DEFENDING DEMOCRACY:

CONFRONTING CYBER-THREATS TO CANADIAN ELECTIONS

September 2019

Holly Ann Garnett
Michael Pal
Christian Leuprecht
Elizabeth F Judge

Contents

INTRODUCTION

Defending Canadian Democracy

In recent years, the cybersecurity of elections and democracy has emerged as a key issue both at home and abroad. Recent examples make the urgency of this issue clear: the 2017 Presidential elections in Kenya were declared invalid amidst allegations of problems with the electoral commission's databases and computers; Estonia's widely respected identity card system, which is used for I-voting in elections and access to government services, was found to be susceptible to identity theft in 2016; and, most infamously, the U.S. Senate intelligence Committee found evidence of Russian interference in the 2016 American presidential election.

While Canada's federal democratic institutions may appear to be relatively immune to cybersecurity issues, with elections that feature paper ballots counted by hand, Canada's outward-facing national security agency, the Communications Security Establishment has outlined several cyber threats to Canadian elections, including data privacy and media manipulation. As such, the cybersecurity of Canada's democratic institutions will be a key concern in the 2019 Canadian federal election.

In response to these important threats to Canadian security, this report addresses two major questions related to cybersecurity and the defense of democratic institutions in Canada and abroad:

1) **What are the major security threats posed by new and emerging technologies to Canada's democratic institutions?**
2) **What are the potential solutions to these threats, and how might they safeguard elections against cyber-attacks while preserving voter privacy, political trust, and overall democratic legitimacy?**

This report takes an electoral cycle approach to understanding the major cyber-threats to Canadian democratic institutions. This approach considers elections as a series of activities that extends from the pre-election period when laws are created and voters registered, through the campaign, to election day polling, the vote count, and the aftermath of the election (Figure 1).

We also consider two related but distinct threats to contemporary Canadian democracy: cyber operations and information operations. Attacks of the first kind may target cyber-infrastructure, including hacking and manipulating information and technological resources, but they can also include information campaigns seeking to spread false, misleading, or incendiary information. Both types of threats are addressed in this report.

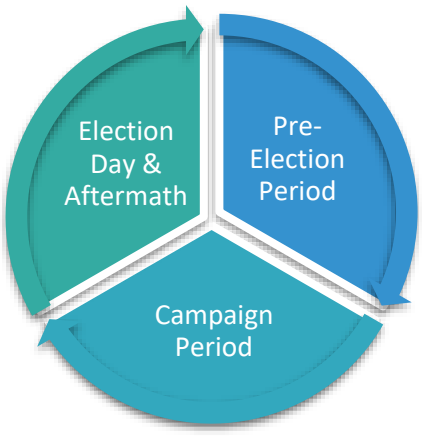


Figure 1: The Electoral Cycle

The content here draws on case studies from each stage of the electoral cycle, as presented at the October 26, 2018 workshop "Defending Democracy," at the Telfer School, University of Ottawa. The challenges identified cross jurisdictions within Canada and national borders. This report therefore engages with Canadian federal and municipal elections, and considers the approaches taken by other democracies, particularly the United States, the Netherlands, and Latvia. It addresses issues from online voting, to voter registration, social media, and privacy, among others. It concludes with lessons learned for policymakers to build democratic resilience in Canada.

AN ELECTORAL CYCLE APPROACH

Pre-Electoral Period

The pre-electoral period encompasses the activities that take place before the official campaign begins. This stage of the electoral cycle commences immediately after the previous election and involves a variety of actors from politicians and policymakers creating new electoral laws, to election administrators registering voters.

The crafting of election laws can occur at any stage of the electoral cycle, as legislators seek to address emerging challenges to electoral integrity through policy responses. This was the case between the 2015 and 2019 Canadian federal elections, with the *Elections Modernization Act*, which amended some of the rules that govern elections in Canada. The second case study presented in this report considers some potential future changes to election law, by exploring the crafting of privacy legislation.

The other major task of the pre-electoral period is the registration of voters. Since the advent of the permanent register of electors, the voter registration process has become a continuous one in Canadian elections, occurring throughout the electoral cycle. However, the process of gathering the personal details of electors brings with it several potential security threats. Electronic registration databases may be susceptive to breaches of privacy, hacking to change or leak information, malware, data corruption, or even ransom of personal data. This has become a particularly concerning threat since registration both federally and in many provinces has become available online.

Perhaps even more important than the actual threats of hacking are the potential changes to voter behaviour due to perceived threats. Voters who fear that their personal information may be accessed by mal-intentioned actors may be reluctant to register. This can put election management bodies at a disadvantage on election day by not knowing where to allocate resources, but also may depress turnout if voters are not provided pre-election information because they are not registered. These concerns regarding online registration are further addressed in the first case study, considering the rise in online registration in American states.

CASE STUDY

Online Voter Registration in the United States

CASE STUDY PREPARED BY: HOLLY ANN GARNETT (ROYAL MILITARY COLLEGE OF CANADA)

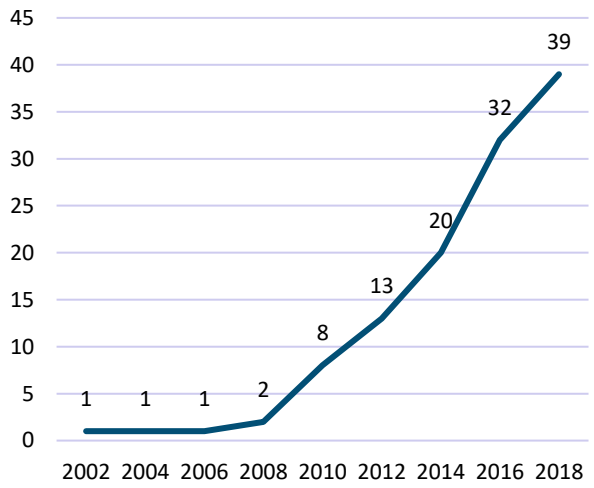
How is technology used?

For most citizens, the first step in the voting process is registration. This can take a variety of forms between, and even within, countries. In some places, registration takes place through door-to-door enumeration. In others, it is the voter's responsibility to submit their registration information before a closing date in order to be eligible to vote.

One method that has been gaining popularity integrates the use of technology into the registration process, allowing voters to register without leaving their home. Online registration allows voters to complete all, or a portion of, the registration process on an online platform. In most fully online systems, voters fill out a registration form entirely online, often providing a driver's license, passport or other identification number to prove identity. Voters can also often access their registration file to amend their legal name or address if it has changed since the last election. In partially online registration systems, voters can fill out an online form to register or amend their registration but must print, sign and mail it to the appropriate election official. Some online registration systems allow voters to apply for special voting options, including absentee ballots, online. These online registration systems are thought to streamline the administration of voter registration records, improve the accuracy of those records, and potentially even increase voter turnout.

In the United States, the number of states with online registration has increased from 1 to 39 since 2006. Arizona was the first state to enact online voter registration in 2002, and since then many states have followed suit, moving parts or all their registration processes online (Figure 2).

Figure 2: Number of States Using Online Registration



Data from: National Council of State Legislatures

Where are the major security concerns?

Despite its popularity, there are several potential concerns related to privacy and security associated with the use of online registration. Public access to online registration could be disrupted by issues of distributed denial-of-services (when a website is overloaded with fake attempts at access) which could limit access at a crucial time in the electoral cycle. One could also envisage hackers gaining access to the registration website and providing false information about voter registration.

There are also issues regarding the privacy and security of voters' personal data, which can be susceptible to breaches of privacy and ransom of information, since most online registration systems require voters to input identifying details such as their driver's license.

Furthermore, if hacking occurs, information could be erased or amended. This could cause serious challenges at the polls if voters were prevented from voting due to an incorrect registration system, especially since election day registration is not universal in the United States.

What are the implications of these challenges?

Whether or not these security breaches materialize, the potentiality of these challenges can have serious implications for elections, especially for public trust. Electoral integrity rests on public willingness to trust the system and candidates' willingness to abide by results. If voters are concerned about security or privacy issues, they may not be willing to provide election administrators with their personal information online, thus impeding the ability of an election management body to plan for election day, or even prevent the voter from casting their ballot.

What solutions have been suggested?

The solutions to these challenges require two very distinct approaches. The first is to build the capacity of election management bodies to respond to new security threats, by contingency planning and running through potential scenarios. The second is to build overall trust in electoral management to ensure that if issues arise voters have legitimate confidence in the electoral officials seeking to address these challenges.

CASE STUDY

Privacy Laws in Canada

PRESENTED BY: ELIZABETH F JUDGE (UNIVERSITY OF OTTAWA)
CASE STUDY PREPARED BY: DESMOND BARTON (QUEEN'S UNIVERSITY)

How is technology used?

Internet usage leaves a trace. Public and private actors can collect this data and create individual profiles with information ranging from purchasing habits, online browsing history, and other personal information (e.g. credit card information). This collection and analysis of data is highly valuable to public and private institutions alike. For example, political parties use these data profiles about voters to determine which campaign strategies would have the best success in appealing to particular demographics and microtargeting their advertising to ask for votes and donations.

What are the major security concerns?

There are significant legislative gaps in protecting voter privacy. First, current privacy statutes apply only to government and commercial actors. Political parties do not fall within the Privacy Act or the Personal Information and Protection Electronic Documents Act. Second, elections law imposes few privacy rules on political parties apart from having a privacy policy. The Canada Elections Act requires that political parties have a privacy policy but does not establish criteria for the policies. Third, self-regulation by political parties suffers from a lack of transparency and accountability.

As a result, there is a lack of transparency about the mass data collective and analytical capabilities of political parties. Specifics such as the terms of data sharing agreements between federal and provincial parties, as well as whether or not political parties sell voter data to third parties, remain unclear.

Further, lawmakers generally underestimate the "increasing sophistication of big data analytics and artificial intelligence" to collect information for "social media companies as well as third party advertisers." The resulting "online data ecosystem" characterized by multiple players who market in personal information is defined by what Judge, in her 2018 presentation, calls "data promiscuity," a particularly apt term given the present mass collection and proliferation of data, as well as the lack of appropriate limitations on these activities. In the context of electoral cybersecurity, data promiscuity, paired with the shortcomings of relevant legal frameworks and the inadequate and inconsistent self-regulation of political parties, leads to the commodification of voter data, and an increased "risk of misuse and improper disclosure of voter data/consumer data."

Figure 3: Fair Information Principles

What are the potential solutions to these challenges?

To protect voter data effectively, a common suggestion is that legislators should draw on the fair information principles to create privacy regulations for political parties. However, as Judge observed, the fair information

principles on which privacy law is based have their own flaws so voter data would be vulnerable even if political parties had the same obligations as government or private companies. Data protection statutes are based on a model that emphasizes consent. This emphasis on consent leaves the average user vulnerable, as they lack an understanding of the variety of ways their data can be used and the multitude of sources drawn upon to construct their respective data profile. Privacy policies are typically framed broadly and offer a "take it or leave it" approach.

These legislative shortcomings could be overcome in a variety of ways: by enacting new legislation applicable specifically to political parties, by further amending elections law to add more privacy obligations, or by expanding privacy statutes to include political parties. Certain academics, however, argue that the online data ecosystem itself must first be re-imagined. Judge envisions an ecosystem modeled around new rights for individuals that focus on decreasing the amount of data that is initially collected and requiring entities to obtain informed consent. One example of this kind of model is Apple CEO Tim Cook's four essential rights. By emphasizing a voter-centered model, legislators could hopefully establish more effective privacy regulations for political parties and stronger privacy protections for voters. Time will tell if there is a political willingness to do so.

Figure 4: Tim Cook's Four Essential Rights

1) The right to have data collection minimized

- **you can consent to, or withdraw consent from, the collection of specific data**

2) The right to knowledge of data being collected

- **you know "what data is being collected and what it is being collected for"**

3) The right to access the data collected

- **you can receive, correct, or delete a copy of your personal data**

4) The right to security

- **your data must be collected, stored, and used responsibly**

AN ELECTORAL CYCLE APPROACH

Campaign Period

As the campaign begins (either officially when the writ is dropped, or unofficially much earlier), a new set of challenges in defending democracy are brought to the forefront. In recent years, these challenges have been focused on threats to the security of information that voters consume regarding electoral procedures, candidates, and issues. These challenges can be generally divided into three categories: intimidation, inequality of access, and disinformation.

The intimidation of voters or candidates, including harassment, hate speech, and threats through online means presents a new set of challenges. This may impede a voter's willingness to engage in healthy debate, or impede a candidate (particularly women or those from a minority group) from entering into the race.

A reliance on online sources of information also presents some unique threats. Information accessed through social media and other niche online platforms may lead to inequalities of information access, and differences in the types of information accessed by different groups. This can lead to increased polarization and division among an electorate. The unique threats posed by social media in Canada is the focus of the second case study on the campaign period in this report.

Disinformation also remains a key concern for electoral integrity. False or misleading information can be provided to voters in many ways, from fake or impersonated accounts, to false and incendiary news. This false information, even if corrected, can impede a voter's ability to make a competent decision on election day, since the damage is already done once the information has influenced the voter. Those seeking to influence elections, including those from outside of Canada, may find manipulating the voter before the election through disinformation campaigns an easier way to effect an election than targeting electoral infrastructure. This is the focus of the first case study on the campaign period, which draws on the experience of Latvia's 2018 parliamentary elections.

CASE STUDY

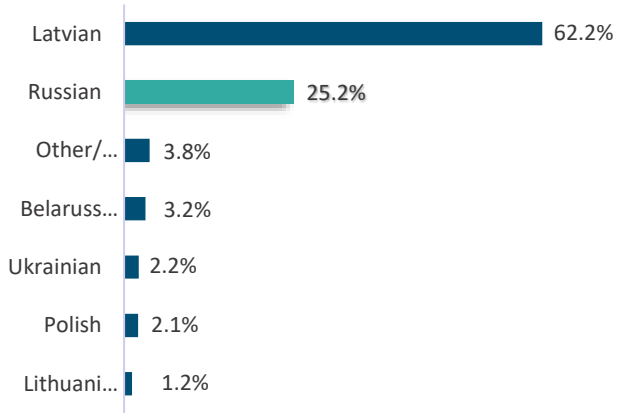
Foreign interference in Latvian Elections

PRESENTED BY: MĀRIS ANDŽĀNS (RĪGA STRADIŅŠ UNIVERSITY & LATVIAN INSTITUTE FOR INTERNATIONAL AFFAIRS)
CASE STUDY PREPARED BY: DESMOND BARTON (QUEEN'S UNIVERSITY)

How is technology used?

Mass media has the capacity to unite as well as divide—and can be a tool of democratic interference. The Kremlin media involvement during the campaign period of the 2018 Latvian parliamentary election highlights these dangers. Latvia, with its sizeable Russian-language population (Figure 4) was particularly susceptible to Russian disinformation campaigns. While Western social media sites such as Facebook and Twitter remain popular amongst the general Latvian population, Russian-language social media such as VKontake (VK) are popular amongst a demographic with no viable Russian-language media alternative to those whose content is partly or fully produced in Russia. Russian-language news sites and television broadcasts known for propagating Kremlin talking points, such as RTR Planeta, NTV Mir, REN TV, thus serve as ubiquitous sources of information for Russo-Latvians.

Figure 5: Ethnic Composition of Latvia



Data from: CIA 2018

What are the major security concerns?

Russian-language media's efforts to promote a narrative portraying Latvia as a fascist, anti-Russian, and failed state stoked major security concerns with regards to Latvian democratic processes. Officials were particularly worried about a potential surge in pro-Russian and populist parties, especially given the prior electoral success of the Social Democratic Party *Harmony*, which predominantly receives votes from Latvia's Russian-speakers. A party of Latvian centre-left politics, *Harmony* possesses historical ties with political parties in Russia such as United Russia, the dominant political power in the Russian Federation. The close relationship between *Harmony* and pro-regime Russian political parties, as well as *Harmony's* sympathetic positions toward Russia, led to concerns that *Harmony* would pander to fringe pro-Russian positions in Latvian politics.

What are the implications of these challenges?

A number of pre-emptive measures were used to address the aforementioned fears and provide a degree of security for Latvia's electoral integrity; An inter-institutional Election Security Working Group was established, the expenditures of political parties were closely monitored, and attempts to educate the public through campaigns raising awareness about disinformation were carried out nationwide, while media channels displaying severe bias faced fines and/or suspension. Highly prominent pro-Russian activists were additionally detained in the period before the election. Just as in the two elections prior, *Harmony* emerged with the majority of votes but did not gain a place in the coalition; this created a coalition government consisting

of the liberal-conservative *New Unity*, the centre-right conservative *New Conservative Party*, the centre-right conservative *National Alliance*, the liberal *Development/For!,* and the catch-all populist party *Who owns the state?.*

While the state's efforts were largely limited to the election period, Latvia has additionally developed solutions with long-term challenges in mind. First, steps have been taken in pursuit of creating more balanced Russian-language news and media alternatives in the hope that the viewership of biased Russian-language services will decrease accordingly. Second, a number of sophisticated cyber security teams have been established to ensure a more coordinated approach to Latvia's electoral cybersecurity. The National Computer Incident Response Team (CERT.LV) responsible for administrating the exchange of information between the public and private sectors, and the Cyber Defense Unit, a team of IT specialists and students from both the public and private sectors are trained to aid the cyber capacities of Latvia's national armed forces and/or CERT.LV in the event of a significant cyber threat.

In sum, the case of the 2018 Latvian parliamentary election is particularly relevant to liberal democracies with unresolved and deeply historical cleavages. As social media has grown as the predominant means of organization for associated movements, so too has the ability of foreign states to manipulate these cleavages over the very same platforms.

CASE STUDY

Social Media in Canadian Election Campaigns

PRESENTED BY: MICHAEL PAL (UNIVERSITY OF OTTAWA)
CASE STUDY PREPARED BY: GANT CROKER (QUEEN'S UNIVERSITY)

How is technology used?

In recent years, social media has emerged as a crucial tool for political advertising during electoral campaigns around the globe. Its effectiveness is unsurprising: social media can reach large audiences while maintaining a low cost compared to traditional advertising. Furthermore, the advent of micro-targeted ads on social media enables campaigns and interest groups to target individuals that are more receptive to their messages. The public is unaware of the ads sent to specific people on social media, and micro-targeting creates incentives to engage in more negative or polarizing advertising than would be the case on television or radio, where the collective general public has access to the content.

In Canada, the regulatory framework for political advertising is focused on television, radio, and print, but is largely out of date regarding social media. As a result, misinformation and foreign interference are legitimate problems on social media. As this aspect of campaign advertising changes, Canada must address issues regarding social media in elections with both legal means, as well as further cooperation with social media platforms.

What are the major security concerns?

Misinformation campaigns and foreign interference present major threats to the integrity of elections both in Canada and abroad. As notably demonstrated in the 2016 US Presidential election, foreign interference, mainly on the part of Russian groups, sought to influence voters through social media campaigns. Specifically, Russian groups purchased advertisements on Facebook meant to polarize voters. Tactics included attacking candidates, while also making divisive ads on key issues such as immigration. These attempts were designed to disrupt the election and influence the results, while also injecting doubt into the democratic process as a whole.

Canadian laws have been slow to react to the transition to social media advertising. Campaign finance laws are generally designed to ensure fair campaigns in the offline world but do not adequately address online ads. These laws effectively manage how much campaigns can spend and regulate fair treatment of campaigns by traditional broadcasters. However, this does not translate easily to social media.

What are the potential solutions to these challenges?

Existing election laws based on the values of transparency and equality can provide a set of solutions. Such solutions emerge in three categories: transparency and disclosure rules, campaign spending rules, and effective enforcement.

Ensuring the transparency of advertising on social media is key. Real-time disclosure should state the cost of advertisements, the source, as well as the search terms that have led a user to receiving a particular ad. This real-time disclosure would ensure that users are able to see who is advertising to them. In addition, by including key search terms in this disclosure, users can be informed that they are being specifically targeted, and the reasons why they are targeted for those advertisements.

While C—76, the *Elections Modernization Act (2018),* made some progress, campaign spending laws still need to be updated to account for social media. Imposing a separate online spending limit on political campaigns

would help level the playing field between parties. Another necessary reform would be to expand the laws already regulating broadcasters who accept election advertisements so that they apply to social media platforms. Broadcasters are not permitted to charge differential rates to political parties, partly to ensure that there is no favoritism. To ensure fairness, this rule should be expanded to cover social media platforms such as Facebook.

Finally, election laws that apply to the campaign period, and now the regulated time immediately before the campaign, may need to be expanded so that they apply much earlier; online campaigning happens year-round. Campaign-focused laws, such as spending limits, may be ineffective in this environment of the permanent campaign.

AN ELECTORAL CYCLE APPROACH

Election Day & Aftermath

Election day is rarely only one day. Most countries have multiple days and options for voting in order to make the process more convenient and accessible. Electoral process innovations have included the increasing usage of advance voting mechanisms (including postal and early voting) and the use of technology in the vote. This use of technology for casting and counting ballots, as well as disseminating the results, is the focus of this stage of the electoral cycle.

One of the most high-profile concerns about the use of technology in the voting process is the hacking of voter information or manipulation of voting data. While Canada's federal elections are completed entirely by paper ballots, provincial and municipal elections have adopted various technologies, from optical scans to online voting for their elections. The two case studies presented in this report focus on the use of technology to cast ballots. The first considers the Netherlands, where electronic voting was cancelled, and ballots unexpectedly hand-counted due to a threat of hacking. The second case study considers the lack of regulation of online voting in Ontario municipalities.

The technology used to cast ballots is not the only concern related to the cybersecurity of election day and its aftermath. Disinformation remains a concern on election day, or whenever the voting process is taking place. One can easily imagine false information about voting locations, times or procedures being propagated online, especially if a reputable election management website or social media account is taken over by hackers. Likewise, a denial of service on these sources of online information through a distributed denial-of-service or defaced website could easily leave voters in the dark about their voting procedures, or the results of an election.

CASE STUDY

Electronic Voting in the Netherlands

PRESENTED BY: LEONTINE LOEBER (UNIVERSITY OF EAST ANGLIA)
CASE STUDY PREPARED BY: JOSEPH SZEMAN (QUEEN'S UNIVERSITY)

How is technology used?

Dutch municipalities first began using technology in the voting process as early as the 1960s. At the time, although there were some regulations regarding voting-computers, their use in the election process was not as closely regulated as that of traditional paper ballots. This has resulted in a lack of standards for storage and upkeep for e-voting across municipalities in the Netherlands. By 2006 roughly 95% of voters were using e-voting machines. Despite nearly 80% of voters indicating that they trusted the accuracy of e-voting machines following a parliamentary election in 2006, electoral laws were changed and the certification for e-voting machines was withdrawn due to concerns regarding a lack of paper trail and accountability. Since then several attempts have been made to re-introduce technology, ranging from voting computers to electronic counting of ballots, in the electoral process. However, none have been successful, due to both security concerns and a lack of a clear focus within the government and Parliament on the use of technology in the electoral process. The Dutch Electoral Council developed new software for the registration of candidates, parties, and the tallying of votes in 2007 (Figure 7) but the security of that software is currently questioned and it is unclear if it will be used again.

Where are the major security concerns?

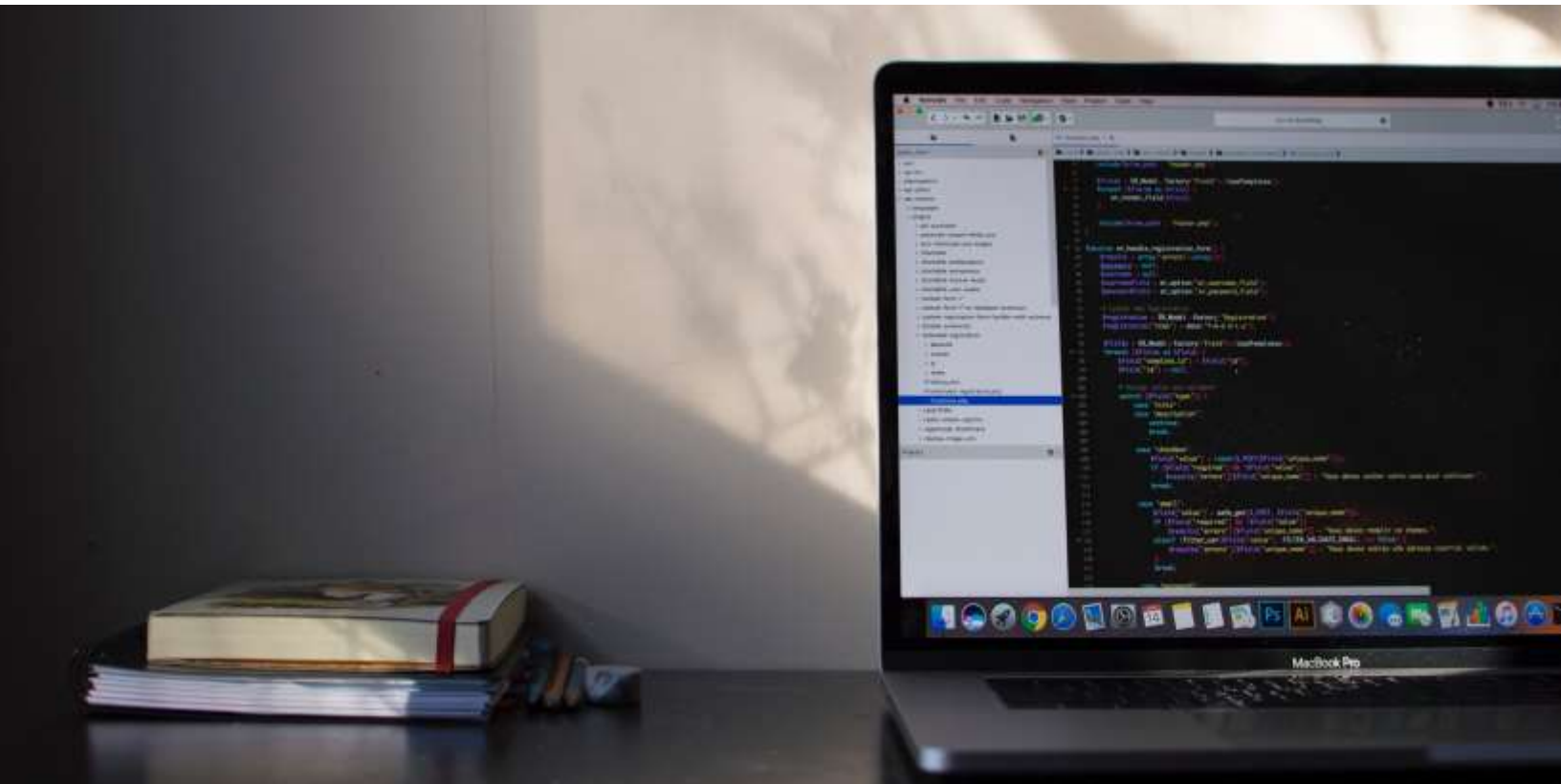
Key security challenges with e-voting in the Netherlands have evolved over time, ranging from inconsistent security standards, to concerns about the reliability and possible vulnerabilities of the software running e-voting machines. These issues, in addition to a lack of a paper trail to check vote counts, have raised concerns related to the possibility of ballot counts being manipulated or altered. This potential, due to lax security standards and exacerbated by lack of a paper trail, remains the most pressing concern surrounding the use of e-voting in the Netherlands.

What are the implications of these challenges?

There are key commonalities between the challenges and security risks of the adoption of technology in the Dutch electoral process and the use of Internet voting processes in municipal elections, particularly with respect to a lack of standards governing the use of Internet voting across municipalities, as well as security flaws in voting systems. Both countries lack a distinct, long-term plan for the consistent use and implementation of e-voting machines in a way that meets expectations of both accessibility and security.

Figure 7: A Timeline of E-Voting in the Netherlands

1960	•E-voting begins in municipalities in the Netherlands
2004	•The Netherlands experiments with Internet voting for citizens abroad
2006	•Nearly 95% of voters use voting machines built by a single Dutch company •Internet voting for voters abroad •The certification for voting machinesis withdrawn and electoral laws for the 2006 election are changed following security and reliability concerns
2007	•A committee appointed by the Dutch government recommends an electronic printer and counter •New software from the Electoral Council developed to assist parties and candidates by tallying and announcing voting results
2013	•New committee installed to investigate technology in the voting process, same recommendations •Bill entered into parliament to re-introduce e-voting
2017	•User experience trials with smaller ballot paper necessary to introduce electronic counting •Bill to introduce smaller ballot paper voted down by Parliament •Discussions on security of software used by the Electoral Council



CASE STUDY

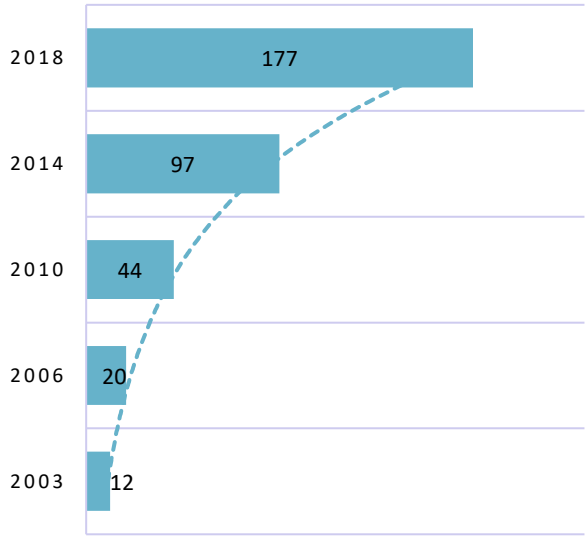
Online Voting in Canadian Municipalities

PRESENTED BY: ALEKSANDER ESSEX (UNIVERSITY OF WESTERN ONTARIO)
CASE STUDY PREPARED BY: JOSEPH SZEMAN (QUEEN'S UNIVERSITY)

How is technology used?

The October 2018 Ontario municipal elections saw the largest deployment of online voting systems in Canada to date. Of the 444 municipalities in Ontario, 391 ran elections in 2018. Of these, 45% employed online voting systems, representing an 82% increase overall in municipalities choosing to use online voting systems since the previous elections in 2014 (Figure 8).

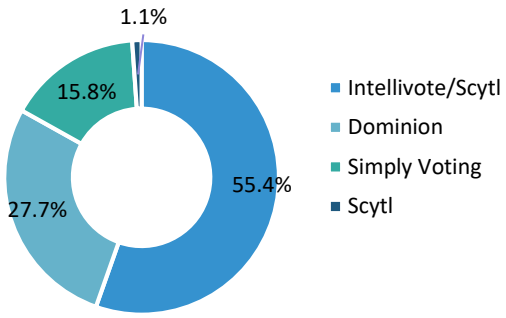
Figure 8: Number of Municipalities in Ontario Using Online Voting



Data from: https://www.tvo.org/article/how-e-voting-is-taking-over-ontario-municipal-elections

There were four vendors that delivered online voting services to Ontario municipalities: Intelivote/Scytl (in partnership), Dominion, Simply Voting, and Scytl (individually). Of these four, the Intelivote/Scytl partnership was the largest, serving 55.4% of the 177 municipalities using online voting systems. Dominion was the second largest serving 28% (Figure 9).

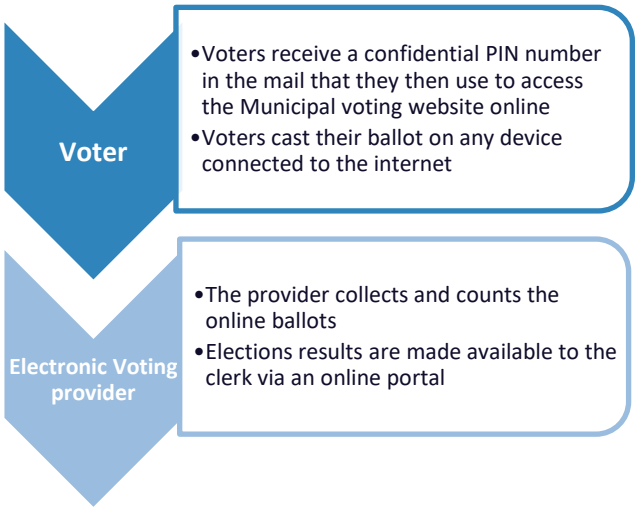
Figure 9: Online Voting Vendors in Ontario



Data from Online Voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology?

The different online voting services in the 2018 Ontario municipal elections generally followed similar processes.

Figure 10: Online Voting Process



Where are the major security concerns?

The legislation that governs municipal elections in Ontario, the *Municipal Elections Act*, includes a set of rules and procedures for paper ballots but not online ballots. While a clause permits the use of "alternative voting methods" (such as online voting) it does not explicitly include the words "internet" or "online." As a result, the procurement, delivery, and counting of online ballots is entirely up to each municipality. This means that there were 177 distinct sets of rules and procedures for online elections.

Several accountability and privacy concerns exist with the current implementation of online voting systems in Ontario. Firstly, vendors sometimes make questionable privacy claims about their products, promising that it is impossible for e-voting staff to see votes that are cast. However, this is not entirely true, as much of the voting data is recorded unencrypted by the server. In turn, this casts some doubt on ballot secrecy and the processes by which vendors tabulate online votes. Second, the envelopes containing the confidential voting PINs that enable online voting were see-through when held up to light, and were frequently sent to voters that had moved or passed away. This could enable voters to vote twice or hijack another voter's PIN without opening their envelope. Finally, a study on Online Voting in Ontario Municipal Elections of the use of date-of-birth as a login credential shows that it could potentially be used to link voter identities with cast ballot preferences.

What are the implications of these challenges?

According to the Association of Municipalities in Ontario (AMO), nearly 3.6 million voters in Ontario cast ballots. Despite the lack of official statistics, we estimate up to one million voters cast a ballot online in 2018. Online voting in Ontario municipal elections is unlikely to stop. However, the lack of consistent regulation of electronic voting is unsustainable and presents significant security concerns. In fact, a number of municipalities including Toronto, Guelph and London refused the use of online voting for security reasons.

Standards for online voting systems are badly needed and will become increasingly important for maintaining a truly democratic process in an environment that is vulnerable to accountability, privacy and security risks.

Lessons Learned

Drawing together the lessons of these case studies, we can suggest a number of lessons learned for policymakers, practitioners, academics and the public. These conclusions suggest that there remain some vulnerabilities in Canadian elections to cybersecurity issues, at all stages of the electoral cycle. These include the vulnerability of voter information, the promises and perils of social media, regulations for campaign finance and foreign interference, and the adoption of regulations for new technologies used at the polls. In addition to the broader task of building societal resilience to these threats, there are a number of ways that a variety of actors from politicians and political parties, from legislators to election administrators, can work together to defend Canadian democracy from cyber-threats.

1

- Elections are vulnerable at all stages of the **electoral cycle**.
- Policymakers must consider these stages while creating solutions for cybersecurity threats to democracy.

2

- Political parties and election management bodies should be aware of, and plan for, the **vulnerability of voter information**, such as data corruption and leakage, that should be considered at all stages of the electoral cycle.

3

- Electoral laws must evolve to regulate the increasing number of entities involved in elections, including the activities of **social media platforms** and the role of targeted advertisements online.
- While the *Elections Modernization Act* made important changes to Canada's federal election laws, more needs to be done to recognize these new actors and acknowledge and regulate their place in elections.

4

- **Campaign finance laws** need to be adapted and enforced for the online world.
- This will especially assist in identifying actors seeking to influence Canadian elections form abroad.

5

- Elections Canada has prudently been slow to adopt **new technologies** into the electoral process. Paper ballots may be the right approach until issues with e- and I-voting are clarified.
- Jurisdictions that were early adopters of election technologies have faced serious challenges and are testing the waters for Canadian adoption in the future.

APPENDIX

Authors

Holly Ann Garnett

Holly Ann Garnett is an Assistant Professor of Political Science at the Royal Military College of Canada. Her research examines how electoral integrity can be strengthened throughout the electoral cycle, including the role of election management bodies, election technologies, civic literacy and campaign finance.

Michael Pal

Michael Pal is an Associate Professor in the Faculty of Law at the University of Ottawa. He researches the law of democracy, comparative constitutional law, and election law and has published in the fields of law, political science, and public policy.

Christian Leuprecht

Christian Leuprecht is the Class of 1965 Professor in Leadership in the Department of Political Science and Economics at the Royal Military College. His research includes work on cybersecurity and the application of social network analysis to transnational crime.

Elizabeth F Judge

Elizabeth F. Judge is Professor of Law and member of the Centre for Law, Technology and Society at the Faculty of Law at the University of Ottawa, where she specializes in intersections of law, technology, and policy. Her research examines legal protections for voter privacy and electoral cybersecurity.

APPENDIX

Acknowledgements

This report was prepared with the assistance of Madison MacGregor (McGill University). Case studies were prepared by Desmond Barton (Queen's University), Gant Croker (Queen's University) and Joseph Szeman (Queen's University).

The associated workshop took place on October 25, 2018 at the Telfer School (University of Ottawa) in Ottawa, Ontario, Canada. It was organized by Holly Ann Garnett (Royal Military College of Canada), Christian Leuprecht (Royal Military College of Canada / Queen's University), Michael Pal (University of Ottawa) and Elizabeth Judge (University of Ottawa). We are grateful for the assistance of the Canadian Defense Association Institute (CDAI), and Matthew Overton in particular, for their assistance in organizing this workshop.

We are grateful to the following partners for their support:

- The Canadian Defense Association Institute
- SERENE-RISC Smart Cybersecurity Network
- The Royal Military College of Canada
- The Telfer School at the University of Ottawa
- The Social Sciences and Humanities Research Council of Canada

This research was supported by:


Social Sciences and Humanities Research Council of Canada
Conseil de recherches en sciences humaines du Canada
Canada