CANADA'S SECURITY POLICY REVIEW

Photo: Markus Spiske, Unsplash

PREPARED BY

Bernard Bishop, MA Candidate
Jake Yeates, MA Candidate

NPSIA
The Norman Paterson School of International Affairs

iAffairs

CFPJ

Canada’s Security Policy Review

Authors: Bernard Bishop and Jake Yeates

Executive Summary

This Policy Review recommends the creation of a new Act of Parliament that performs two functions; (1) creates regulations seeking to control the prevalence of disinformation on social media platforms, and (2) creates a new independent government agency to enforce these regulations.

Disinformation is false or inaccurate information that is *deliberately* created and propagated for malicious purposes. Social media facilitates the spread of disinformation by allowing for the rapid and unaccountable sharing of information from any source. As such, Canadians are being exposed to both accurate and inaccurate information simultaneously. The equal nature by which both credible and non-credible information is presented to readers can make differentiating the two very difficult.

Significant portions of the disinformation being consumed by Canadians is originating from foreign actors who seek to influence Canadian's thoughts and actions. These efforts are often meant to affect Canadian electoral decision-making. As such, given social media's unprecedented ability to propagate disinformation to a nation-wide audience, disinformation presents a significant threat to Canadian interests. Disinformation can be used to suppress Canadians’ ability to vote, namely by sharing incorrect voting-related information which challenges their ability to attend the poles during the designated period. However, disinformation is primarily designed to influence *how* its victims vote, rather than *whether* they vote.

The new *Digital Information Integrity Act* would address this threat by reducing the amount of disinformation seen by Canadians online. It would do this by creating a new independent agency responsible for identifying and reporting disinformation online and drafting new regulations requiring specific responses by social media platforms hosting the disinformation.

Canada does not currently have any means to obstruct the dissemination of disinformation online. This Policy Review seeks to provide the Government with limited tools to reduce the amount of disinformation subjected to Canadians. The threat of disinformation is expected to grow - this proposal would allow the Government to begin working towards meeting that growing threat.

Abbreviations

BQ	Bloc Québécois
CCCS	Canadian Centre for Cyber Security
CDII	Commission of Digital Information Integrity
CEA	Canadian Elections Act
CEIPP	Critical Election Incident Public Protocol
CPC	Conservative Party of Canada
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DIIC	Digital Information Integrity Commissioner
DND	Department of National Defence
DoJ	Department of Justice
EC	Elections Canada
GAC	Global Affairs Canada
GoC	Government of Canada
ISEDC	Innovation, Science and Economic Development Canada
KPI	Key Performance Indicators
LPC	Liberal Party of Canada
NDP	New Democratic Party
NCSB	National and Cyber Security Branch
RCMP	Royal Canadian Mounted Police
SITE	Security and Intelligence Threats to Elections Task Force
PCO	Privy Council Office
PSC	Public Safety Canada

Background, History and Policy Process

Problems Facing the Nation

Various democracies, including Canada, are being subjected to disinformation campaigns designed to encourage internal disorder and manipulate election outcomes.[i] These campaigns are originating from foreign states and are believed to be state-sponsored.[ii] By manipulating social media and other digital tools, including creating fake accounts and false messaging, "foreign adversaries" are attempting to affect the way Canadians view policy issues, promote particular political parties, and intensify partisan divisions.[iii] These disinformation attacks are intended to destabilize the political system and undermine the public's "trust in the truth."[iv] Given the generally strong protections among advanced democracies for freedom of expression, their vulnerability to false information deliberately created to disrupt the political process is particularly acute. Compared to traditional media sources, social media can transmit disinformation at a much quicker pace which enables the information to be spread faster than ever before. This problem is especially challenging to democracies, as any meaningful response to disinformation is likely to clash with common democratic freedoms – namely freedom of expression.

Disinformation campaigns designed to encourage internal disorder and manipulate election outcomes are now part of modern life.[v] Many of these campaigns are from state-sponsored entities originating in foreign countries, most notably Russia, China and Iran, with the express intent of destabilizing the political system and undermining the public trust.[vi] Per capita, Canadians spend 43.5 hours online per month, and that online activity inevitability leaves both individuals and organizations vulnerable to disinformation programs. [vii] Any governmental response to these campaigns must be balanced against Canadians democratic freedoms.

Past Policies and Critical Decisive Moments

As Brent J. Arnold writes in Cyber Security in Canada: Structure and Challenges, "Canada's approach to cybersecurity is threat-based, federal, multi-stakeholder and international." [viii] As cyber systems and social media grew, the need for a more comprehensive plan was needed. The *Action Plan 2010-2015 for Canada's Cyber Security Strategy* (2013) was to use a combination of heightened prosecution capabilities and education to secure and improve government and public cyber-security systems.[ix] The federal government intended to use this strategy to streamline policy and mandates, with the ability to identify, prevent and mitigate incidents. After the U.S.

election in 2016 and the accusations of foreign interference, the *National Cyber Security Action Plan* (2018) was put forward to update and further extend the ongoing cyber-security environment. As online disinformation and influence campaigns amplified in the lead up to a federal election in 2019, Bill C-59 was implemented containing the *CSE Act*.[x] The Act was instrumental in creating a new unit within CSE to monitor and respond to any cyber threat to government operations, systems and critical infrastructure.

In 2017, the United States released a report asserting that the Russian Government had ordered an "influence campaign," including the dissemination of false information, designed to manipulate the American electorate in the 2016 election.[xi] This report concluded that U.S. allies, including Canada, should expect similar "influence campaigns" targeting their election processes going forward. In 2019, the CCCS warned Canadians to expect similar foreign disinformation campaigns for the 2019 federal election.[xii] Since then, various sources have documented suspected foreign influence campaigns targeting North Americans.[xiii] These campaigns sought to amplify divisions on pipeline issues, "Wexit," and immigration and refugees issues, using "provocative statements.[xiv] Recently, disinformation campaigns have been documented seeking to undermine COVID-19 public health measures, posing an immediate risk to public health security.[xv] A Leger survey from October 12th, 2020 found that due to ongoing disinformation campaigns, the number of Canadians favouring mandatory vaccinations dropped from 57 percent to 39 percent and that 17 percent of those polled said they would not take the vaccine.[xvi] Highlighting the effect of disinformation on the public, a survey by Carleton University's School of Journalism found that 46 percent of Canadians polled believed at least one Covid-19 conspiracy theory.[xvii]

Trends and Indicators

The current trend of disinformation is using social media platforms like Facebook, Twitter, Pinterest, etc. An IPSOS poll found that roughly 90% of Canadians say they have fallen for some type of fake news online through these social media outlets.[xviii] This finding demonstrates the power digital media has on impacting Canadian's understanding of internal and external political matters. Artificial Intelligence and online bots are being used to disseminate disinformation into networks of unsuspecting or duplicitous influencers. In a September 2020 article, The Atlantic theorized that "In this future, AI-generated content will continue to become more sophisticated, and it will be increasingly difficult to differentiate it from the content that is created by humans."[xix] AI coupled with data mining and intelligence analysis will have far-reaching effects on the spread of disinformation. The propagation and augmentation of strategic issues such

as immigration, climate change, and left vs right issues will increase. According to a report released by the CCCS in 2020, online foreign influence operations against Canada are an ongoing threat.[xx] These influence campaigns are aimed not only at Canadian elections but seek to influence domestic discourse regarding such varied topics as the Covid-19 pandemic and critical infrastructure. Twitter accounts that act as proxies for foreign disinformation are increasingly coming from Canadian based links. Between April and June 2020, thousands of tweets were flagged as sharing disinformation, which are used to vilify and amplify the propaganda message.[xxi]

Current Policies and Policy Alternatives

Presently, Canada's response to disinformation is largely ad-hoc in nature and entirely focused on Canadian election periods. Current geopolitical tensions and emergent digital technologies indicate that Canada will have to anticipate, respond and adapt continuously to disinformation campaigns. In 2019, as online disinformation and influence campaigns amplified, changes to both the Canadian Elections Act and Bill C-59 were introduced to combat cyber disinformation campaigns. Those changes, in the form of the Elections Modernization Act, included a prohibition on foreign funding for political activity, restrictions on foreign third parties influencing electors and required that social media companies create political advertising registries to enable tracking of advertising funds on social media sites. The Act's response to disinformation specifically is limited - only introducing new prohibitions against making false statements regarding candidates' personal characteristics and criminal history.

Additionally, the GoC created the CEIPP to address election interference during the election writ.[xxii] SITE was also implemented. Composed of partners from Elections, CSE, CSIS, GAC, and RCMP, SITE was tasked to assess and respond to foreign disinformation threats during the 2019 election. The SITE team reported to the CEIPP during the 2019 election period, made recommendations, and then returned to their respective mandates after the election. No law in the Criminal Code specifically prohibits the propagation of disinformation at this time, although some have called for increased legislation, including additions to the criminal code.

Policy Analysis

Interests and Values

Addressing disinformation will require consideration of two fundamental values; free and fair democratic elections and freedom of expression. Canadians are interested in ensuring that their electoral process is not influenced by foreign parties whose interests differ from those of Canadians. Simultaneously, Canadians have vested interests in ensuring they are free to express their thoughts and beliefs – without requirement that those thoughts or beliefs be "truthful" – be unimpeded. Any initiatives which seek to restrict the deliberate spread of false information with the purpose of affecting electoral outcomes must be balanced with Canadians' formal freedom to express themselves, regardless of the truthfulness of their expression.

Goals and Objectives

The overarching goal is to protect the integrity of the digital information available to Canadians. Many Canadians are largely informed by the information they consume online - including social media platforms, information that is among the factors which influence their decision-making. This information can be deliberately manipulated to influence Canadian public opinion - including electoral preferences. Specifically, the goal is to defend the Canadian electoral processes - federal, provincial, and otherwise - from foreign interference. This is to be achieved by reducing or eliminating the deliberate promotion of disinformation on online social media platforms – with a specific (but not exclusive) focus on disinformation originating from non-Canadian nationals. Objectives include making Canadians aware of disinformation, reducing the likelihood that they are exposed to disinformation, and deplatforming disinformation when especially harmful to Canadian interests. While not explicitly targeted, disinformation designed to suppress Canadians' ability to vote would be inherently included as well.

Stakeholders/Allies and Detractors

Stakeholder	Description	Ally/ Detractor
PCO (GoC)	Responsible for creating and implementing the *Act* and the	**Ally -** Responsible for the creation and

	affiliated CDII	implementation of the recommendation included herein.
Canadian Federal Political Parties and their Members	The various federal political parties which currently hold seats in the House of Commons	**Mixed** - While support is expected from the Government (LPC), opposition is expected from the opposition - particularly the CPC. Successful implementation of the *Act* before the next election will rely on support from either the BQ or the NDP.
The Canadian Public	Directly affected by both disinformation and restrictions on disinformation	**Mixed** - While some may appreciate the risk that disinformation causes to their interests, many will likely object to government restrictions on freedom of expression
The Canadian Civil Liberties Association and other Civil Liberties organizations	Organizations which promote the protection of Canadian civil liberties, including freedom of expression	**Detractor** - Despite efforts to reduce the degree to which expression is infringed, given disinformation is a form of expression, and disinformation is to be restricted (including censorship), freedom of expression will inevitably be infringed.

Social Media Companies	Includes all popular social media platforms which allow users to post and share information for public consumption.	**Detractor** - While efforts can be made to reduce the administrative and financial burdens placed on social media companies, they will likely object to increased regulations of their operations. Consultation with these stakeholders during the policymaking process will be important.
Other Liberal Democracies	States that hold democratic elections and whose population enjoy widespread use of social media	**Allies** - disinformation presents a problem to liberal democracies. While the extent of the problem may vary (i.e., extent to which foreign adversaries are targeting the state), all liberal democracies will likely need to address disinformation in some manner. Given digital information is largely unrestricted by national borders (especially in liberal democracies), the fight against it is improved the more states cooperate to identify and restrict it.
Certain Non Liberal Democratic Nations	States which do not legitimately hold regular democratic	**Detractors** - Non-liberal democracies, such as Russia, Iran, and

	elections and whose interests are aligned against Canada's	Venezuela have been accused of being responsible for creating and propagating disinformation in Canada. As efforts are made to restrict disinformation, these stakeholders will likely seek to innovate tactics to defeat these restrictions.

Programmatic Needs

The PCO will require the cooperation of various ministries and agencies (including PSC, DoJ, DnD, Elections Canada, etc.) in order to draft and implement policy directed at combatting online disinformation. A subsequently created agency will require funding and personnel - including cyber-security and information technology experts. These may be drawn from other ministries and agencies throughout the Public Service. Where insufficient, additional personnel will need to be hired. DoJ will be required to organize a defence for the legislation against an anticipated Charter Challenge.

Recommendation and Implementation

Costed Options

1. CRIMINALIZATION

Make it a criminal offence to knowingly create and/or propagate disinformation with the intention of influencing public opinion and manipulating electoral outcomes.

Pros

This option provides a strong response to acts of disinformation. A similar approach with regards to COVID-19 is already in consideration.[xxiii] By prohibiting disinformation initiatives in criminal law, Canada would be clearly indicating its strong objection to such practices. It would also allow Canada to leverage its law enforcement agencies in combating disinformation campaigns. Freedom of expression would continue to be

protected, including “false” expression (declarative statements which lacks any evidence), so long as that expression failed to meet the specific criteria for harm as defined in the new offence (influencing public opinion with false information to manipulate electoral outcomes). As such, the act of influencing public opinion with false expression, rather than the false expression itself, would be prohibited. The risk of harm to Canadian society posed by disinformation, along with the offence’s targeted approach, would increase its likelihood of surviving a Charter challenge related to 2(b) expression protections.

Cons

Enforcement of the offence may prove difficult - especially with regards to foreign actors. The Government would maintain responsibility for identifying and prosecuting perpetrators of disinformation. The judiciary would continue to ensure the legitimacy of government prosecutions. However, Canadian criminal jurisdiction on the internet is ambiguous and enforcement capabilities against foreign nationals residing outside of Canadian enforcement jurisdictions would be limited. This fact limits the option’s ability to effectively prevent foreign disinformation campaigns designed to influence electoral outcomes, as this harmful information would continue to exist online. The criminalization of expression can also be politically controversial. It is also ultimately uncertain whether the provision would be upheld given a Charter challenge.

Expected Outcomes

The criminalization of disinformation would, for those considering a disinformation campaign, increase the costs of doing so - both domestic and foreign actors. As such, a reduction in the deliberate creation and propagation of disinformation would be expected. Foreign disinformation, however, would likely fail to be significantly reduced. Furthermore, the spreading of disinformation by “innocent” actors would continue unimpeded.

2. INTRODUCE THE “DIGITAL INFORMATION INTEGRITY ACT”

The GoC would create the *Digital Information Integrity Act,* containing within it three primary elements. First, the *Act* would mandate the creation of the DCII headed-by the DIIC. Second, the *Act* would create a new set of regulations defining disinformation and prescribing appropriate responses to it by social media platforms.

As a baseline, “disinformation” would be defined as “misinformation (information that is not supported by evidence) *deliberately* created and/or propagated to influence

Canadian electoral preferences or otherwise cause harm to the Canadian public." The CDII would be responsible for further defining disinformation - including differentiating its varying degrees of seriousness and determining intent.

The new regulations would provide expected responses to disinformation in a tiered format. The tiered format would be designed to offer responses proportional to the seriousness of the disinformation - determined at the discretion of the *Digital Information Integrity Commissioner*. The available responses would be as follows;

1. *Promoting and demoting content (algorithm adjustments)*
2. *Flagging disinformation with a warning*
3. *Removing disinformation*
4. *Banning online accounts sourcing/ propagating disinformation*

Social media platforms would be exclusively responsible for initiating these responses. The DIIC would be responsible for identifying and reporting disinformation to them, while recommending a response. While the DIIC would maintain the formal authority to require a specific response, they would be mandated to exercise restraint in the specificity of their recommendations. The DIIC would also possess the authority to issue charges against social media platforms which fail to abide by their recommendation. Recognizing the sensitive nature of suppressing certain expressions, the CDII would be required to submit public quarterly reviews to Parliament. These reviews would outline the *Commission*'s decision-making process - including examples of digital expression it designated as disinformation and its recommended responses. The quarterly review would help ensure both public and Parliamentary oversight over the CDII's operations.

The *Digital Information Integrity Act* would also require that social media platforms identify and respond to disinformation independently, as regulated in the *Act* and in cooperation with the Commission of Digital Information Integrity - as able. Social media platforms would not be subject to penalties in relation to their responses (or non-response) for self-identified disinformation - nor would they be subject to penalties for failing to identify disinformation. The CDII would ultimately maintain the responsibility for identifying disinformation and ensuring it is appropriately addressed. The CDII would operate both through independent investigation and on a complaints based basis.

Pros

The *Digital Information Integrity Act* would allow the GoC to increase its ability to combat disinformation without invoking criminal law. It would also leverage existing expertise possessed by social media platforms, increasing the *Act's* effectiveness. It is also expected to not require social media platforms to perform any activities not already performed by them, reducing the *Act's* intrusiveness against them. Given that digital disinformation is primarily propagated on social media platforms, this policy would be addressing the issue as close to its source as possible. The CDII's effectiveness will likely be reliant on its available resources - allowing the GoC to actively adjust *The Commission's* funding proportional to the active threat of disinformation. Examples include increased funding throughout and around election periods, for example.

Cons

Defining disinformation will likely provide for some controversy and invoke Canadian Charter of Rights and Freedoms s.2(b) Freedom of Expression concerns. The CDII will be obligated to define disinformation with considerable specificity, to avoid unjustified (non-compliant with s.1 Charter "reasonable limits") infringements on Freedom of Expression. This required specificity may limit the definition's ability to encapsulate all instances of disinformation and limit the effectiveness of the CDII. The vast quantity of digital information across social media platforms will also present an incredible challenge to the CDII in its efforts to monitor and identify disinformation online. The CDII will either require significant funding, both for personnel and technological advancements, or accept limited functionality. Finally, social media platforms will likely resist government regulation of their operations. The GoC should work with these platforms to ensure its regulations are consistent with the capabilities of the social media platforms.

Expected Outcomes

A decrease in the amount of disinformation seen by Canadians on social media platforms is expected. This includes disinformation designed to suppress Canadians' ability to vote. While unidentified disinformation will continue to propagate until identified, the newly created CDII will increase the GoC's ability to identify it. While this option does little to directly target the individuals responsible for creating and sharing disinformation, it does reduce their ability to engage in the practice. A Charter challenge, on the grounds that the *Act* infringed on Canadians' S.2(b) Charter Rights, is expected.

The Government will be required to demonstrate that the *Act*, and its efforts to combat disinformation, represents a justified breach (s.1) of Canadian's Charter Rights and Freedoms (*Oakes test*).

3. STATUS QUO

Continue moving forward with Canada's existing policies; the *Elections Modernization Act (2019)* and the *CSE Act (2019).*

Pros

This option allows the government to continue working against disinformation without having to pursue any additional efforts. Maintaining the status quo would allow the government to avoid expending the resources required to develop and enforce new criminal laws and/or develop a new agency and regulations. It would also avoid the political risks associated with enacting restrictions on expression and increased regulation of private online social media companies.

Cons

These options would likely fail to adequately address the disinformation problem. The existing regulations are limited to election candidate-specific information and fail to address disinformation related to policy issues. [xxiv] Furthermore, the existing policy prohibits the selling of online advertising to non-Canadians only during election times and requires that online platforms maintain a digital registry. While the *Elections Modernization Act* focuses on online advertising, it does nothing to address all other sources of information (and information sharing) via online social media. The status quo is limited by its focus on elections and election-specific disinformation and fails to address the fact that disinformation persists throughout the year. It also fails to account for disinformation related to policy issues which, by extension, can influence electoral decision-making.

Expected Outcomes

Continued reduction in online advertising on social media platforms by non-Canadians during election periods. Little change to the spread of disinformation, especially that which focuses on policy issues, via social media platforms is expected.

Recommendation

This review proposes moving forward with **option two**. The implementation of the *Digital Information Integrity Act* allows the GoC to increase its ability to combat disinformation in Canada, while limiting its infringements on freedom of expression. Option two would include the creation of the *Commission of Digital Information Integrity*, an independent agency responsible for assisting in the identification of disinformation and regulations mandating expected responses from social media platforms for when it is detected. These regulations would provide for tiered options by the platforms - allowing for a flexible response proportionate to the nature of the disinformation. Government intervention would be limited to instances where social media platforms fail to meet the regulations' requirements and would be directed against the platforms directly (in the form of punitive measures - i.e. fines). This decision-making process, with regards to declaring expression as "disinformation," will be overseen by Parliament, by form of quarterly reviews. While existing government agencies, including the CSE, may be suitable for performing these responsibilities, their formal connection to Cabinet may raise concerns as to their impartiality. The CDII's direct connection to Parliament, rather than Cabinet, seeks to address these concerns. Ultimately, a reduction in the amount of disinformation seen by Canadian citizens - particularly for those not actively seeking it - is expected. Correspondingly, a reduction in the risk of Canadian opinion and voter preferences being unduly affected by disinformation is expected, as well.

Communication Strategies

Given the sensitive nature of this proposal, the government should emphasize the potential harm caused by disinformation *against Canadian interests*. Specific reference to the fact that significant portions of disinformation originate from foreign sources may prove beneficial to encouraging public support. Simultaneously, the GOC must reassure the Canadian public that the importance of Charter freedoms is understood and respected. This effort should be supported by citing disinformation's concise definition, the quarterly review process (Parliamentary oversight), and the CDII's independent status (non-partisan).

Timeline with Key Performance Indicators

All components are targeted to be complete in time for the next federal election (expected October 2023 or sooner).

Drafting	Adoption	Implementation
The PCO, in cooperation with the DoJ, would be responsible for drafting the *Act*. A consultation period should be expected to allow for input from relevant stakeholders (social media companies, civil liberties groups, cyber-security experts, etc.).	Parliament of Canada will need to pass the *Digital Information Integrity Bill*. The Government should expect resistance from opposition parties - especially the CPC, who will likely emphasize Freedom of Expression concerns.	1. Once enacted, the PCO will need to establish the CDII and Parliament will need to appoint a DIIC. 2. The CDII will formalize its internal procedures and begin identifying disinformation and reporting it to the relevant social media companies. 3. It will provide quarterly reports to Parliament for review, as scheduled.

Annexes

A. ELECTIONS MODERNIZATION ACT, BILL C-76

Online platforms that are subject to requirements

325.1 (1) This section and section 325.2 apply to any online platform that, in the 12 months before the first day of the pre-election period, in the case of the publication on the platform of a partisan advertising message, or the 12 months before the first day of the election period, in the case of the publication on the platform of an election advertising message, was visited or used by Internet users in Canada an average of at least the following numbers of times per month:

(a) 3,000,000 times, if the content of the online platform is available mainly in English;

(b) 1,000,000 times, if the content of the online platform is available mainly in French; or

(c) 100,000 times, if the content of the online platform is available mainly in a language other than English or French.

Registry of partisan advertising messages and election advertising messages

(2) The owner or operator of an online platform that sells, directly or indirectly, advertising space to the following persons and groups shall publish on the platform a registry of the persons' and groups' partisan advertising messages and election advertising messages published on the platform during that period:

(a) a registered party or eligible party;

(b) a registered association;

(c) a nomination contestant;

(d) a potential candidate or a candidate; or

(e) a third party that is required to register under subsection 349.6(1) or 353(1).

Information to be included in registry

(3) The registry referred to in subsection (2) shall include the following:

(a) an electronic copy of each partisan advertising message and each election advertising message published on the platform; and

(b) for each advertising message referred to in paragraph (a), the name of the person who authorized the advertising message's publication on the platform, namely

(i) a registered agent of the registered party or eligible party, in the case of an advertising message whose publication was requested by a registered party or eligible party,

(ii) the financial agent of the registered association, in the case of an advertising message whose publication was requested by a registered association,

(iii) the financial agent of the nomination contestant, in the case of an advertising message whose publication was requested by a nomination contestant,

(iv) the official agent of the potential candidate or candidate, in the case of an advertising message whose publication was requested by a potential candidate or a candidate, and

(v) the financial agent of the registered third party, in the case of an advertising message whose publication was requested by a registered third party.

B. COMMUNICATIONS SECURITY ESTABLISHMENT ACT (BILL C-59)

Cybersecurity and information assurance

17 The cybersecurity and information assurance aspect of the Establishment's mandate is to:

(a) provide advice, guidance and services to help protect

(i) federal institutions' electronic information and information infrastructures, and

(ii) electronic information and information infrastructures designated under subsection 21(1) as being of importance to the Government of Canada; and

(b) acquire, use and analyse information from the global information infrastructure or from other sources in order to provide such advice, guidance and services.

Defensive cyber operations

18 The defensive cyber operations aspect of the Establishment's mandate is to carry out activities on or through the global information infrastructure to help protect

(a) federal institutions' electronic information and information infrastructures; and

(b) electronic information and information infrastructures designated under subsection 21(1) as being of importance to the Government of Canada.

References

[i] Canadian Centre for Cyber Security. 2019. EXECUTIVE SUMMARY. https://cyber.gc.ca/en/guidance/executive-summary-1.

[ii] Rocha, R. and Yates, J., 2019. Twitter Trolls Stoked Debates About Immigrants And Pipelines In Canada, Data Show | CBC News. [online] CBC News. Available at: https://www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.5014750; Nemr, C. and Gangware, W., 2020. Weapons Of Mass Distraction: Foreign State-Sponsored Disinformation In The Digital Age. [online] Park Advisors. https://www.state.gov/wp-content/uploads/2019/05/Weapons-of Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

[iii] Ibid.

[iv] Canadian Centre for Cyber Security. 2019. EXECUTIVE SUMMARY. https://cyber.gc.ca/en/guidance/executive-summary-1.

[v] Nemr, C. and Gangware, W., 2020. Weapons Of Mass Distraction: Foreign State-Sponsored Disinformation In The Digital Age. [online] *Park Advisors*. https://www.state.gov/wp content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the Digital-Age.pdf, 4.

[vi] Ibid.

[vii] Pariona, Amber. "Countries Where People Spend The Most Time Online". *World Atlas*, 25 April 2017, https://www.worldatlas.com/articles/top-countries-which-spend-the-greatest-amount-of-time-online.html [viii] Centre of International Governance Innovation, 2020. Governing Cyber Security in Canada, Australia and The United States. [online] Waterloo, ON: *Centre of International Governance Innovation*. Available at: https://www.cigionline.org/sites/default/files/documents/SERENE-RISCweb.pdf [ix] Government of Canada, 2013. *Action Plan 2010-2015 For Canada's Cyber Security Strategy*. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf. [x] *Communications Security Establishment Act, Statutes of Canada* 2019, c.19. https://laws lois.justice.gc.ca/eng/acts/C-35.3/page-1.html.

[xi] Office of the Director of National Intelligence, 2017. Assessing Russian Activities And Intentions In Recent US Elections. *Intelligence Community Assessment*. Available at: <https://assets.documentcloud.org/documents/3719492/Read-the-declassified-rep

ort-on-Russian.pdf, 1,4.

[xii] Communications Security Establishment. 2019. "2019 Update: Cyber Threats To Canada's Democratic Process". Government of Canada. https://cyber.gc.ca/sites/default/files/publications/tdp-2019- report_e.pdf.

[xiii] Associated Press, 2020. *Russia Used English-Language Sites To Spread Covid-19 Disinformation, US Officials Say.* https://www.theguardian.com/us-news/2020/jul/28/russia-covid-19-disinformation websites-us-intelligence.

[xiv] Rocha, R. and Yates, J., 2019. Twitter Trolls Stoked Debates About Immigrants And Pipelines In Canada, Data Show | CBC News. [online] CBC News. Available at: https://www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.5014750.

[xv] Associated Press, 2020. Russia Used English-Language Sites To Spread Covid-19 Disinformation, US Officials Say. https://www.theguardian.com/us-news/2020/jul/28/russia-covid-19-disinformation websites-us-intelligence.

[xvi] Leger. 2020. "In The News: COVID-19 Symptoms And Vaccines". Weekly Survey. The Canadian Press. https://leger360.com/wp-content/uploads/2020/10/Legers-Weekly-Survey-October -13th 2020.pdf?x43558.

[xvii] Carleton Newsroom. 2020. "New Carleton Study Finds COVID—19 Conspiracies And Misinformation Spreading Online." https://newsroom.carleton.ca/2020/new-carleton-study-finds-covid 19-conspiracies-and-misinformation-spreading-online/.

[xviii] Ipsos Public Affairs, CIGI-Ipsos Global Survey: Internet Security & Trust 2019 Part 3: Social Media, Fake News & Algorithms (2019), https://perma.cc/X5RX-PL76.

[xix] DiResta, Renée. 2020. “The Supply of Disinformation Will Soon Be Infinite.” *The Atlantic*, https://www.theatlantic.com/ideas/archive/2020/09/future-propaganda-will-be-computer generated/616400/.

[xx] Canadian Centre for Cyber Security. 2020. "National Cyber Threat Assessment." Government of Canada. https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2020

[xxi] McKeen, Alex. 2020. "Why Canada Appears To Be One Of The Top Spreaders Of Russian Disinformation Online". *Toronto Star*, 2020.

https://www.thestar.com/news/canada/2020/10/25/why canada-appears-to-be-one-of-the-top-spreaders-of-russian-disinformation-online.html.

[xxii] Cabinet Directive on the Critical Election Incident Public Protocol https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election incident-public-protocol/cabinet.html.

[xxiii] Thompson, Elizabeth. 2020. "Federal Government Open To New Law To Fight Pandemic Misinformation." *CBC News*. https://www.cbc.ca/news/politics/covid-misinformation-disinformation law-1.5532325.

[xxiv] Canada Elections Act § 319.

