using the Internet, adversaries could use cyber capabilities to disrupt or change the vote results while they are in transmission.

If this tampering were discovered, and if there were robust safeguards in place (e.g. paper ballots that can be recounted), the correct results could eventually emerge. However, the delay and confusion would likely reduce the public's trust in the process and perhaps impact the winner's ability to govern. In the worst case, it could even lead to challenging the results of the election, sparking a democratic challenge.

THE NETHERLANDS (2017)

Responding to perceived software vulnerabilities in its vote tabulation machines and warnings that the election may be targeted by Russia, the Netherlands amended voting procedures in their most recent election. To avoid the possibility of adversaries interfering with the election, all votes were hand-counted.[11]

If this tampering were not discovered, then the vote count would be covertly changed to select one candidate (or party) over another. Covertly changing election results using cyber capabilities is difficult, but not impossible, for an elite handful of adversaries. An adversary's decision to try – as well as the odds of success – would depend on the safeguards and risk mitigation activities incorporated into the election system.

GHANA (2016)

In December 2016, adversaries gained access to the website of Ghana's Central Election Commission during the general election as the votes were being counted. An unknown adversary tweeted fake results that the incumbent candidate had lost. The electoral commission then sent out its own tweets claiming these results to be false. While the outcome of the election was not altered, this incident served to sow confusion in the minds of many voters.[10]

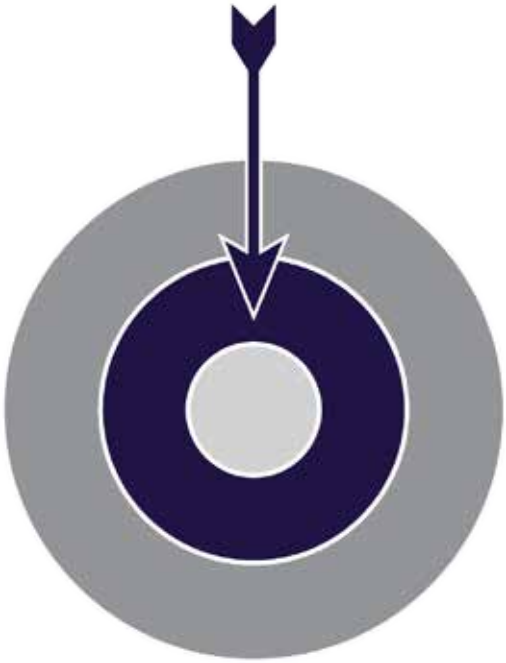
MANAGING CYBER THREATS TO CANADA'S FEDERAL ELECTIONS

Federal elections are largely paper-based and Elections Canada has a number of legal, procedural, and information technology measures in place, which mitigate cyber threats. We assess that it is nearly certain that, regarding Canada's democratic process at the *federal* level, political parties and politicians, and the media are more vulnerable than the elections themselves.

TARGET: POLITICAL PARTIES AND POLITICIANS

- **Key threat:** Conduct cyberespionage against a political target
- **Key threat:** Blackmail a political target
- **Key threat:** Embarrass or discredit a political target
- **Key threat:** Steal or manipulate voter or party database

During the electoral process, voters are judging and assessing political parties and politicians as they decide who will get their vote. Political parties and politicians try to persuade voters using specific messages and ideas. Adversaries may try to obtain damaging information to gain control over individuals and/or sway public opinion against them.



CONDUCT CYBERESPIONAGE

Political parties and politicians use smartphones, devices, and computers to handle and store personal and political information. This can include databases with detailed personal information about millions of Canadians, both registered voters and political donors. Political parties are authorized to receive parts of the voter registry from election bodies, and they may supplement this with more detailed information about voters. Personal and political information is valuable, enticing adversaries to use cyberespionage to gain access.[12]

BLACKMAIL OR MANIPULATE A TARGET: USE INFORMATION OR THREATEN TO RELEASE INFORMATION

Adversaries may choose to use private information about a politician (or political staff) to try to manipulate or coerce the individual. This type of activity could involve blackmail, bribery, or orchestrating situations to attempt to push the target into behaviours or activities that would otherwise not occur.

UNITED STATES (2016)

In the last US presidential election, both major political parties were subjected to cyberespionage attempts by Russia. Russian operatives used cyber capabilities to gain access to the emails of key political staff working on the Democratic Party campaign. The emails were subsequently leaked to embarrass the Democratic Party candidate.[13]

EMBARRASS OR DISCREDIT A TARGET: RELEASING INFORMATION

Another way adversaries can target political parties and politicians is by first collecting information (as above), then releasing it to the public for the purpose of embarrassing or discrediting the target. In order to enhance this effect, an adversary may make modifications to the information before releasing it to the public. Adversaries might use a third party (e.g. journalists or WikiLeaks) to try to increase the legitimacy of the information and to keep their identities hidden or less obvious. The purpose of this activity is to embarrass or discredit the target, or to help the target's political rival.

EMBARRASS OR DISCREDIT A TARGET: MEDDLING WITH WEBSITES OR SOCIAL MEDIA

Another way to discredit a political party or politician is to disable or compromise their presence on the Internet. For example, adversaries can target a social media account or a website and deface it with obscene or misleading information, which can fool voters and embarrass the politician. Depending on the timing of such an event, the impact could range from mere nuisance to a major turning point in a close election campaign.

The cyber capabilities required to disable a website are relatively simple to buy or rent, which allows adversaries who do not possess technical abilities to easily and cheaply acquire them to accomplish their goals.

When adversaries try to publicly embarrass or discredit a target, they are doing so with the intent that it will enter the mainstream news cycle, knocking a party "off message", even if only temporarily. The media itself can also be targeted in order to influence the political process and public opinion. This is discussed in the next section.

In the long term, this type of activity can have a chilling effect on democracy. Qualified candidates may decide that running for public office is simply not worth the potential negative effect on their personal life and reputation.

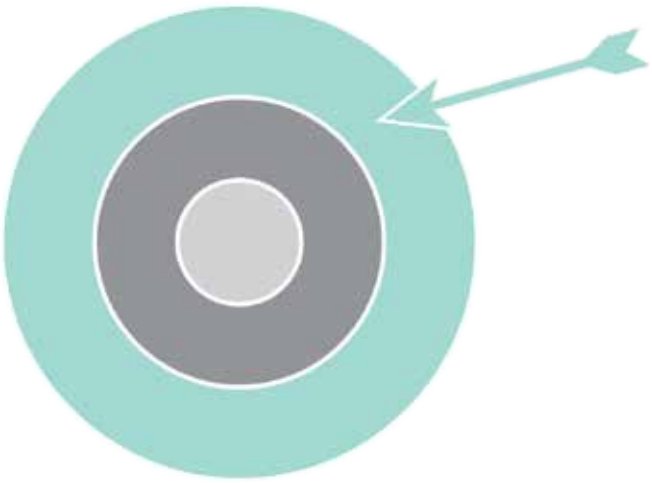
STEAL OR MANIPULATE VOTER OR PARTY DATABASE

Adversaries might steal voter or party databases because they fetch a price on illicit parts of the Internet (i.e. the Darkweb), where large quantities of personal identity information are constantly bought and sold.[14]

Adversaries might also decide to change data, or make it unavailable (e.g. by encrypting it) to political parties and politicians that use the information to identify and communicate with voters. If adversaries targeted a political party with this activity, it could impact the election campaign by denying the party a valuable tool used for voter outreach and engagement.

TARGET: THE MEDIA

- **Key threat:** Covertly manipulate traditional media and social media in order to influence the political discussion and/or reduce trust in the democratic process



Both the right to freedom of expression and freedom of assembly are protected by the *Canadian Charter of Rights and Freedoms*. As in all Western democracies, Canada's media (both traditional media and social media) facilitate the exchange of information and opinions and are where political ideas and movements gain momentum.

Meaningful political participation in Canada's democratic process depends on the public having access to a broad spectrum of information and competing political viewpoints. Nowadays, Canadians mostly get their information online – either through traditional media establishments, social media, or both. It is also online where most Canadians contribute their own views on the political issues of the day.[15]

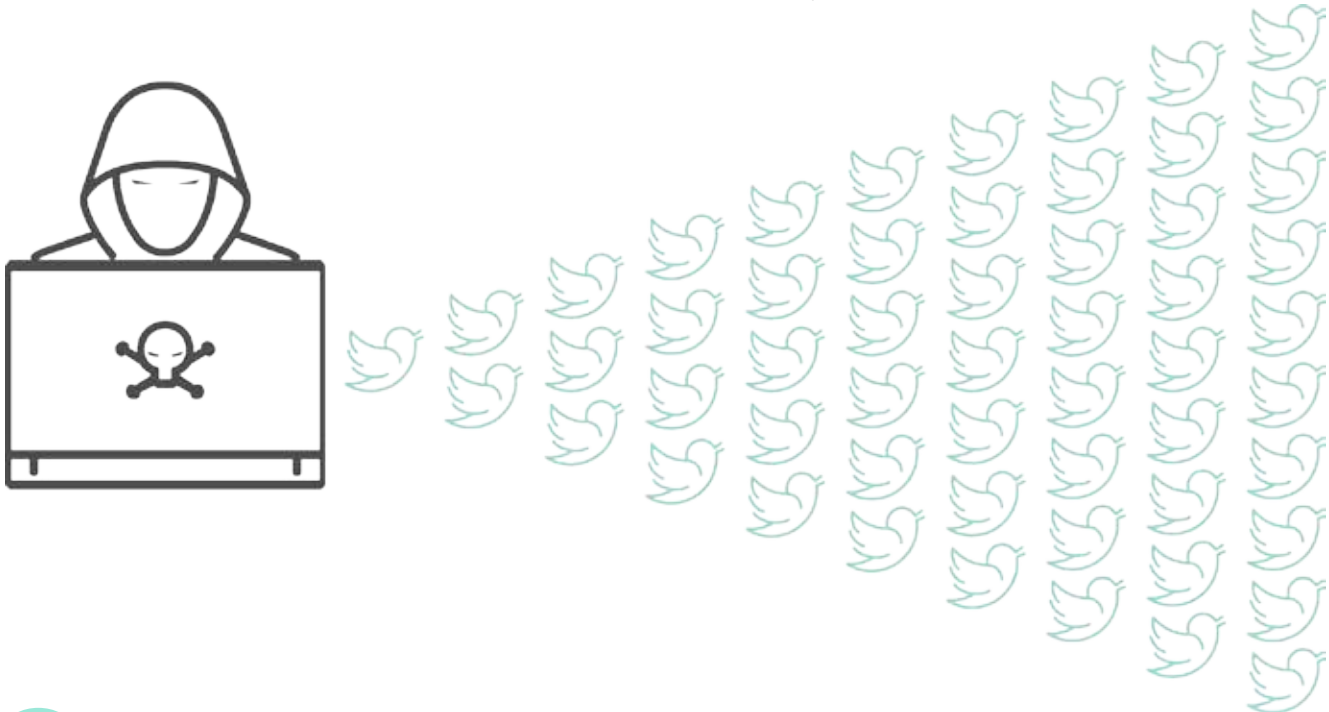
FRANCE (2017)

According to media reports, French intelligence believes that social botnets were used to influence the presidential election. Certain social media accounts, the same ones that were active during last year's US election, were promoting false and defamatory information against a leading candidate. In the final days of the election, one party was also victimized by the unauthorized release of thousands of campaign-related emails.[16]

The concern arises if foreign adversaries use cyber capabilities to try to covertly influence Canada's media environment. Adversaries could achieve this through a thorough understanding of how traditional media and social media work and how Canadians consume information. The existence of foreign influence, or the perception of such, could shape the opinions of voters and reduce the trust that Canadians have in the information they are getting.

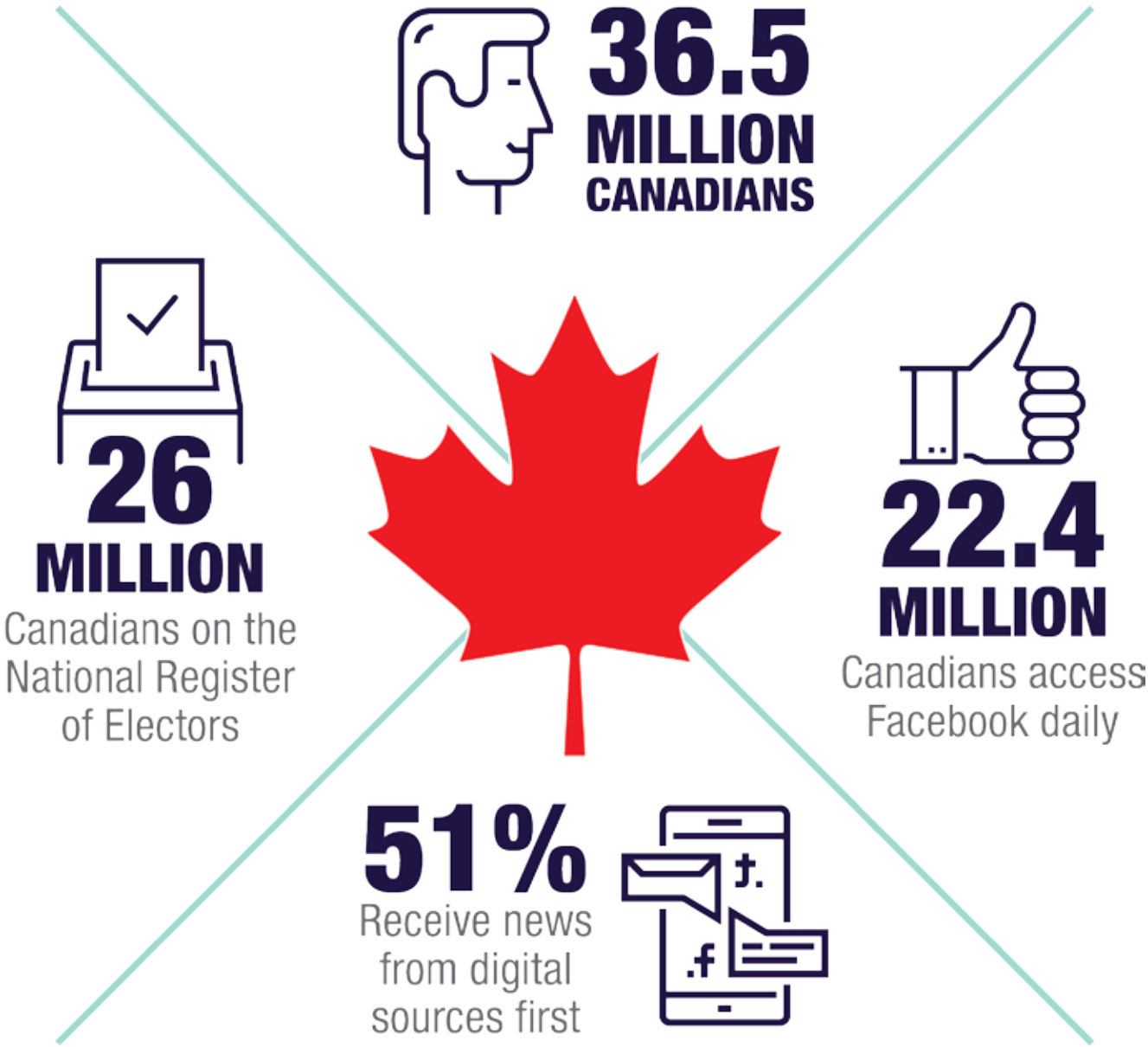
Adversaries could use social media to spread lies and propaganda to a mass audience at a low cost. Adversaries could masquerade as legitimate information providers, blurring the line between what is real and what is disinformation. They could do so by hijacking social media accounts, or they could create websites or new social media accounts that purport to be trustworthy producers or disseminators of news and information.

FIGURE 5: Social media botnet amplification



Some adversaries will use "troll farms" – groups of people who are paid to spread propaganda on comment sections of traditional media websites, as well as Twitter, Facebook, and anywhere else they can reach their audience. In a similar manner, adversaries use social botnets – a series of computers that are all coordinated by one user. As shown in Figure 5, a single individual can harness hundreds or even thousands of accounts in order to amplify his/her message, artificially giving rise to the appearance of public consensus in support of a particular view.

Adversaries may choose to subject journalists, or anybody they wish to deter, to a broad campaign of harassment and intimidation. If journalists or citizens try to counter the abuse, they may imperil their privacy, finances, or personal safety. This could result in self-censorship, and has a chilling effect on political discourse and investigative activity that runs contrary to the adversary's interests.



EXPLAINING CYBER THREAT ACTIVITY

The following sections discuss cyber capabilities and the manner in which adversaries use cyber capabilities to affect the democratic process.

THE CYBER TOOLBOX

In today's world, so much of what we do, think, and communicate happens online and on our devices (e.g. computers, smartphones, and tablets). As a result, our work, personal information, relationships, memories, knowledge, and passions have become vulnerable to those who can gain illicit or unauthorized access to our devices or online spaces. Like computers and the Internet, cyber capabilities have evolved substantially over the decades. Not only have cyber capabilities become more advanced, they are also much easier to use. In today's world, some of the most technically advanced and powerful cyber capabilities are free or offered as a service, which allows more people and groups to use them.

Cyber capabilities present many challenges to defenders. When deployed against the democratic process, they often blend in with regular Internet activity and, as a result, their use often goes unseen, unattributed, and unpunished. The low risk of negative consequences and low cost provide excellent incentive for adversaries to use them. Adversaries also benefit as more information and more devices are connected to the Internet because they are often done so insecurely.

It is beyond the scope of this assessment to identify all of the cyber capabilities that adversaries could deploy against email, databases, websites, and communications methods used by the media, political parties and politicians, and election agencies across Canada.

Below, we present a number of common and effective cyber capabilities that have been used to influence democratic processes in various countries across the world.

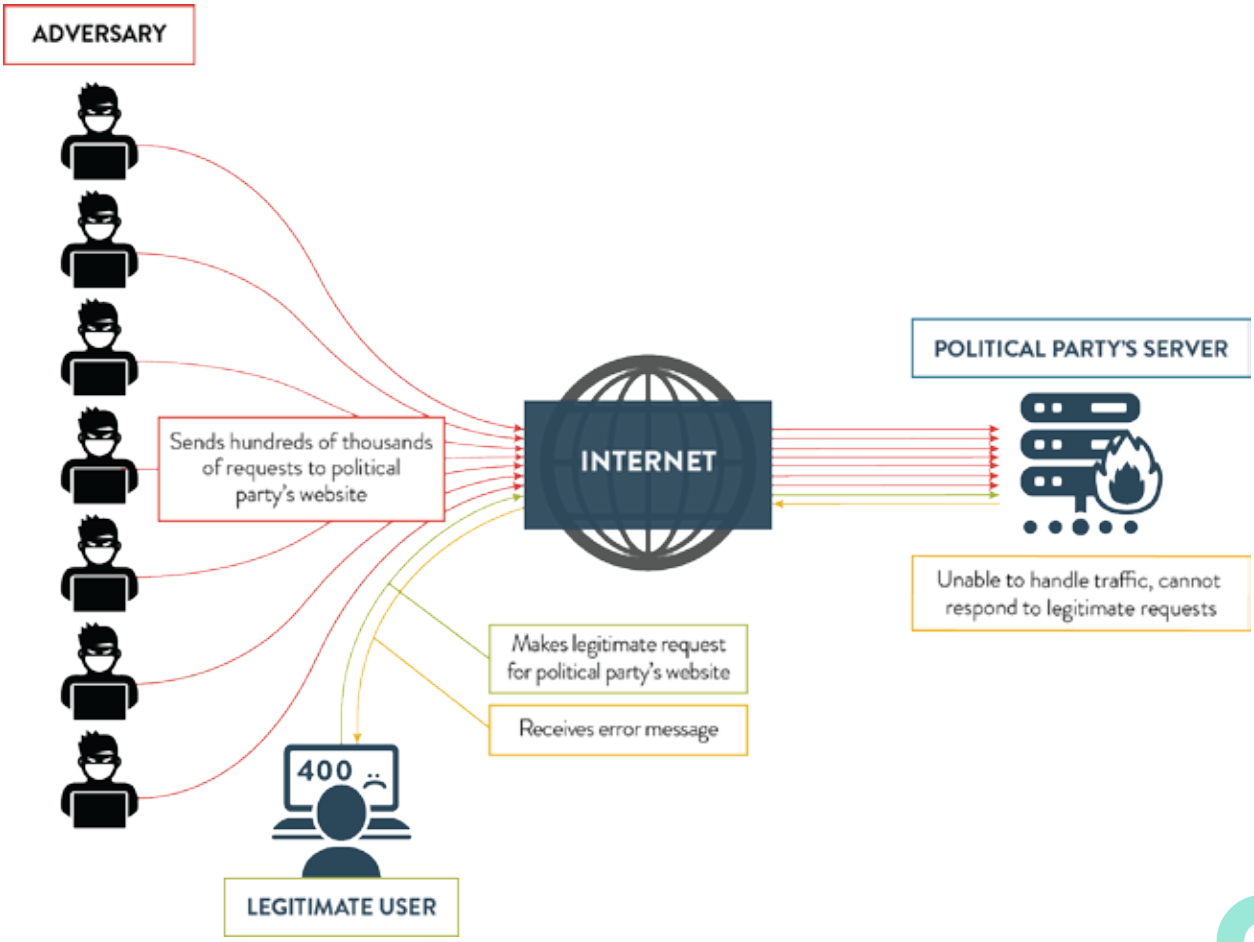
DISTRIBUTED DENIAL OF SERVICE AGAINST A WEBSITE

A distributed denial of service (DDoS) attack temporarily disables a website by flooding it with such high levels of Internet traffic that it is unable to respond to normal requests. This capability can be obtained for free. Alternatively, adversaries can pay others to deploy this tool on their behalf.

For as little as $25, adversaries could launch a DDoS attack that temporarily disables access to a website. The impact of this type of attack depends on the size of the DDoS in relation to the cybersecurity capability of the website host or Internet service provider. We assess that it is likely that many websites related to the democratic process (e.g. politicians' personal websites) would not withstand major DDoS attacks.[17]

To illustrate how a DDoS works, Figure 6 (below) outlines an attack against a political party's website. Such an attack could prevent legitimate users from accessing the website. Depending on the timing, a DDoS against a party's website can cause embarrassment and confusion, particularly if it occurs within days of Election Day.

FIGURE 6: Distributed denial of service



DEFACE A WEBSITE

Defacing a website is akin to digital graffiti. An adversary could change the content of the website with an image or a message designed to embarrass the political party or election agency, or in an attempt to raise awareness of a particular issue.

FIGURE 7: Deface a website

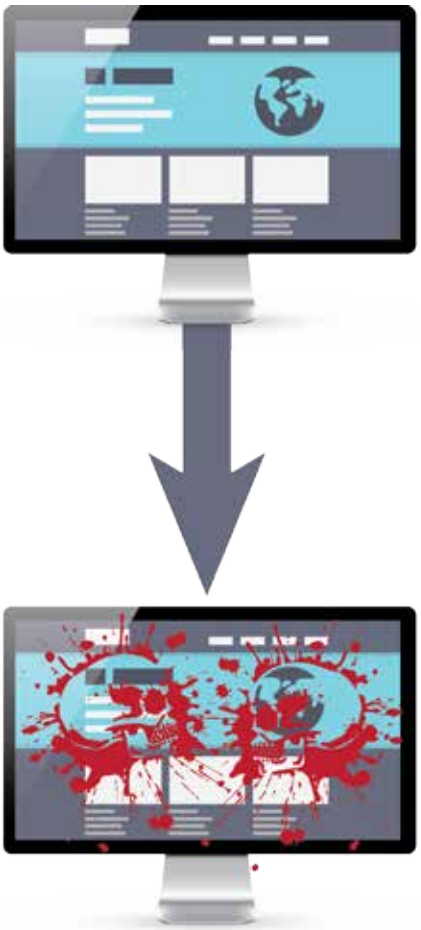
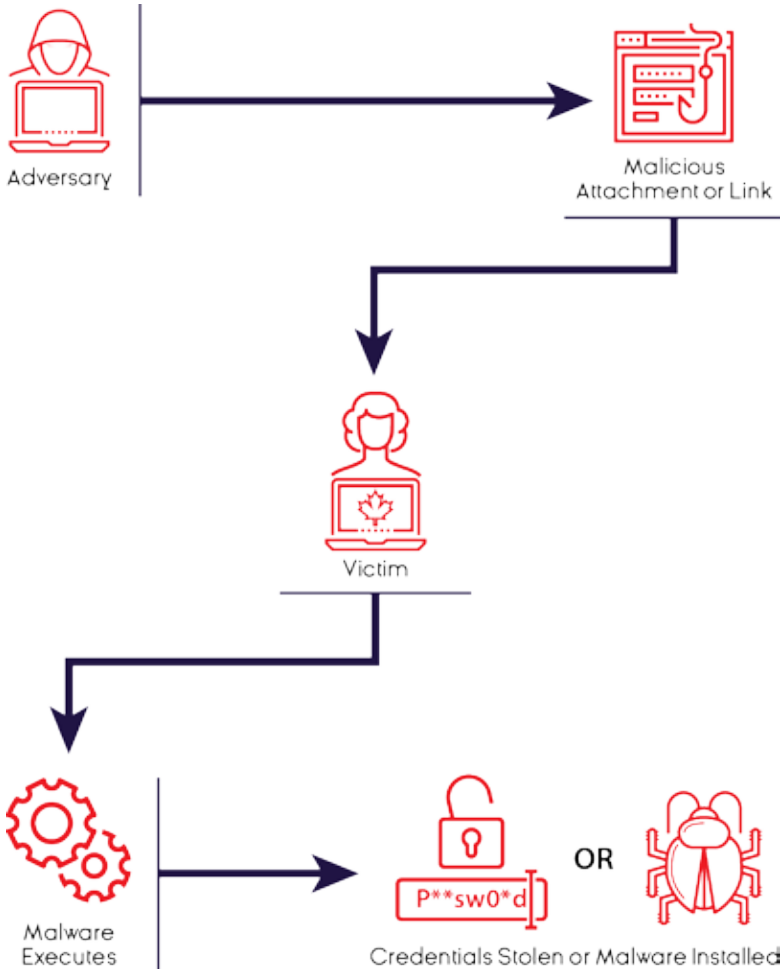


FIGURE 8: Spear-phishing



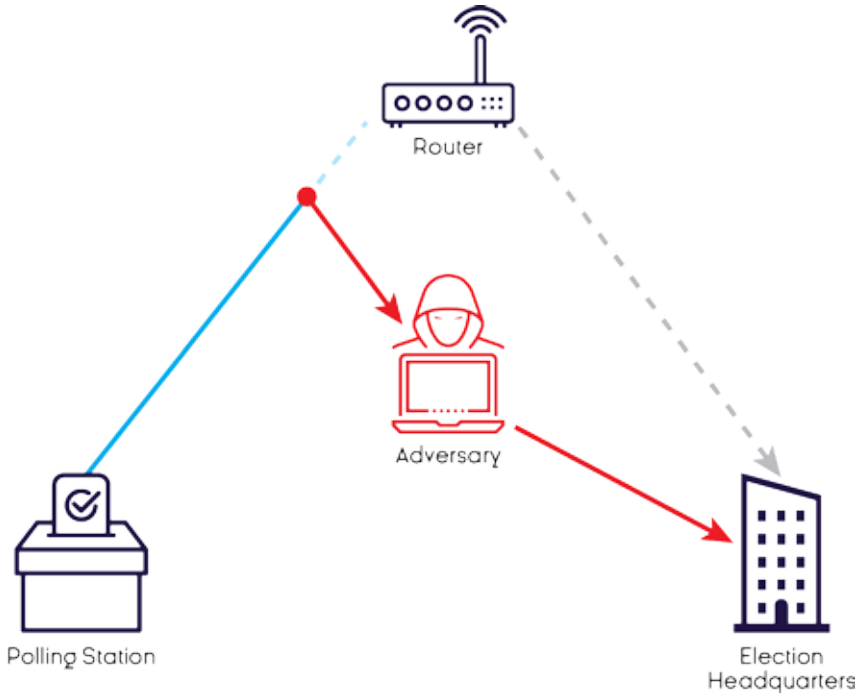
SPEAR-PHISHING

Spear-phishing is a common technique used to gain access to a victim's device, personal information, and credentials (i.e. usernames and passwords). The victim receives a tailored email that appears to be legitimate. After receiving it, the victim is enticed into clicking on a malicious link in the email or opening an attachment that infects the device with malware that gives control of the victim's device or private information to the adversary.[18] Political parties and politicians are often targets of this activity.

REDIRECT (MAN-IN-THE-MIDDLE) ATTACK

A man-in-the-middle attack reroutes a communication between two connections, such as between a polling station and election headquarters, for the purposes of monitoring or altering the information. For example, the vote count transmitted from a polling station could be changed using this cyber capability.

FIGURE 9: Redirect (man-in-the-middle) attack



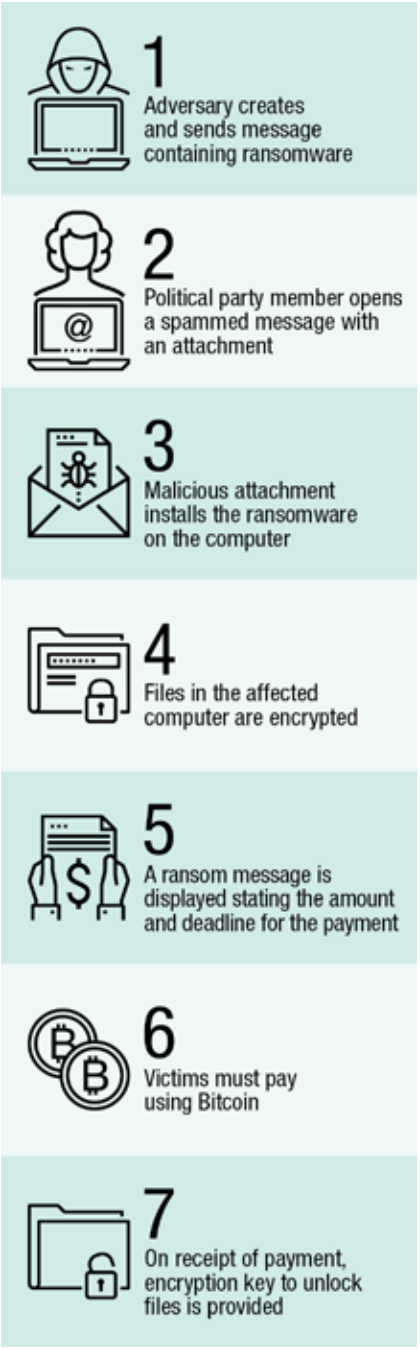
PENNSYLVANIA (2017)

In early 2017, a political party in the US state of Pennsylvania had its computer systems encrypted by ransomware, rendering them unusable.[19]

RANSOMWARE

Ransomware is malware that, once installed, restricts access and compels the victim to pay a ransom in order to regain access to his/her data or device. Ransomware is increasingly common, and victims are often chosen based solely on the vulnerability of their systems, rather than for strategic purposes.

FIGURE 10: Ransomware



CYBER CAPABILITIES: SOPHISTICATED USES

As discussed earlier, cybercriminals and thrill-seekers use cyber capabilities for financial gain or for the thrill of it. We are more concerned with adversaries who use cyber capabilities strategically, with the express intent of covertly influencing the democratic process. As with any type of tool, cyber capabilities can be used in amateurish or sophisticated ways.

When assessing the sophistication of these strategic threats to the democratic process, we consider a combination of three things:

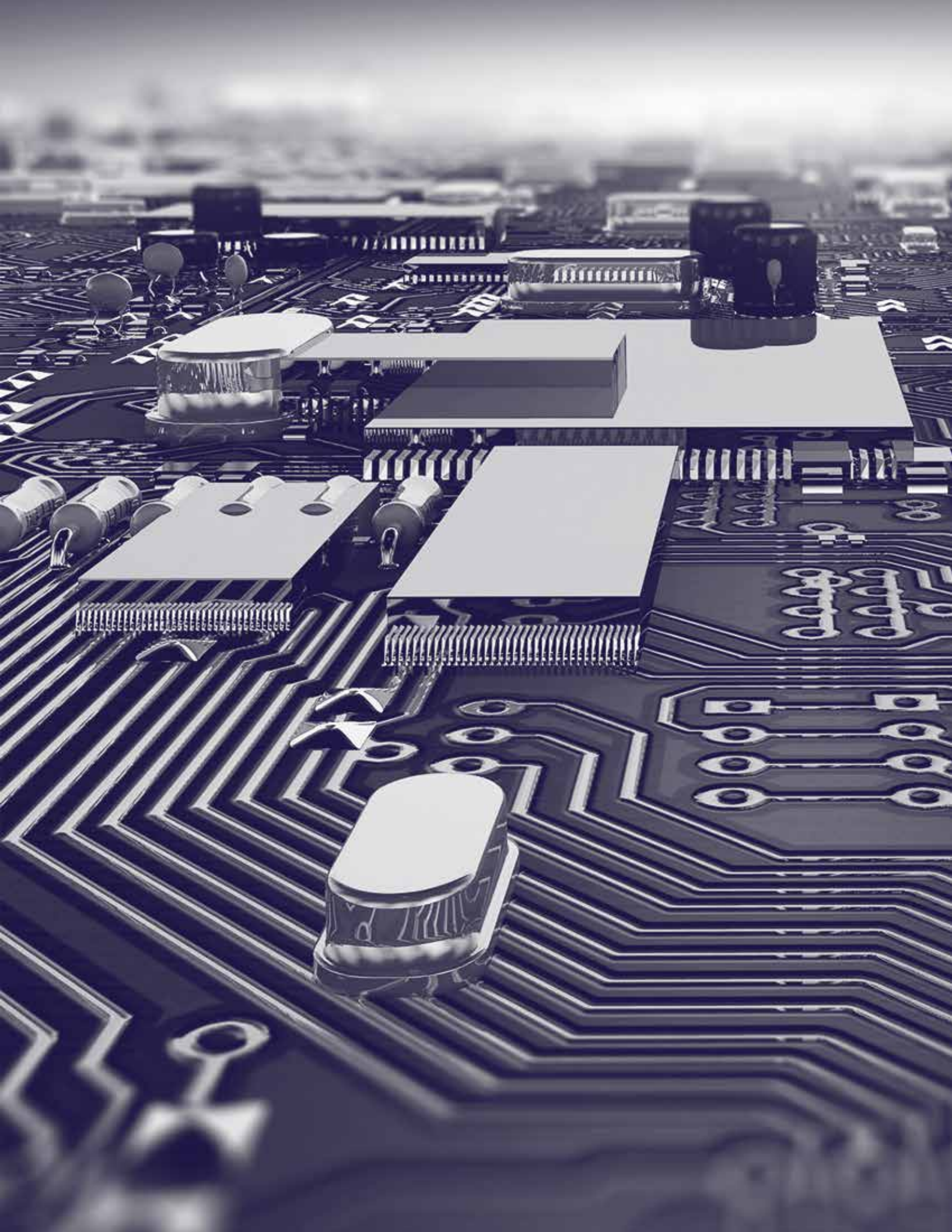
1. **Technical sophistication of the cyber capabilities:** Some cyber capabilities are easily obtained on the Internet and require little skill to deploy. More sophisticated capabilities, however, are custom-designed for a particular set of circumstances (e.g. to gain access to a particular smartphone or computer network) and require much more skill to build and deploy.
2. **Knowledge of Canada's democratic process and how it can be manipulated:** Canada's democratic process includes elections, political parties and politicians, media, and other institutions, ideas, and events that, when taken together, constitute a very complicated and dynamic environment. More sophisticated strategic threat activity reflects an understanding of the environment of a democratic process and how it could be influenced through the use of cyber capabilities.
3. **Ability to orchestrate activities and people:** An individual acting alone is far less likely to influence a democratic process than an adversary that can coordinate a number of activities and groups of people. More sophisticated adversaries make use of organizational and financial capacity, which is often built up over time.

In general, we assume that the more sophisticated the use of cyber capabilities, the more likely it is to influence the outcome of a given democratic process (see Figure 11 below). However, as noted in point two above, a democratic process is a complicated and dynamic environment, and many things besides adversaries influence a democratic process and can account for its outcome. In general, it is very difficult to say whether a given set of adversary activities has influenced the outcome of a given democratic process and to what extent.

FIGURE 11: Description of sophistication

LEVEL OF SOPHISTICATION	SOPHISTICATION CHARACTERISTICS	ADVERSARIES OBSERVED
Low	◉ Uses a single, simple cyber capability ◉ Single target ◉ Little or no planning involved ◉ Likely impact: Nuisance, no lasting effect on anybody	◉ Nation-states, hacktivists, cybercriminals, political actors, thrill-seekers
Medium	◉ A few cyber capabilities used competently ◉ More than one target ◉ Planning required ◉ Likely impact: Multiple people affected, divert time and resources to dealing with activity	◉ Nation-states, hacktivists, political actors
High	◉ Several cyber capabilities used expertly ◉ Numerous targets ◉ Extensive, long-term planning and coordination ◉ Likely impact: Numerous people affected and forced to divert significant time and resources to counter the activity	◉ Nation-states, political actors

To illustrate how adversaries use cyber capabilities strategically to influence the democratic process, we present two **hypothetical** case studies. The first is a description of activities designed to sway public opinion against a political candidate. The second is a description of activities in which cyberespionage is used to obtain campaign strategy documents and personal information to benefit a political rival.



CASE STUDY: SWAYING PUBLIC OPINION AGAINST A CANDIDATE

TARGET: Social media

OBJECTIVE: Reduce popularity of a candidate

Scenario: *In the lead-up to a federal election, an adversary creates a plan to tarnish the reputation of a candidate who espouses policies that are antagonistic to the adversary's own interests. The adversary's plan is to influence voters' opinions by injecting disinformation into social media.*

The result of this influence operation, if successful, is that the candidate loses popularity and potentially the election. The adversary can accomplish this activity by understanding how social media works, and using cyber capabilities that are easy to acquire and to use. While this process can occur in a number of different ways, this case study illustrates the basics of a social media influence operation.

1. **Planning:** In this phase, the adversary surveys the existing media environment and designs a strategy for manipulating the environment to discredit the federal election candidate. The adversary identifies what types of issues are important to the candidate's followers, and what types of stories are likely to be widely covered by the traditional media and widely shared on social media.
2. **Taking action on the Internet:** In this phase, the adversary designs activities based on a comprehensive understanding of how voters' information and opinions are formed and perpetuated in social media. For example, each social media provider uses different algorithms to promote trending content to users. The adversary understands how this works, and manipulates the system in order to introduce ideas and information that are likely to damage the reputation of the candidate.

   Three key ways the adversary manipulates the media is with troll farms, social botnets, and account hijacking. The adversary pays groups of people – troll farms – to spread disinformation and propaganda on the Internet. They post disinformation on websites that resemble reputable news websites, in the comment sections of traditional media websites and on social media.

   The adversary purchases social botnets, which are a series of social media accounts that are all controlled by one user. In this way, one person can control many accounts and inject thousands of messages into political conversations to suppress certain opinions and facts and popularize others.

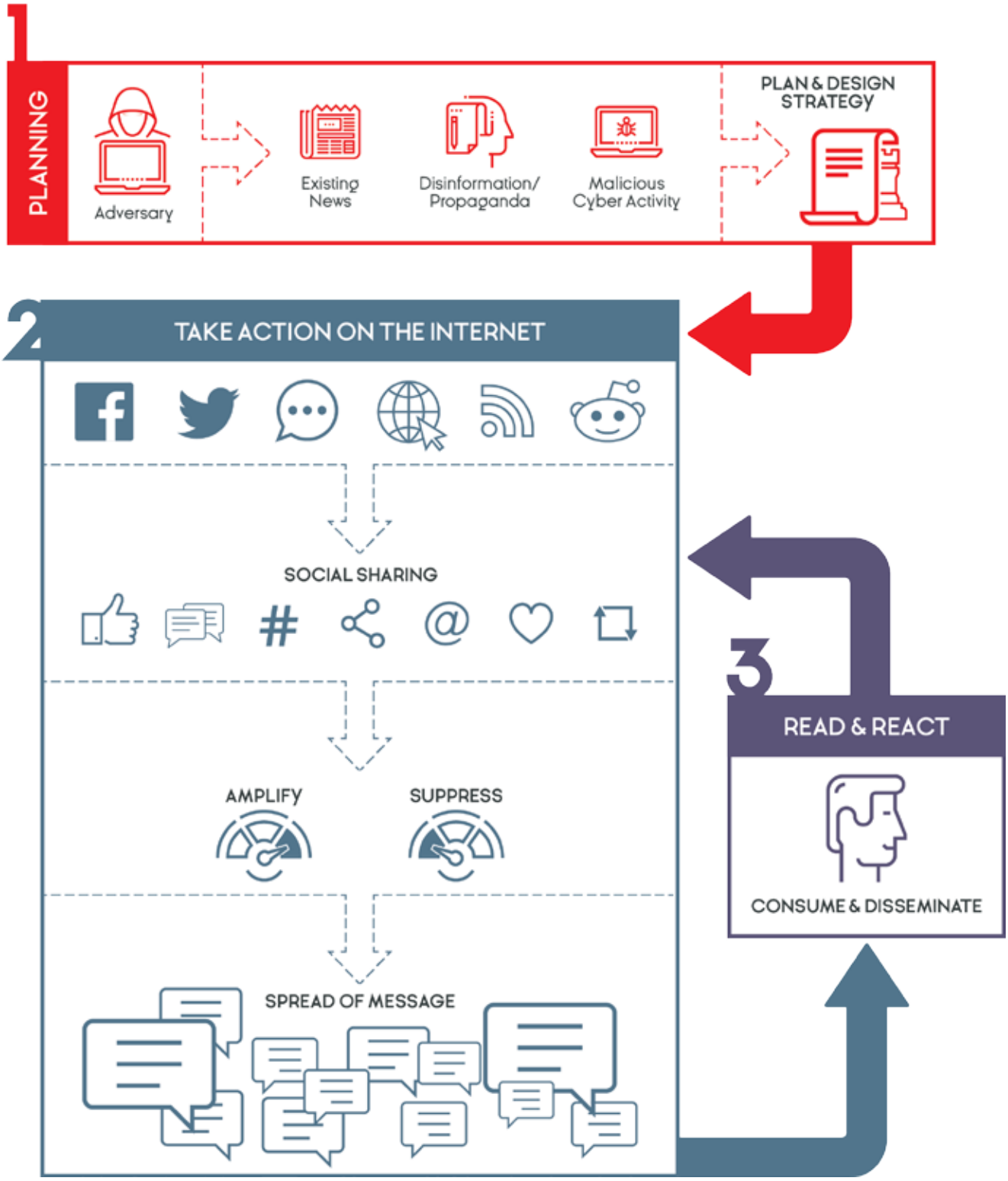
   Account hijacking is a practice whereby the adversary has used cyber capabilities to gain control over the social media accounts of opinion-makers whose followers would be likely to vote for the candidate.

   By harnessing these capabilities toward a particular objective, the adversary is able to insert disinformation and propaganda in social media, amplify messages that discredit the candidate (e.g. trending content), and suppress messages that could be neutral or favourable to the candidate.
3. **Voters read and react:** To voters, there is no evidence of this manipulation taking place and that their personal social media content feed is filled with disinformation and propaganda.

   Voters react to the information they receive, which affects their views of the candidate. Voters also react by sharing and/or commenting on what they see, thereby further spreading the message, helping to accomplish the goal of the adversary.

   A political adversary may also react to this news and use it to his/her benefit, further amplifying the impact of the message.

FIGURE 12: Case study: Cyber-enabled influence operation



CASE STUDY: CYBERESPIONAGE AGAINST A CANDIDATE

TARGET: Mayoral candidate

OBJECTIVE: Obtain campaign strategy and personal information and provide it to his/her rival

Scenario: *In a close-fought municipal campaign, an adversary gains access to the smartphone and then the computer system of a mayoral candidate. Once in the system, the adversary is able to find the candidate's campaign strategy and compromising personal information. The adversary steals this information and provides it anonymously to the candidate's rival, who can use it to help his/her own campaign.*

Beyond open-source research, illegal access to a candidate's email, smartphone, or computer can be very valuable to adversaries. While this process can occur in a number of different ways, this case study illustrates the basics of cyberespionage.

1. **Gain access to the target's smartphone:** The adversary sends a spear-phishing email directly to a candidate (or to someone close to him/her). The purpose here is to entice the target to click on a link or open a file. For example, the subject line of the email could be "draft of speech for your approval" and the link is to a word document file entitled "draft with your changes". The candidate clicks on the link from his/her smartphone. Clicking on the link installs malware.

   Because of the malware, the adversary now has access (via the Internet) to the smartphone, allowing him/her to monitor all text, email, instant messaging, and photos, and even turn on the video and audio recording features of the smartphone, unbeknownst to the victim.

2. **Jump from the smartphone to the laptop (move laterally):** With control of the first device (e.g. a smartphone), the adversary can gain access to other devices, such as laptops and other Internet-connected devices. The adversary may try to move laterally to the devices of the candidate's staff or family members.

3. **Monitor the smartphone and the laptop:** In addition to documents that outline the candidate's campaign strategy, some of the most intimate and private details of a candidate's life are stored electronically, including the candidate's political, financial, health, and romantic history.

4. **Profile and look for exploitable information (analyze):** The adversary profiles the documents, text messages, and audio and video, and finds the campaign strategy and politically sensitive or personally embarrassing information.

5. **Send the information to the rival:** The adversary anonymously contacts the candidate's rival, and sends him/her the potentially helpful information.

   The rival uses the information: The rival gains critical insight and can act on that information, either using it privately or releasing it publicly, to help his/her campaign.

FIGURE 13: Cyber intrusion process

GLOBAL TRENDS AND THE THREAT TO CANADA

GLOBAL BASELINE OF KNOWN EVENTS

CSE has examined dozens of incidents over the past ten years in which adversaries used cyber capabilities to target the democratic process. These incidents victimized almost 40 nations, on five different continents, and include some of the richest – and poorest – nations in the world. Given the covert nature of many of these activities, we assume that there is likely to be a significant number of incidents for which we have no visibility.

Strategic and incidental threats

Over the past ten years, the majority of adversary activity against the democratic process has been strategic (approximately 80 percent). This means that adversaries took action for the express purpose of influencing the democratic process. About three-quarters of this strategic activity have been of medium or high sophistication. The remaining 25 percent mostly involved cybercriminals stealing voter information and was mostly low-sophistication activity.

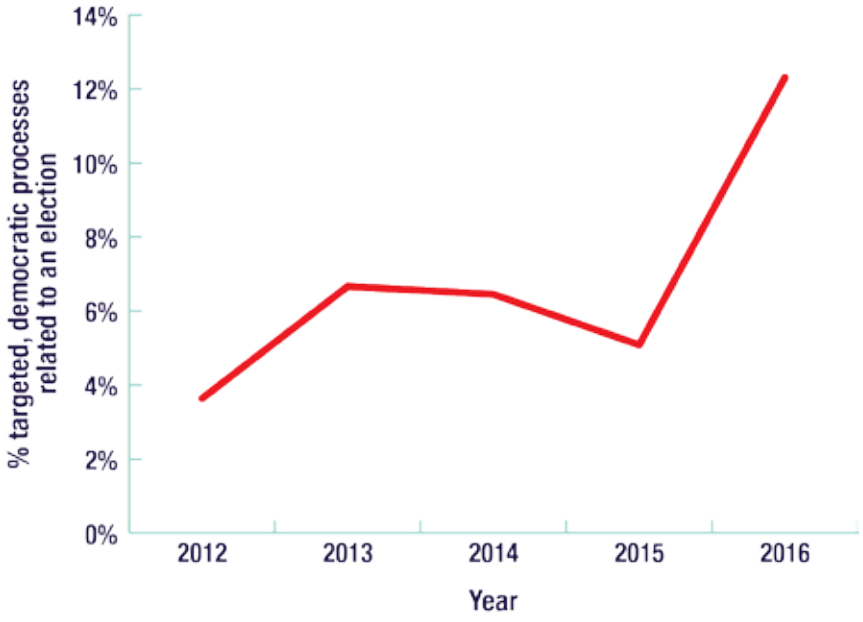
Of the strategic activity observed, 53 percent of the time adversaries targeted more than one aspect of the democratic process. Electoral activities were targeted just over half the time (53 percent), followed by political parties and politicians (47 percent) and media (46 percent). Therefore, all three aspects of the democratic process appear to attract adversaries.

Worryingly, there is an upward trend in the amount of cyber threat activity against democratic processes. So far, in 2017, 13 percent of countries holding national elections have had their democratic process targeted. We judge that it is highly probable that cyber threat activity against democratic processes worldwide will increase in quantity and sophistication over the next year, and perhaps beyond that.

There are a number of factors that contribute to this increase in cyber threat activity.

- Many effective cyber capabilities are **readily available, cheap, and easy to use**.
- **Deterring cyber threat activity** is challenging. We are unable to attribute about 20 percent of incidents to a particular adversary. Of those incidents that are attributed, most appear to have gone unpunished.
- The rapid **growth of social media** coupled with the decline in longstanding authoritative sources of information make it easier for adversaries to use cyber capabilities and other methods to inject disinformation and propaganda into the media to influence voters.
- Elections and election agencies are adopting **more online processes**, making them more vulnerable to cyber threats.
- There is a dynamic of **success emboldening adversaries** to repeat their activity, and to inspire copycat behaviour.

FIGURE 14: Targeting of democratic processes related to a national election, globally



CANADIAN CONTEXT

CYBER THREATS TO CANADA'S DEMOCRATIC PROCESS

Cyber threat activity affecting the democratic process in Canada is a small fraction of the much larger global experience. During the 2015 federal election, Canada's democratic process was targeted by low-sophistication cyber threat activity. It is highly probable that the perpetrators were hacktivists and cybercriminals, and the details of the most impactful incidents were reported on by several Canadian media organizations.[20]

The next federal election in Canada is set to occur in 2019. Setting aside unforeseeable events, we judge that, almost certainly, multiple hacktivist groups will deploy cyber capabilities in an attempt to influence the democratic process in 2019. Hacktivists will likely study the success of past influence operations and adopt more sophisticated and successful activities.

While much of this activity will be low-sophistication, we expect that some influence activities will be well-planned and target more than one aspect of the democratic process, and could almost be characterized as medium-sophistication.

Nation-states have demonstrated the highest sophistication (mostly medium and high, but some low) and a small number of nation-states have undertaken the majority of the cyber activity against democratic processes worldwide. Nation-states also use non-cyber methods (e.g. traditional espionage, manipulation and coercion, or state-sponsored newspapers and television stations) to try to influence the media and political parties and politicians.

Against Canada, nation-states are constantly deploying cyber capabilities to try to gain access to Government of Canada networks and the communications of federal government officials.[21]

Terrorist groups have not demonstrated the intent to use cyber capabilities to influence democratic processes globally or in Canada. However, some groups have demonstrated that they are capable of using cyber capabilities, orchestrating a wide range of activities and manipulating traditional and social media.

To date, we have not observed nation-states using cyber capabilities with the purpose of influencing the Canadian democratic process during an election. We assess that whether this remains the case in 2019 will depend on how nation-state adversaries perceive Canada's foreign and domestic policies over the next two years, and on the spectrum of policies espoused by Canadian federal candidates in 2019.

Outside Canada, corrupt political actors use cyber capabilities to influence their domestic democratic processes, although this represents only 9 percent of observed activity. Given the prevalence of cyber capabilities and the advantages they confer, it is likely that political actors outside Canada will increasingly avail themselves of these capabilities to shape their political fortune. As Canada ranks low in corruption, this type of activity is far more likely to be seen elsewhere.[22]

Looking beyond the federal level, in Canada, CSE has no indication that the democratic process has been targeted in relation to the thousands of elections held at the provincial/territorial or municipal level over the past five years. This is good news.

We assess that the threat to the democratic process in relation to Canada's sub-national elections is very likely to remain at its current low levels. However, the trends we identify above are likely to act as a tailwind, putting some of Canada's provincial/territorial and municipal political parties and politicians, electoral activities, and relevant media under increasing threat.

In particular, we know that certain nation-states have core interests that can be affected by Canadian policies related to natural resources, which are often made at the provincial/territorial level. In addition, Canada has provincial/territorial and municipal leaders that have made policies and statements garnering national and international attention. Hacktivists may begin to view sub-national elections, political parties and politicians, and the media as worthy targets.

CONCLUSION

In this assessment we identified how key aspects of the democratic process (i.e. elections, political parties and politicians, and the media) are vulnerable to cyber threat activity and related influence operations. We described the different types of adversaries that could use these cyber capabilities, and we assessed how the cyber threats to Canada's democratic process are likely to evolve.

In a general sense, many of the cyber threats that we discussed can be mitigated through cybersecurity, physical security, and business-continuity best practices. However, cyber threats and influence operations are often successful because they take advantage of deeply rooted human behaviours and social patterns, and not merely technological vulnerabilities. Defending Canada's democratic process against cyber threats and related influence operations requires addressing both the technical and social elements of the problem.

FURTHER READING

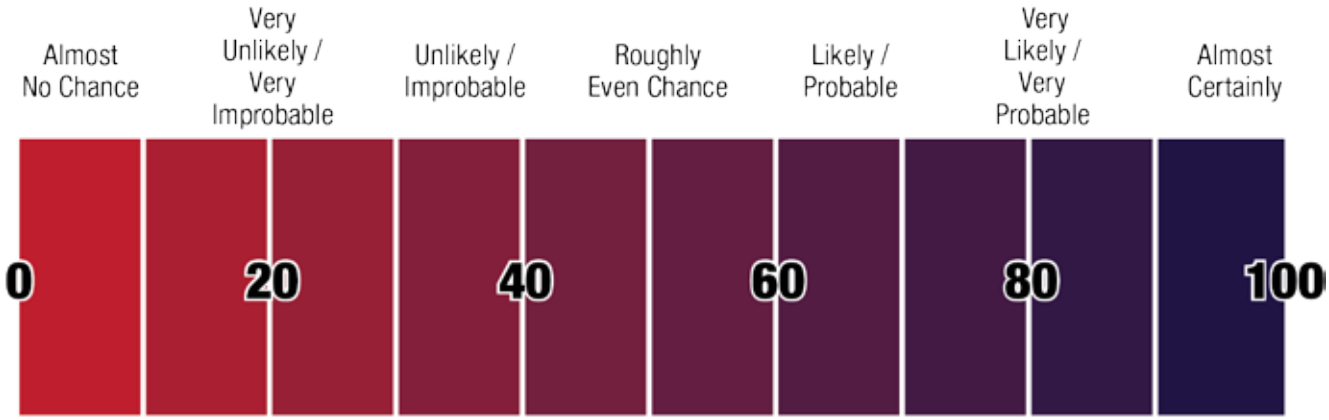
For more information about mitigating cyber threats see:

- CSE's Top 10 IT Security Actions
- CSE's advice on Cyber Hygiene
- CSE's advice on Mobile Security

ANNEX A

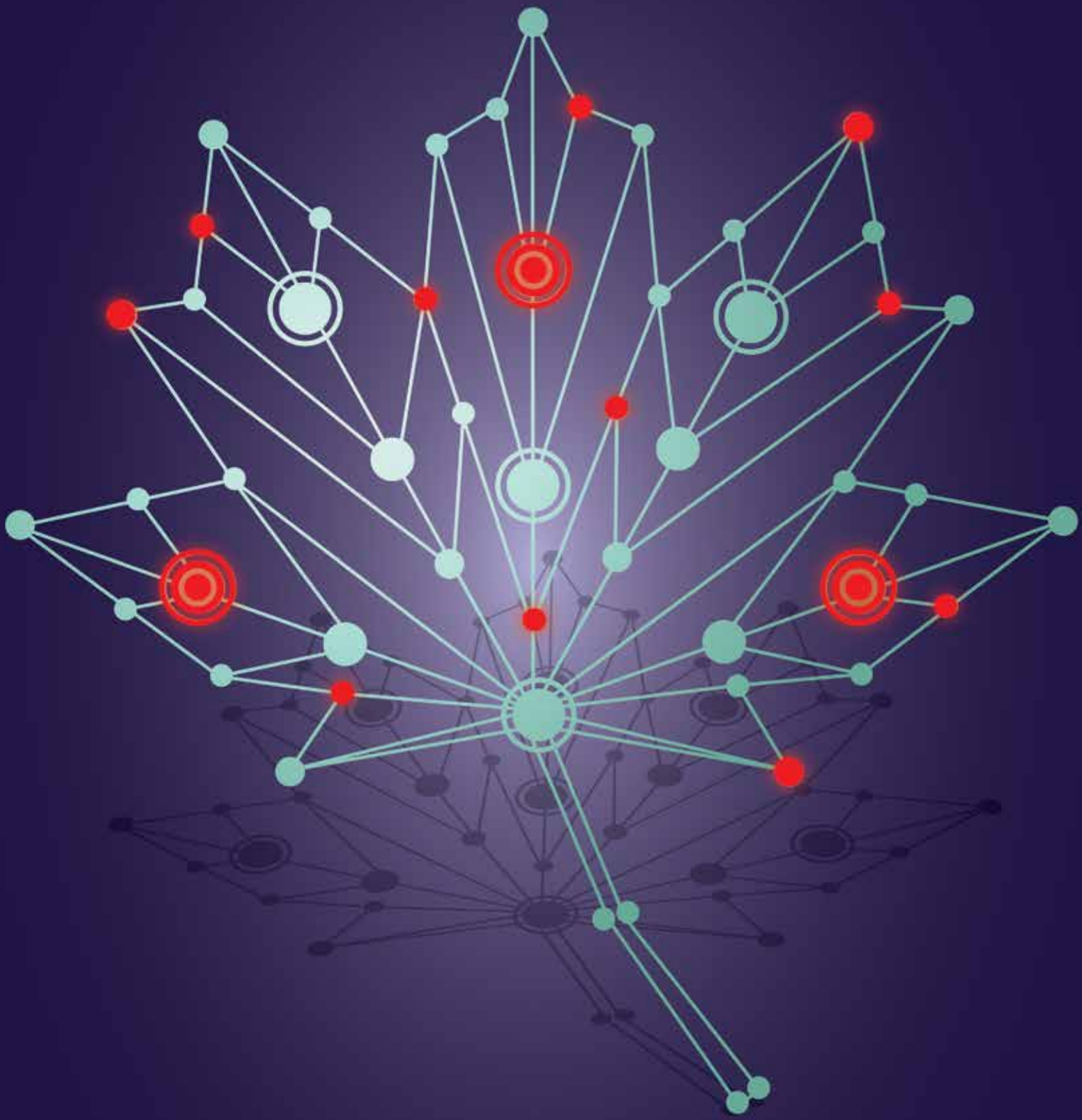
ESTIMATIVE LANGUAGE

The chart below matches estimative language with approximate percentages. These percentages are not derived via statistical analysis, but are based on logic, available information, prior judgements, and methods that increase the accuracy of estimates.



ENDNOTES

1. See Figure 11 for a description of sophistication levels.
2. Humphreys, Adrian. "Anonymous leaks another high-level federal document as part of vendetta against government." The National Post. 26 September 2015. <http://news.nationalpost.com/news/canada/anonymous-leaks-another-high-level-federal-document-as-part-of-vendetta-against-government> Accessed: April 2017.
3. Cyber threats against Canada are individuals or groups that use cyber capabilities against Canadian computers, networks, and other information technology, or the information they contain.
4. Cyber capabilities are computer and Internet-related activities that can be used to affect the confidentiality, integrity, and availability of information and information technology.
5. Cybercriminals hired by other adversaries (e.g. nation-states or political actors) are acting as service providers. We consider such examples based on the intention of the group hiring the service.
6. In some cases, Canadian election agencies share their voter lists. For example, Elections Canada sends parts of the National Register of Electors to provinces, some municipalities, and to political parties. "Description of the National Register of Electors." *Elections Canada*. 20 February 2017. <http://www.elections.ca/content.aspx?section=vot&dir=reg/des&document=index&lang=e> Accessed: February 2017.
7. Electronic voting machines are not regularly used in Canada but are used in some other countries. To use these machines, voters will go to the polling station and, rather than use paper ballots, will cast their votes on a touchscreen.
8. Nakashima, Ellen. "Russian Hackers Targeted Arizona Election System." *The Washington Post*. 29 August 2016. <https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html?utm_term=.76054fb28944> Accessed: February 2017;. and "Illinois Voter Registration System Records Breached." State Board of Elections. 31 August 2016. <https://www.elections.il.gov/Downloads/AboutTheBoard/PDF/08_31_16PressRelease.pdf> Accessed: February 2017.
9. "Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information." *Communications Security Establishment*. <https://www.cse-cst.gc.ca/en/publication/itsb-89v3> November 2014.
10. BBC News Staff. "Ghana Election Commission Website Hit by Cyber Attack." *BBC News*. 8 December 2016. <http://www.bbc.com/news/world-africa-38247987> Accessed: February 2017.
11. Escritt, Thomas. "Dutch will hand count ballots due to hacking fears." *Reuters*. 1 February 2017. <http://www.reuters.com/article/us-netherlands-election-cyber-idUSKBN15G55A> Accessed: April 2017.
12. See page 30 for a case study of how cyberespionage works.
13. Office of the Director of National Intelligence. "Assessing Russian Activities and Intentions in Recent US Elections." 6 January 2017. <https://www.dni.gov/files/documents/ICA_2017_01.pdf> Accessed: February 2017.
14. The Darkweb is a collection of websites that are publicly accessible but obscured because users need specific software, configuration, and authorization to access these sites.
15. 75% of surveyed Canadians access the news online. Newman, Nic, et al. "Reuters Institute Digital News Report 2016." Reuters Institute for the Study of Journalism. <http://www.digitalnewsreport.org/survey/2016/canada-2016.> Accessed: April 2017.
16. Auchard, Eric, and Bate Felix. "French candidate Macron claims massive hack as emails leaked." *Reuters*. 6 May 2017. <http://reuters.com/article/us-france-election-macron-leaks-idUSKBN1812AZ> Accessed: May 2017.
17. BBC News Staff. "Push to tackle online 'booter' services." *BBC News*. 5 August 2016. <http://www.bbc.com/news/technology-36993107> Accessed: April 2017.
18. Malware is short for malicious software and includes any software used to gain access to private computer systems, disrupt computer operations, or gather sensitive information.
19. The Associated Press. "Ransomware Attack Hits Pennsylvania State Senate Democrats." *The Wall Street Journal*. 3 March 2017. <https://www.wsj.com/articles/ransomware-attack-hits-pennsylvania-state-senate-democrats-1488584037> Accessed: April 2017.
20. Humphreys, Adrian. "Anonymous leaks another high-level federal document as part of vendetta against government." *The National Post*. 26 September 2015. <http://news.nationalpost.com/news/canada/anonymous-leaks-another-high-level-federal-document-as-part-of-vendetta-against-government> Accessed: April 2017.
21. CSE detects adversaries probing Government of Canada systems hundreds of millions of times per day.
22. Freedom House. "Freedom in the World 2017." <https://freedomhouse.org/report/freedom-world/2017/canada> Accessed: April 2017.



National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu