THE SCHOOL
OF PUBLIC POLICY

**MASTER OF PUBLIC POLICY
CAPSTONE PROJECT**

**Campaigns of Disinformation: Modern Warfare, Electoral Interference, and Canada's
Security Environment**

Submitted by:

Devin Tuttle

Approved by Supervisor:

Jean-Sébastien Rioux

Submitted in fulfillment of the requirements of PPOL 623 and completion of the requirements
for the Master of Public Policy degree

THE SCHOOL OF PUBLIC POLICY

Capstone Approval Page

The undersigned, being the Capstone Project Supervisor, declares that

Devin Tuttle

has successfully completed the Capstone Project within the

Capstone Course PPOL 623 A&B

Jean-Sébastien Rioux, Ph.D.

(Supervisor)

Signature

(Supervisor's signature)

July 30, 2019

(Date)

UNIVERSITY OF
CALGARY

THE SCHOOL OF PUBLIC POLICY

Acknowledgements

I would like to thank Dr. Jean Sebastien Rioux for his guidance and support in completing this capstone. I would also like to thank my friends and family for having to endure my endless rants throughout this process.

THE SCHOOL OF PUBLIC POLICY

Table of Contents

Introduction.....	1
Literature Review	2
<i>Modern Warfare and State Interference.....</i>	<i>2</i>
<i>Political Communication.....</i>	<i>6</i>
<i>The Information Age.....</i>	<i>8</i>
<i>Political Mobilization</i>	<i>11</i>
A Hostile Environment	14
<i>Russia.....</i>	<i>15</i>
<i>China.....</i>	<i>21</i>
Canada as a Target	29
Actors and Institutions at Risk	32
<i>Elections.....</i>	<i>33</i>
<i>Parties and Politicians.....</i>	<i>34</i>
<i>Voters</i>	<i>36</i>
Canadian Safeguards to Democracy	38
<i>Infrastructure Protection.....</i>	<i>38</i>
<i>Information Security</i>	<i>39</i>
<i>Prohibitive Mechanisms</i>	<i>41</i>
<i>Detection Mechanisms</i>	<i>42</i>
<i>Social Media Regulations and Advertising Restrictions</i>	<i>43</i>
<i>Voter Resiliency.....</i>	<i>47</i>
What's the Risk?	48
Modern Problems Require Modern Solutions	54
<i>Policy Recommendation</i>	<i>54</i>
Conclusion	60
References.....	62

THE SCHOOL OF PUBLIC POLICY

Capstone Executive Summary

This capstone develops a risk assessment of Canada's democratic institutions as it relates to potential foreign interference in the 2019 federal election, determining what factors should be of most concern for Canadian policymakers charged with defending Canada's democratic infrastructure from foreign interference.

Through a literature review of non-linear warfare, social media networks and algorithms, I discuss the technological and behavioural factors that have contributed to the vulnerabilities in Western states, namely the advent of a changing media and information environment. I argue that changes in technological and information accessibility have allowed states who have been traditionally disadvantaged in terms of warfare capabilities to overcome these asymmetries.

I go on to explore cases of recent interferences in domestic by Russia and China, providing a comprehensive overview of each state's motivations for engaging in non-linear warfare: historical grievances against the Liberal International Order, changing tactics in modern warfare, and interference strategies in foreign elections. Following these case studies, I then assess why Canada is viewed as a target from the perspectives of both Russia and China, and the different motivations of these states in intervening in Canada.

Following an assessment of Canada's security environment as it relates to election interference, I evaluate the safeguards Canada has put in place to defend against attacks to its democratic institutions. I devise a risk matrix that codifies the threats Canada will likely face during the pre-election and election period leading up to the 2019 federal election.

This capstone concludes with a recommendation that urges Canada to institute a National Centre for Strategic Communications and Digital Democracy that would develop cohesive strategies to safeguard democracy in Canada against foreign influence campaigns, cyber-attacks, and disinformation.

Introduction

The Maginot Line was constructed following World War I along the French-German border to deter a future German invasion into France. Based on previous warfare strategies, the Maginot Line was thought to be impenetrable; however, this ultimately proved to be a false sense of security. While the French were focused on defending themselves against WWI tactics, the Germans developed a new mode of warfare – Blitzkrieg – making the Maginot Line a relic, ultimately resulting in a Nazi occupation of France. This should be the fear for national security policy makers in the 21st century: developing strategies to defend against obsolete warfare tactics. Recent events such as the 2016 US presidential election or the 2018 Taiwanese municipal elections demonstrated the capabilities of hostile foreign actors to influence the outcomes of democratic processes (DiResta 2018a). Foreign actors, especially those outside of the Liberal International Order¹, increasingly employ tactics to influence another country's democratic institutions where the goal is to achieve an outcome that serves its domestic interests. Thus, I argue, Western democracies are currently in crisis as foreign adversaries can effectively infiltrate the decision-making process of sovereign nations, where effective counter-measures are only instituted *following* an attack.

Looking ahead to our own environment, there must be concern at the highest levels as to whether Canada is properly equipped and prepared to defend the integrity of the 2019 federal election against foreign intervention. This question will be answered through a carefully designed risk assessment of Canada's position in the international environment and the government's existing strategies to deter methods of "non-linear warfare," a term that will be

¹ The application of liberal ideas to the organization and practice of international relations, under the form of the promotion of universal human rights, through the patronage of the United Nations, where sovereign states can relate to one another (Charvet and Kaczynska-Nay 2008, 3).

defined further in subsequent sections but which essentially means the employment of all available resources to achieve a strategic objective. Through a qualitative evaluation of interested actors, potential strategies, and objectives as well as an assessment of current policies and regulations, I will illustrate possible scenarios that could leave Canada susceptible to foreign intervention in the 2019 federal election.

Given the result, it is necessary to revamp Canada's current strategies, regulations, and policies to counteract a potential influence campaign. Rather than designing strategies to defend against previous influence campaigns, Canada, and other Liberal democratic states, must be proactive in their policy development, focusing on new and future iterations in [non-linear] warfare. If Canada and other Western Liberal states continue to deploy strategies that primarily focus on previous iterations of foreign interference, the result may be as damaging as the Maginot line was to France. Hostile actors are demonstrating a willingness to push back against a rules-based system, which should indicate a willingness to use tactics outside of traditional warfare. Much like the development of Blitzkrieg was for Nazi Germany, non-linear warfare has been just as useful for states outside of the Liberal International Order to overcome an asymmetric power balance. Strategies of hybrid warfare caught Western policy makers off guard in the past few years; if Canada expects to maintain order in its democratic systems, it must not fall victim to these same mistakes again.

Literature Review

Modern Warfare and State Interference

In February of 2013, Russian General and Chief of the General Staff Valery Gerasimov published an article in Russia's *Military-Industrial Kurier*, titled "The Value of Science is in the Foresight." What has become to be known as *The Gerasimov Doctrine* sets forth a series of

concepts in which Western analysts have defined as “Hybrid Warfare” (Bartles 2016, 30). Gerasimov articulates a strategy of warfare, not dissimilar from the Soviet era strategies of leveraging all means of national power to achieve a desired end; however, Gerasimov’s strategy is distinct in how power is exerted, with a heavy reliance on non-military measures as opposed to traditional military tactics (Bartles 2016, 34). While subsequent Russian behaviour in Ukraine, Britain, and the United States have demonstrated Gerasimov’s concept, scholars are divided as to whether these actions accurately represents the definition of Hybrid Warfare. Schnauffer II (2017), argues that Russian military strategy should instead be defined as “Non-Linear Warfare (NLW),” to include information, cyber, economic, political, and social means in their strategy, not simply the application of criminal, conventional, irregular, and terrorist measures (Schnauffer II 2017, 19).

However, both Gerasimov doctrine of Russian warfare tactics and Schnauffer’s theory of non-linear warfare are not all that distinct from the United States doctrine of “Unconventional Warfare” whose conduct incorporates supporting a resistance movement or insurgency to “coerce, disrupt, or overthrow a government or occupying power through or with an underground, auxiliary, and guerilla force in a denied area” (Joint Publication 3-05 2014, II-9). While these definitions are distinct, they share many of the same key concepts. Most notably for the context of this study is *the use of all available resources, both military and non-military alike, to achieve a particular objective* (U.S. Department of the Army 2008, 6-1-2; McCulloh and Johnson 2013, 16; Chivvis 2017, 3-4). This includes the use of information, psychological, and cyber warfare tactics, which are largely described as the new generation of warfare (Thornton 2015, 42; Hoffman 2007, 28; Radin 2017, 5-9).

Hybrid Warfare was originally understood as the application of criminal, conventional, irregular, and terrorist measures within a given time and battlespace to achieve an advantage or political objective (Hoffman 2007, 29). Hoffman (2007) defined this as the future of warfare in terms of hybrid threats, arguing that future conflict will be multi-modal or multivariate rather than a singular application of tactics. While Hoffman was correct in his view of the future of warfare being multi-modal, hybrid warfare has expanded to include the usage of information, cyber, economic, and social means to achieve an objective, or more generally the usage of all available resources to the state (Schnauffer II 2017, 19; Chivvis 2017, 4; McCulloh and Johnson 2013, 16). Hereafter, hybrid warfare will now be referred to as non-linear warfare.

If all warfare is inherently political, where Clausewitz defined warfare as the continuation of politics by other means (Clausewitz 1832, 24), then non-linear warfare is no different since the goal is to influence the domestic politics of targeted countries, intending to destabilize a functional state and polarize its society (Radin 2017, 5-6). Conscious of this, an adversarial state is no longer exclusively targeting military personnel; rather the targeted population is extended to include civilians. As in all wars, the goal is to force an enemy to submit to your will; rather than employing solely conventional kinetic tactics, non-linear warfare utilizes strategies of propaganda and cyber-attacks to coerce an opponent (Radin 2017, 6; Schnauffer II 2017, 21; Thornton 2015, 41-42). In a similar manner as focusing on non-military targets, those conducting information or cyber-attacks are also increasingly non-military actors. For instance, China employs a series of independent contractors known as the “50 Cent” Army to conduct its online influence campaigns abroad. This action of using non-military personal to conduct a warfare campaign creates plausible deniability for the aggressor, leaving the defending state without just cause for conventional retaliation (Thornton 2015, 46; Radin 2017, 7). Instead of simply

coercing a population to believe certain propaganda, non-linear warfare employs a tactic of confusion and disinformation to sow the seeds of doubt in the enemy (Pomerantsev 2015, 46; Thornton 2015, 43-45).

As it relates to electoral interference, non-linear warfare campaigns attempt to foster a “post-truth” body politic. As more sources of information (some of which may not be credible) flood the public’s consciousness they begin to form various interpretations of the same event; however, due to a lack of a unifying premise from which deliberation can occur (a universal appeal to reason) peer communication becomes fractured. In this regard, even credible information becomes subjective because there is no longer a common standard to deliberate from. As post-truth radiates throughout society, the electorate becomes is confused and can longer trust actors and institutions within their regime (Lanoszka 2016, 180). These strategies have become increasingly useful due to recent developments in information and communication technologies, whereby the spatial, temporal, and information gaps between populations have reduced significantly.

The changing nature of warfare is largely two-fold. First, in developing a hybrid strategy, less powerful states can counter the conventional strength employed by Western states, thus attempting to reverse an asymmetry of power. In addition, the constitutive basis for enacting war is now blurred, where an act of war is no longer clearly defined (Banasik 2016, 40; Schnauffer 2017, 22; McCulloh and Johnson 2013, 7). From here, Western states, especially those who are members of NATO, can no longer readily defend themselves (or their allies) from these tactics because the lines between war and peace and combatant and non-combatant are no longer clear.

Schnauffer (2017, 23) posits that a successful non-linear warfare campaign will result in one of the following outcomes:

1. A state no longer has the political will power to engage and will leave the aggressor alone;
2. Alliances and conventional forces are no longer tenable to the point where they could be defeated in a conventional setting;
3. A state will submit to the aggressor from the threat of force;
4. A state becomes indifferent to their aggressor and allows them to continue without obstruction.

While the motivation and tactics for all states varies, the ultimate desire of a state is to navigate freely in the international community, able to conduct their operations as they please.

Political Communication

Influencing elections requires a necessary understanding of how information is disseminated and how the electorate will receive that information. This follows a three-part process of *agenda-setting*, *framing*, and *priming*. **Agenda-setting** refers to the construction of narratives through the discourse of elites and media, where the saliency of a narrative can be correlated to the emphasis placed on it by the elites and the media (McCombs 1972, 179).

Framing effects provide context to an event, selected through a process of exclusion, to establish a causal interpretation, where the characterization of an event impacts the public's interpretation (Kahneman and Tversky 1984, 343). Frames can be fabricated internally, through journalistic bias or through the values or beliefs of an institution, or, they can be constructed externally, through elite pressure on an institution or a salient social movement (Entman and Rojecki 1993, 169-172). Take for example the Conservative's attack ads on Justin Trudeau leading up to the 2015 election, where the Conservative party framed Trudeau as "just not ready"

to be Prime Minister. This frame was constructed internally by the Conservatives and then transmitted to the public through a nexus of media channels. **Priming** of public opinion can be viewed as an extension of the agenda setting process, whereby an increase in the saliency of an issue will shape an individual's opinion of that issue. As an individual's exposure to an event increases their time spent focusing on that event will increase alongside (Higgins and King 1982, 39).

Organizations must be conscious of how the public will respond to a frame; will their frame create a positive or negative effect? Upon reflection, individuals often revert to previous knowledge when presented with new information. Defined as "chronic accessibility", individuals rely on their encapsulated belief systems as they attempt to decipher an event (Shen 2004, 128). Understanding the process of individual decision making enables actors and institutions to construct narratives that would have the greatest potential to influence. On aggregate those who are least sophisticated with strong biases will be most influenced by single coverage of an event, where influence is enhanced if narratives and frames focus on emotional appeals (Hersh 2015 128; Marland 2017, 151). With this mind, a frame is most effective if delivered in a negative context, where negative information will resonate greatest with the public, becoming part of their chronically accessible information (Kahneman and Tversky 1984, 345). As political events are increasingly framed in a negative context, the public becomes susceptible to cynicism, resulting in a political malaise, contributing to decreased trust in institutions alongside peer capacity to elect effective government (Hersh 2015, 112; Fredkin and Kenny 2012, 179).

The Information Age

In the Information Age, successful campaigns have embraced the usage of “Big Data” analysis, namely targeted behavioral analytics (Kreiss 2016, 127-128). While data has always been a fixture in influencing electorates, the internet has fundamentally transformed accessibility and significantly reduced the cost of acquisition (Finlay 2014, 73-75). These transformations provide organizations with a capability to process deep insights into individual belief systems and preferences. Advancements to machine learning algorithms and analytics have allowed developers to process user-generated unstructured data, where all digital interactions can be transcribed into data points (Burke 2017, 43-58; Tufekci 2014). Recent advancements to analytics in conjunction with the advent of social media usage enables organizations to accurately model individual interactions, developing real-time analyses of human behavior. As organizations develop increasingly accurate behavioural models, their potential to influence the persuadable voter –those who are undecided without strong values or bias– increases continuously.

To briefly describe the process, organizations utilize regression modelling to attempt to describe the relationship between the dependent variable and the independent explanatory variable – and in relation to electoral persuasion, what variables impact voter mobilization. A quintessential example is the algorithms developed by Michael Kosinski. Using Facebook’s analytics to mine user-generated data, organizations can model individual behaviour, generating accurate psychometric profiles in coordination with the “Big 5” personality traits² (Kosinski, Stillwell, and Graepel 2013, 5802-5805). These are then used to create predictive models, aimed

² Measuring psychophysical differences in individuals based on perceived personalities traits; these being the “Big Five” as defined as: Introversion/Extroversion (the level of social agreeableness), Neuroticism (levels of security), Agreeableness (compliance, cooperative), Consciousness (an individual’s willingness to achieve), Intelligence (imaginative, cultured, open-mindedness) (Burke 2017).

at triggering emotive responses in the electorate. *i.e.*, what emotional trigger (*Independent variable*) will cause a reaction in the persuadable voter (*Dependent variable*), with the goal being *what factor contributes to generate an increased or decreased mobilization outcome*. When applied to traditional qualitative methods of electoral analytics, these algorithms further distinguish the fault lines in populations; enabling organizations to triage information to population subsets therefore reaffirming that population's bias (Gibson and Ward 2012, 65; Albright 2016a). As user rates of social network sites and information technologies increase, so will the availability of user generated data. As more data is generated on individual behavioural preferences, the possibility of effective persuasion through predictive analytical techniques will also increase.

While social media provides the bulk of user generated unstructured data, leading to improvement of individual modelling, the greater desire for organizations is developing *network centric models*, understanding the relationships between groups and where influence occurs (Finlay 2014, 186-193). If organizations can monitor the flow of information, their capacity to effectively influence an electorate will increase alongside. Observing the rise in “fake news” sites such as RT, InfoWars, or China Daily and the prominence of disinformation posts on social media sites, organizations utilize their reach to microtarget the user base with deliberately “triggering” advertisements. Propaganda or “fake news” sites do not have effective safeguards to protect its user's data, where sites are susceptible to in depth monitoring and potential hacking, leading to the capture and sale of individual's information (Albright 2016a). While these sites have in-house data collection, there are additional behavioral tracking algorithms on these sites derived from Alphabet, Amazon, Facebook, and Twitter analytics. Sites that contain a “like” or “share” function monitor activity and transcribe personal data back to said site to create targeted

advertisements (Albright 2016a). As data collection increases more insight is known about individual behavior, informing organizations of potential psychological triggers that would capture the attention of their targeted user base. When predictive analytics are added to the equation, content is increasingly tailored to direct individual attention towards disinformation. Actors in the international environment have an incentive to use this data for their personal convictions, where the potential for influence increases alongside the availability of data. Eventually the average population falls victim to a vicious feedback loop that results in homophilic populations and users that are addicted to content produced entirely to manipulate their decisions.

The ability to quantify foundations of voter's belief systems, emotional empathy, and networks generates an increased effectiveness of non-linear warfare tactics, namely bots and trolls. **Bots** are algorithmic programs designed to conduct tasks online, including scraping data, mimicking human users online, and producing consistent streams of information (Woolley and Howard 2016, 4885). **Trolls** are humans acting online, spreading disinformation or deliberately inducing visceral responses from their targeted population (Schnauffer II 2017, 27). Utilizing troves of individual data, organizations construct algorithms to predict when and where a bot, botnet (a series of bots acting in coordination), or trolls would have the greatest effect to manipulate individuals, targeting their cognitive vulnerabilities (DiResta, 2018). Bots represent a substantial population of social media accounts, where they leverage their network connectivity to spread disinformation via coordinated actions of posts. Due to their network centrality, their posts trend more often, resulting in a vast swarm of disinformation beyond their direct node connectivity (Woolley and Howard 2016, 4886; DiResta 2017). Comparatively, peer interaction for trolls are both in the form of posts and comments. Trolls attempt to sow chaos, doubt, and

fear into the electorate, where their comments are often highly divisive, spreading disinformation and stoking identity based grievances (Schnauffer II 2017, 27; DiResta 2018b, 14). Moreover, bots and trolls also attempt to recruit and manipulate activists, employing sophisticated individual modelling algorithms they can provoke individuals to parlay their digital discord into real world protest (DiResta 2017).

Adversarial actors have recently deployed a tool known as **Deepfakes** to increase the potential for voter manipulation. Deepfakes are realistic manipulations of audio or visual recordings designed to impersonate an individual (Chesney and Citron 2019). These recordings utilize machine learning processes, such as neural nets to infer the speech and movement patterns of individuals, where these algorithms can improve themselves through generative adversarial networks. This process pits algorithms against each other, where one machine learning model creates the “deepfake” and the other attempts to decipher the legitimacy of the video/image, where it is unable to decipher whether the visual is real or not (Porup 2019). In a similar vein to bots and trolls, this tactic improves as the availability of data increases. Moreover, as these technologies become more prevalent, it will become increasingly difficult to rely on traditional means of verification – our eyes. These voter manipulation technologies have introduced a new precedent: believe nothing of what you hear and half of what you see.

Political Mobilization

While an understanding of human behaviour and an integrated analytics strategy generate a potential to influence the hearts and minds of citizens, the effectiveness of a campaign is dependent on its capacity to mobilize an electorate towards a unifying action. I utilize a variation of arguments from social movement theory and information technologies to articulate the receptiveness of an electorate during campaigns.

Carty (2011, 13) argues that movements are most effective when framed around a unique political dimension, where collectivization of social and political grievances are a requisite condition for mobilization. Marginalized populations whose grievances were once a minute factor, due to an isolated population are now reduced thanks to the information age. New technologies have contributed to a significant decrease in the barriers for organizations to engage with the electorate; decentralizing the hierarchical information structure in favour of horizontal structure that is more conducive for collective engagement (Castels 2001, 138-140). This decentralization contributes to an expansion of collective identities, where previously isolated population subsets now possess the tools to form communities through a digital medium. Tilly (2006) reiterates the notion of collective behaviour, arguing that effective social movements require three elements (Tilly 2006, 182-183):

1. A sustained campaign of claim making, there must be some grievance that invokes mobilization that persists over a lengthy period;
2. Numerous public performances and the creation of coalitions, groups must display their grievances in the public sphere;
3. Repeated public displays of Worthiness, Unity, Numbers, and Commitment or WUNC. Together, these illustrate a variety of claims a group can invoke: an *identity* claim of “us” versus “them”, a *standing* claim where one’s grievance is experienced by others, and a *program* claim of specific support for the groups proposed action against their grievance.

Given the interconnectedness afforded by the online environment, organizations can enhance their administrative abilities alongside the scale and scope of their operations.

We must also be cognisant of the regime and political opportunity structure of a movement within a given state. Where the type of regime establishes the parameters of available actions to a movement, limiting the claims and performances they can take, who can articulate a claim and who can be the object of that claim, and what grievance a claim is centered around (Tilly 2006, 186; Tilly and Tarrow 2005, 92-94). The governing regime also partially determines the political opportunity structure that effect the success of a movement, which are as follows: a multiplicity of centers of power within the regime, the openness of the regime to new political actors, the instability of political alignments, the availability of potential coalitions, and the repression of claims by the regime (Tilly 2006, 187). Within democratic systems, discourse is rooted in the subjectivity of the claimant, such that grievances can be made based on marginalization from any supposed privileged groups. Due to a foundation of liberal principles, movements have significant potential openings in power structures within Western states. Thus, the effectiveness of mobilization becomes easier as the internet decentralizes information structures and allows minority populations to collectivize online.

Mobilization also requires a significant understanding of the psychological underpinnings that encompass an electorate. Using an understanding of framing analysis, we can further understand the grievances that enable mobilization. Framing analysis refers to the manifestation of collective identity through the present narrative, where cultural groups form their collective identity through a preordained socialization process (Gamson 1992, 31-32). How groups utilize resources within their respective regime is not enough to understand the occurrence of social movements, rather there must be an exploration of the narratives that enabled collectivization. Growing theories within behavioural economics posits that individuals should no longer be perceived as *Homo Economicus*, rather we are *Homo Sapiens*: irrational with normative

aspirations (Thaler and Sunstein 2008, 55). It is this understanding that necessitates alternative approaches to classical theories, where an appeal to a sense of identity enables group mobilization. Social movement organizers need to frame issues that will resonate with specific cultural narratives. David Snow argues that when articulated as “Injustice Frames,” an appeal to moral principles, social mobilization will have a greater resonance with societal actors (Snow *et al* 1986, 467). As it relates to Russian interference in the 2016 American presidential election, Russian actors stoked the grievances of perceived persecuted communities. Whether it be the progressive communities and the Black Lives Matter protests or conservative communities and the formation of the “alt-right,” each organized around a sense of injustice created by the current and historical regime. Social movements should utilize the scapegoating of outsider factions, propose solutions to contending problems, generate appeals to third parties, and insist on a call to arms to generate a tangible plan of attack. If this precedent is compounded with a frame around moral principles, a sense of longevity, and urgency, the movement would be in a convincing position to capitalize on their environment (Snow *et al* 1986, 474-475; Tilly and Tarrow 2005, 74-75).

A Hostile Environment

The Post-Cold War Liberal International Order is under threat. Recent actions by hostile states have illustrated a desire to push back against a perceived liberal hegemony, attempting to undermine stability both within these states and the larger international order. While the goals of states differ, those whose values do not align with liberal principles share a fundamental commonality: a desire to operate freely within their sphere of influence, absent of the constraints imposed by liberal rules-based institutions. This section will categorize who these actors are, while attempting to clarify their motivations and reasoning behind actions. I will also clearly

identify the strategies and tools available to each state. Following this, there must be a discussion as to Canada's position within this hostile environment, making a case as to why the threat of electoral interference subsists.

Russia

Observing events in former Soviet satellite states (Estonia 2007, Georgia 2008, Ukraine 2004 & 2014) and established Western democracies (United Kingdom 2016, United States 2016, European Parliament 2019), Russia has positioned itself as an aggressive actor that seeks to undermine the Liberal International Order, while reclaiming its sphere of influence (Davis 2018, 1; Pomerantsev 2015, 48; Chivvis 2017, 5; Lanoszka 2016, 186-187). However, contrary to traditional propaganda campaigns, Russia is not attempting to persuade or garner credibility. Instead, Russia attempts to foster an environment that is consumed with doubt and confusion, where individuals no longer trust democratic institutions and reality becomes an abstract concept, free of objective truth (Giles 2016, 37; Sukhankin 2019, 5). As individuals believe they can no longer trust their institutions or officials this generates a malaise in political consciousness (Fredkin and Kenny 2012, 179). This malaise results in voter apathy, which then allows for demagogues or "pro-Russian" candidates to achieve success in otherwise Western democratic states.

These influence campaigns are effective due to the opportunity structure within liberal regimes, alongside the relative ease and inexpensive cost of connectivity. Their motivations behind this behavior can partially be attributed to fear: Russia is highly disadvantaged in terms of monetary and military capacity when compared to the West, resulting in an asymmetry of power (Davis 2018, 2; Lanoszka 2016, 181). Due to this asymmetry, there are fears that liberal ideology will soon overtake the current oligarchical regime structure. Because of this power asymmetry,

non-linear warfare tactics serve as the most effective measure to counter traditional power and undermine Liberal order.

Russia's propaganda efforts are best described as a "Firehose of Falsehood," (Paul and Matthews 2016, 1) comprised of two features: an enormous number of available channels to spread their messaging, and an unabashed enthusiasm to circulate partial truths or outright fabrications. Their strategy is to disseminate information in high volumes through a multiplicity of channels, ensuring a rapid and continuous stream of information that lacks objective truth, where messaging lacks the consistency of a common narrative (Giles 2016, 38; Davis 2018, 2-4; Sukhankin 2019, 6). Russia's fluid ideology allows it to remain uncommitted to a consistent narrative, co-opting messaging around whomever provides the greatest potential to further discord and eradicate trust (Paul and Matthews 2016, 4; Pomerantsev 2015, 42). Broadly speaking, Russian propaganda falls into four distinct categories: *Political*, *Financial*, *Social*, and *Conspiracy*.

Political propaganda aims to undermine trust in democratic leadership along with the institutions they represent (Davis 2018, 2). Narratives surrounding this effort involve allegations of voter fraud, "rigged" election results, and arguments around political corruption (Miller 2018, 177-179).

Financial propaganda attempts to erode individual confidence in the market while discrediting Western financial institutions. To this effect, messaging is largely in line with fears of national debt and illuminating past misdeeds of financial institutions (Pomerantsev and Weiss 2014, 22).

Social propaganda attempts to exacerbate pre-existing grievances within a social environment, facilitating ideological polarization. Narratives focus around identity politics,

including divisions between progressives and conservatives, race relations, government mistreatment of marginalized communities, and police violence (Lanoszka 2016, 184).

Conspiracy propaganda promotes existential fears, designed to create catastrophe. Narratives are focused on questioning enlightenment principles such as the scientific method. Most notably these have emanated in the form of “Anti-Vax” and Anti-Environmentalism movements (Broniatowski *et al* 2018, 1382; Timberg and Romm 2018).

These propaganda narratives are then disseminated throughout the public sphere in the form of three differing channels: *Overt*, *Grey*, and *Covert*.

Overt channels are those which are plausibly Russian, these include official government sources, state controlled media such as RT or Sputnik, and Russian think tanks or academic institutions (Helmus *et al* 2018, 12). RT is a powerful media conglomerate, with an annual operating exceeding \$300 million USD, and a broad audience around the world operating in five languages (Pomerantsev and Weiss 2014, 14). Their network power enables them to craft narratives as they see fit, relaying a message that serves Russian interests globally.

Unsurprisingly, these stories are often rife with disinformation, however they commonly contain a kernel of truth, further blurring the lines of reality to their viewership (Davis 2018, 4; Thornton 2015, 44). The state controlled media apparatus creates the guise of “factual” information due to their legitimization as an established network, aiding Russia’s more general non-linear warfare campaign. Russia also utilizes captured think tanks or organizations to the same extent. Due to their legitimization as institutions, the lay person is often inclined to believe published material (given they do not previously exert a bias against the scientific method). Russia will seek out academics they believe can be “captured”, due to their own self-interest, to publish research that is favourable to the grand Russian narrative (Chivvis 2017, 3; Sukhankin 2019, 25).

Grey channels create an element of plausible deniability for Russia due to an inability to accurately decipher the locus of information (Sukhankin 2019, 14; Thornton 2015, 45). These include conspiracy websites such as Infowars, severely biased news outlets such as Fox News or Daily Beast, news aggregators, and data dumping sites like WikiLeaks. Russia utilizes these media organizations as a proxy to relay disinformation (Paul and Matthews 2016, 4). The structure of Western media institutions ensures a proxy tactic is highly effective for two reasons: events are reported across all ideological perspectives and a discourse characterized by entertainment (Giles 2016, 34; Pomerantsev 2015, 41). Providing multiple viewpoints will not induce a rational response because humans are not always acting within their own self-interest, rather they revert to their existing belief system. In this sense, “bias free” coverage does not provoke a change in ideology for the average voter. To compliment this, media coverage garners the most reception if it provokes a visceral response. Knowing that media organizations increasingly rely on advertisement revenue to sustain operations (DiResta 2018b, 16) and their user base desires captivating content they are necessitated to promote content that induces site visitation. Media organizations also have an obligation to provide their viewers with real time information regarding current events.

Like grey channels, covert outlets allow for plausible deniability. *Covert* channels focus on user-generated content platforms including, but not limited to Facebook, Twitter, and YouTube. Russia utilizes a variety of strategies and tools on these platforms to achieve a favourable outcome, including trolls, bots, and hackers. Russia utilizes bots and trolls to capture the information marketplace, attempting to sow the seeds of confusion, discord, and malaise from the digital to physical environment (Giles 2016, 37; Paul and Matthews 2016, 4). Russian activities in this regard can be demonstrated through its operations in the USA during the 2016

presidential elections. Described as the “Translator Project,” Russian trolls were deployed to create pages on social media sites designed to represent American based identity groups (Miller 2018, 177-179). These pages posed as American based organizations, focusing on issues pertaining to their select identity group. For example, the account @blackstagram on Instagram was widely successful with a direct audience of 300,000 viewers, eliciting more than 28 million interactions (Thompson and Lapowsky 2018). Russian organizations would then use a series of trolls and botnets to post divisive issues between identity groups. For the African-American community, these would be #Blacklivesmatter, police brutality, or anti-Clinton rhetoric regarding comments about “super predators” or mandatory minimums (DiResta 2018b, 18; Green and Issenberg 2016). These pages were not isolated to the African-American community: they also focused on the LGBTQ community, immigration issues, and gun rights activists, engaging vast networks because of their adaptability, cohesion into American cultural norms, and an understanding of social media algorithms (Albright 2016a).

The typical playbook for these agents is as follows: start by advancing a beneficial narrative, something with a wide emotive appeal, then create content, a social media post, video, or meme. Once the content is created, capitalize on social media’s algorithmic vulnerabilities to amplify the narrative, using either a botnet or series of trolls. If the narrative is effective, the message will be disseminated into individuals feed population where they will then amplify the narrative further through their own network presence (Helmus 2018, 23; DiResta 2018a).

However, this operation is not static: successful non-linear warfare campaigns will continually alter their playbook and employ new methods and modes of disinformation. A variety of tools are now emerging following Russia’s last major campaign; these include “bikini trolls,” who use photos of attractive women as their profile pictures to lure “vulnerable”

populations (Incels, those who are unable to find romantic relationships due to a perceived inferiority, and men over 45) to either provide personal information or serve as another node to amplify disinformation (Giles 2016, 46). Other tactics involve creating accounts posing as government officials. Observing the recent 2019 European Parliament elections, a Twitter account “@Vaalit” (‘elections’ in Finnish) posed as an official European Parliament account and provided false sources of election materials and results (Giles 2016, 46); In addition to these new strategies, deepfakes are becoming increasingly common, where videos of prominent elites are doctored to alter their messaging while still giving the appearance of a verified video (Paul and Matthews 2016, 4; Chesney and Citron 2019). A recent deep fake of US House speaker, Nancy Pelosi, showed her slurring her words following a meeting with Donald Trump, attempting to illustrate her lack of respect for the office. While this video was not high quality and was eventually removed from social media sites, it was shared more than 2.5 million times, demonstrating the power of network effects for these new technologies of disinformation (Towers-Clark 2019).

Russia has also illustrated its readiness to target both elections more generally and political parties and their politicians. Observing their first endeavour into non-linear warfare in Estonia in 2007, Russia strategically targeted government websites, political parties, national banks, news outlets, and internet service providers with DDoS attacks (Ottis 2008 164). Russia’s attack left Estonia without access to critical infrastructure for several days. Since 2000 Estonia has been a global leader in digital connectivity, so much that internet is a human right (Chakravoti, Tunnard, and Shankar 2015) Russia’s ability to undermine the digital environment of a state whose essence is built upon digital activity serves to reinforce their power as other states increasingly rely on digital services to conduct their daily activities.

Observing the 2016 US presidential election, Russian intelligence units launched a “spearfishing” operation to access the Democratic National Committees (DNC) network of information (Miller 2018, 20). Two separate hacks occurred which would later be coined from officials as “Cozy Bear” and “Fancy Bear”. These advanced persistent threats would delve through the DNC’s network, collecting emails, chat logs, and research files (Miller 2018, 47). The information collected was strategically leaked through WikiLeaks over the course of the election period by an alleged agent of the Russian state, known online as Guccifer 2.0. These leaks were done at crucial times to discredit Hilary Clinton in her victory over Bernie Sanders in the DNC primaries, demonstrating her poor judgement in handling her personal emails, the Benghazi decision-making process, and the behaviour of the Clinton Foundation. The anti-Clinton agenda created a sense of malaise within the democratic party for African-American, young liberal, and women voters, illustrated by low voter turnouts of these groups in swing states (Green and Issenberg 2016).

Russia utilizes a variety of tactics, affecting all three targeted areas (Elections, Politicians, and Voters), where they will incorporate all available resources in the process of a non-linear warfare campaign. Russia’s integrated operations, fluid ideology, and unabashed willingness to engage against the West illustrates a likely risk for Canada’s election in 2019.

China

China’s approach to non-linear warfare is starkly different from that of Russia’s: while Russia attempts to foster an environment of discord and post-truth, China focuses on promoting a positive image of abroad (USCC 2018, 307; Brady 2015, 57). Observing Chinese influence campaigns in established democracies (Australia, New Zealand, and Taiwan), China has focused

on suppressing actors, institutions, and policies that it finds unfavourable to its strategic goals, in addition to undermining other states reliance on Western markets (USCC 2018, 321; Wortzel 2014, 30; Brady 2015, 53; Kurlantzick 2007, 43). China perceives the Liberal International Order as unfair and heavily biased, where the institutions and policies are restrictive to its state sovereignty (USCC 2018, 306). Due to this creeping fear of liberalism as a restrictive mechanism, China's pushback is not unexpected. In this regard, China's motivation to conduct a non-linear warfare campaign is not all that dissimilar to Russia's. The Chinese Communist Party (CCP) utilizes these tactics for two primary reasons. The first is a preservation of party power and stability, where the CCP views threats to its permanence in the form of ideas, namely Liberal ideology and multicultural society (Mattis 2018). Given the threat emanates through ideas and deliberation, kinetic tactics will not mitigate its problem. The second is due to an asymmetry in the Peoples Liberation Army (PLA) capabilities and the inability to protect party power (Mattis 2018). Having to defend both kinetic and non-kinetic threats remains a daunting task, hence the CCP's focus on pre-emptive measures of influence operations.

The CCP utilizes a variety of differing tactics and agencies to conduct its non-linear warfare campaign, ranging from the "Three Warfares" doctrine of the PLA – psychological operations, media manipulation, and legal warfare – to its "United Front" Work Department agency designed to co-opt or neutralize sources of opposition to the CCP (USCC 2018, 14; Mattis 2018; Bowe 2018, 4; Brady 2018, 34). Strategies overlap between the various CCP apparatuses; however, all remain committed to a unified goal of maintaining ruling party control and advancing a positive image of China abroad. Utilizing numerous academic and government contributions, I define four general strategies that encompass the varying tactics of the CCP's

operations: *Economic Coercion, Perception Management, Information Warfare, and Cyber Tactics*.

Economic Coercion is a frequently used strategy in Beijing's nexus of influence tactics designed to undermine the sovereign policy making of states. China's "One Belt One Road" policy of economic cooperation designed to expand global trade routes, serves as an overt expression of its desire to counter Western power and promote its assertiveness against the Liberal International Order (Chanda 2015). The concern with Chinese foreign direct investment can be noted through the responses of minor power states, where China now exerts significant political influence. Take for example the case of Norway when the Nobel Peace Prize was awarded to the Chinese activist Liu Xiaobo. China imposed economic sanctions, cancelled trade negotiations, and froze free trade agreements, in addition to diplomatic sanctions of restricting visa free travel between the two states (Zhang 2019; Harrell, Rosenberg, & Saravalle 2018, 24). As a result, Norway cancelled visits with the Dali Lama and expressed they would not support any behaviour that could be detrimental to China's core interests (Zhang 2019 Brookings; Harrell, Rosenberg, & Saravalle 2018, 24). China also utilizes its economic clout to garner beneficial policies from other states, providing financial incentives to sway diplomatic favour (USCC 2018, 307). China's clout has also contributed to the concept of pre-emptive obedience, where the notion of Chinese investment has the potential to influence policies beneficial to China (USCC 2018, 308). States without the means to develop large scale and necessary infrastructure behave in a manner consistent with China's core interests in the hopes of securing investment.

Perception Management aims at controlling the external narrative around China, where it promulgates a notion of a "peaceful rise" to power, arguing that its ascent to prominence should not be viewed as a threat to international peace and security, rather its emergence as a regional

hegemon should be viewed positively in furthering international cooperation and development (Kurlantzick 2007, 37-38). This aim is advanced largely through the United Front Work Department, whose goal is to coopt and suppress sources of opposition to the policies of the CCP (Brady 2018, 35; Bowe 2018, 3). For the interests of this paper, the two most pressing areas of the United Front policy are *the coopting and cultivation of foreign elites* and *a strategic communication strategy to promote the CCP agenda* (Brady 2017, 7). While China advances their narrative through a multiplicity of channels, which I will discuss further in subsequent sections, I will focus on two specific tactics here.

First, is the promotion of Confucius Institutes abroad. Used as a tool to promote the CCP perspective, Confucius Institutes operate within the confines of established universities, teaching Chinese language, culture, and history (Bowe 2018, 12; NATO 2018a, 41). However, these institutions could constitute a larger concern to national security as citizens are subjected to views that oppose democratic values (NATO 2018a, 34). Confucius Institutes are an extension of the CCP Propaganda Department – formally affiliated with the United Front – where the teachings purported are used to legitimize the CCP’s power and promote a sympathetic view of China (NATO 2018a, 34). These institutes do not merely promote China abroad, rather they conduct a much more sinister activity, including organizing protests around topics deemed to be a threat to CCP ruling power, censoring academic debate that could undermine CCP legitimacy – Tiananmen Square, internment of Uyghurs in Xinjiang, Tibet occupation, in addition to “strings attached” research funding where publication is based on CCP approval (Bowe 2018, 12-14; NATO 2018b, 41). By undermining debate and creating a contrary narrative, China can influence voter’s belief systems through what appears to be a legitimate academic exercise. Confucius

Institutes are an extension of the CCP, serving a calculated means of advancing its agenda, attempting to undermine democratic freedom in host countries.

Second is the China Association for International Friendly Contact (CAIFC). The official mandate of the organization is to “establish friendly ties with foreign government agencies, political parties and prominent political and military figures” to promote its policies, achievements, and goals (CAIFC 2019). These contacts are strategically selected because of their potential to influence policy making, in addition to their perceived naivety or self-interested leaning (Bowe 2018, 10; Wortzel 2014, 33). This strategy enables the CCP to have seeded allies throughout the political and economic elite in a multiplicity of states, where their action could have direct impact on influencing policies favourable towards Beijing (Brady 2018, 36; Bowe 2018, 10). Like Confucius Institutes, these visits are promoting a heavily distorted image of China and its policies, designed to coopt decision-maker’s belief systems and promote a favourable perspective. Cultivating elite allies establishes credibility, where China can then mobilize these coopted actors to publish or purport favourable opinions to the benefit of the CCP (Brady 2017, 190).

Information Warfare is not only concerned with the narrative encapsulating China, it is also attempting to control the information space from which the narrative is disseminated. To control the media environment, the CCP focuses on three distinct efforts. First, is through establishing Chinese media conglomerates in foreign states or coopting already established media companies, such as China Central Television (CCTV) or China Radio International (USCC 2018, 315; Wortzel 2014, 32; Mattis 2018; Brady 2017, 9). Chinese propaganda campaigns abroad focus on two populations: Overseas Chinese and non-Chinese foreigners. China views all its overseas population as potential agents of influence that can be used to

achieve its ends (Kynge, Hornby, and Anderlini 2017). In this sense, its media operation will differ between the two populations. For the Chinese diaspora, media outlets such as CCTV or Xinhua News Service ensure that Beijing's agenda prevails in the Chinese community, subverting influence from Western media (Brady 2017, 189; Wortzel 2014, 32). The Chinese diaspora will then remain loyal to the state, where they can then be used either as strategic voters or potential political candidates.

Influence campaigns directed towards non-Chinese foreigners follow a slightly different strategy. While still promoting Beijing's agenda abroad, the CCP will use both directly associated Chinese news outlets – *China Daily*, *Beijing Review*, or CCTV – and existing Western channels to coerce individual belief systems (Brady 2017, 190; Qing and Shiffman 2015; Mattis 2018). The CCP has recently purchased failing media companies under the parent company *China Radio International*, where they are then able to establish its preferred narrative and disseminate it through an established institution (Mattis 2018). This is a highly effective tactic that subverts the level of distrust of foreign populations towards China as the content appears to be issued through a trusted source.

Second, is a Mao era strategy of “borrowing a boat to go out on the ocean”, where the CCP will either coopt Western journalists, or insert its own articles to promote Beijing's agenda abroad (USCC 2018, 316; Brady 2017, 190). The CCP will insert its narrative through what appears to be a legitimate media source, subverting the narrative and attempting to foster belief in Beijing's agenda. Take for example a recent article published by Karen Woods (2018) in the *Toronto Star*, “Huawei Crisis has Chinese Canadians Worried.” The article alleges that Chinese-Canadians will soon face “McCarthy Era” discrimination due to perceived allegiances to the CCP, noting a historic policy of the Chinese Exclusion Act to legitimize their fears. She

appeared to be a knowledgeable author with established credentials, however, on further investigation Mrs. Woods was a paid lobbyist on behalf of the Canadian Chinese Political Affairs Committee.³

Third, is the deployment of online Trolls that safeguard the preferred narrative of Beijing in the digital sphere. These Trolls are part of a coordinated group effort to promulgate the digital environment with disinformation, countering negative rhetoric, and promoting Beijing's agenda globally (Repnikova 2018; Yang 2017). Groups have been come to be known as the "50 Cent Army," a name given for the alleged 50 cents each agent would earn per post, or "Little Pinks," named after the colour of the forum they operate out of (Yang 2017). Much like Beijing's other media influence operations its nexus of trolls operate under a similar premise, crafting narratives on both Chinese social media sites (Weibo, WeChat, Tencent QQ) and Western social media (Facebook, Twitter, Reddit). Trolls operate under a decentralized nexus, meaning that the CCP can maintain plausible deniability while individual agents can circulate the CCP's preferred narrative online (Sigur Center for Asia Studies 2019, 3). Literature on Chinese trolling efforts have broadly shown three distinct tactics: first, is to engage with critics of the CCP, where efforts are focused on countering rhetoric and defending party practices (Greitens 2013, 265; Han 2015, 116). Second, are those who attack liberal values and policy-making, often with memes, disinformation, or in comment sections (Yang 2017). Third, are those who act as a "cheerleader" for the CCP, flooding feed algorithms with content that promotes the Beijing agenda abroad (King, Pan, & Roberts 2017, 490-494). Like other actors in this space, Chinese operatives utilize social media bots and content farms to flood the digital space, utilizing algorithmic knowledge to tailor messages and effectively engage the population (King, Pan, & Roberts 2017, 487-488).

³ The article was later revised to indicate that Karen Woods was the co-founder of the Canadian Chinese Public Affairs Committee and her association with the Chinese Consulate-General.

Cyber Tactics involve a range of actions defined as “third-generation controls,” including surveillance applications, targeted espionage, and covert interferences in the digital environment (Diebert 2016, 69). Noting the Shanghai tech conglomerate Huawei, former National Security Agency and Central Intelligence Agency chief Michael Hayden has lodged several accusations against the firm for assisting in espionage tactics with the CCP (Joye 2013). His accusations precede the formal sanctions imposed by the US government and the restrictions placed by the “Five Eyes” – intelligence sharing nations of US, Canada, UK, Australia, New Zealand – citing concerns to critical national infrastructure (Holden and Stubbs 2019). There are fears that the CCP would leverage their power and force Huawei to participate in espionage on behalf of the party. While Huawei adamantly denies their participation in espionage, there is *prima facie* evidence to suggest “backdoor” access tools were incorporated into its software (Lepido 2019). Although Huawei denies any malicious intent with this software, authorities must be cognizant of the CCP’s non-linear warfare tactics and the willingness to leverage all resources to achieve a desired outcome.

In addition to corporate-state espionage partnerships, the CCP has also engaged in targeted cyber-attacks. Noting a 2013 investigation by CitizenLab on malware targeting, CitizenLab examined emails sent to prominent members of the Tibetan-Canadian community, finding malicious malware attached to unassuming emails (Kleemola and Hardy 2013). If the documents were opened, the threat would have gained backdoor access to the device, able to log keystrokes, file directories, and execute commands remotely. The hacks were allegedly conducted by members of the PLA, who were later identified as APT1 by the cyber security firm Mandiant. The military hackers were formally charged by the US Department of Justice in 2014 for computer hacking, economic espionage, and aggravated identity theft (US DOJ 2014). This

team of hackers is just one iteration of a coordinated Chinese campaign attempting to covertly access and influence vital information systems.

Canada as a Target

Observing the 2015 federal election, security experts determined that Canada was victimized by targeted cyber-attacks. While these efforts were not sophisticated, indicating the threats were likely not part of a coordinated state effort, Canada's security systems were violated (CSE 2017). The Communications Security Establishment states that Canada's democratic process could once again be a potential target in 2019; however, the understanding is that future attacks will be part of a coordinated state-level effort due to our strategic relationships in the international community (CSE 2019, 9). Canada is a G7 country, a NATO member, and actively involved in other international bodies such as the United Nations and "Five Eyes" intelligence community. Due to Canada's position in the international community its decisions are impactful, where choices regarding diplomacy, immigration, investment, military, and trade have the potential to influence the interests of other states. At an actor specific level, both Russia and China have an incentive to engage in campaigns of influence against Canada's democratic process, which I identify below. **Russia** views Canada as a potential target for the following reasons:

1. *Canada as "Russophobic"*: Canada was among the first states to mobilize against Russian non-linear warfare efforts in the Ukraine, implementing sanctions on March 17th, 2017 (Canadian Sanctions Related to Russia 2019). Canada has also deployed troops and contributed more than \$700 million in funding to aid in Ukraine's security dilemma (Operation UNIFER 2018). Also, noting Canada's decision to adopt *Magnitsky* legislation in October 2017 - subjecting foreign governments who violate human rights to

the *Special Economic Measures Act* – has been a core foreign policy concern for the Russian government (Kolga 2019, 20). Finally, Russian commentators have linked Russia's exile from the G7/G8 to Canadian decision, arguing that the G7 has become an international platform for anti-Russian rhetoric and behaviour (Natsional Sluzhba Novostey 2015).

2. *Canadian participation in the Baltics*: Canadian military participation alongside NATO deployment in the Baltic states have resulted in insistent disinformation campaigns against its armed forces (Kolga 2019, 15). The claims insinuated by the Kremlin are strategic to the narrative that NATO exercises are conducted to lay territorial claims to the region in the future (EU vs Disinfo 2018). As Russia aspires to maintain its grip on former Soviet satellite states, NATO remains a threat to its vision. Russia utilizes a similar non-linear warfare strategy in the Baltics to sow the seeds of doubt against Canadian and NATO involvement in the region, claiming Canadian military frequently engages in drunk and disorderly behaviour, desecrates national symbols, harasses local women, and routinely engages in unsanctioned military exercises (Sukhankin 2019, 30; Blackwell 2017).
3. *Fear the West*: Russia currently exists in an asymmetrical power relationship with the West. While Canada's military and economic strength is lesser to Russia on a state-to-state level, its membership in powerful international bodies is enough to constitute a threat. Canada has been a pioneer in the West with regards to social policy trends - legalizing gay marriage, legalizing marijuana, and recognizing claims of reconciliation against marginalized and minority populations. There is growing fear in Russia that

globalization and the spread of Western values into former Soviet satellite states will creep into Russia's mainstream culture, displacing its oligarchical power structure.

China views Canada as a target for the following reasons:

1. *Promotion of China Abroad*: In contrast to America's rise to global hegemony, China does not wish to overturn the international order, rather it merely wants to expand its influence abroad. To this end, China wants states to align its policies with the long-term goals of the CCP, stability and economic might. In this regard, Canada is as much of a target as any state, where the CCP has an interest in ensuring allies globally.
2. *Tit-for-tat*: China has a vested interest to engage in similar practices as Western states. States who have committed to the Liberal International Order routinely attempt to intervene in sovereign Chinese policy, positing claims of human rights abuses, like the treatment of the Uighur population and "re-education camps" in Xinjiang to international institutions. Canada has previously attempted to integrate Liberal principles (human rights, gender, environmental issues) into trade negotiations with China (Duckworth 2018). These principles do not have priority in Chinese political affairs, where China views the forceful action of Western states as an attempt to undermine its political sovereignty, which could in turn threaten the regimes stability. To this, the principal aim of the CCP is to ensure legitimacy and longevity, where the party will in turn mobilize all available resources to ensure a successful path forward. Furthermore, the recent capture and extradition of Meng Wanzhou (Huawei's Chief Financial Officer) by the Canadian government has led to an intensified dispute in Canada-China relations (Proctor 2019).

3. *Chinese Territorial and Identity Claims:* The “One China Policy” lays claims over neighboring territories (Tibet, Taiwan, South China Sea) in addition to recognizing only the Han population as legitimate Chinese citizens, creating an exclusionary class of people including those from the aforementioned territories as well as the Uighur’s and Falun Gong. China has a vested interest in ensuring diaspora communities from these identity groups do not engage in counter-claims against the state in their new host countries. Observing the malware attacks on Tibetan-Canadians, China has demonstrated its willingness to engage in cyber-attacks on diaspora communities who do not abide by the One China Policy, which in turn should be classified as an attack on the Canadian state. Canada’s willingness to aid marginalized communities who have been a victim to the Chinese state could have implications for non-linear warfare actions against Canada in the future.

These motivations have been defined based on the publically available knowledge and may not constitute the full scope of potential reasoning behind a non-linear warfare campaign against Canada. While there are other actors in the international environment who may have a vested interest in conducting an influence campaign against Canada, this capstone focuses on the two most notable and powerful actors who operate in contrast to the Liberal International Order. Moving forward, I will now identify the potential targets and strategies that could be employed by hostile foreign actors against Canada and its citizens.

Actors and Institutions at Risk

Having described what states may attempt to conduct a non-linear warfare campaign against Canada and strategies that would be effective, we can now turn our attention to where

these states will focus its power. Electoral interference efforts focus on three targets: *Elections*, *Parties and Politicians*, and *Voters*. Each target faces a differing strategy designed to influence the outcome of an election. While the motivation and strategies of states will differ, these represent the current state of knowable tactics.

Elections

Elections in Canada are comprised of three aspects: registration, voting, and distributing the outcome. As such, each aspect has some variance of risk which could be exploited by adversarial foreign actors. The Communications Security Establishment (CSE) has identified threats to this election procedure (Communication Security Establishment 2017, 15), these are:

1. **Prevention of voter registration**, where online voter registries could be polluted with false voter records; the online registration platform could be made inaccessible; or existing voter registration could be erased.
2. **Inhibiting voting**, where the physical ballot boxes could be tampered with to provide inaccurate results.
3. **Tampering with election results**, where the results could be changed while being transmitted (noting that the occurrence of this is only present where the voting procedure is digital).

These threats could then be realized using a variation of differing strategies, each with a specific intent:

1. **DDoS attacks** (Distributed Denial of Service) are conducted to prevent access to a website/platform, utilizing ping flooding, udp flooding, creating malicious web queries, and communication spam (Ottis 2008, 166). As it relates to Canada's election, this strategy is useful to prevent voter registration;

2. **Redirect attacks** reroute the communications from the sender through an adversary before the information reaches its intended target. The adversary can then alter the information undetected and the recipient would be unaware an attack had occurred. This strategy is used to tamper with election results if those results are transmitted digitally.
3. **Hacks** are used to break into secure systems or networks and can involve a variety of tactics, generally focusing on exploiting existing security weaknesses. This strategy could be used to manipulate existing voter registration records or stealing voter records.
4. **Defacing a website** would involve altering the sites information, which could take various forms such as, providing inaccurate voting times and locations. This strategy could be employed to suppress voter turnout.

Parties and Politicians

Political parties and politicians are sought after targets for hostile foreign actors due to their nature as decision-makers in government, where adversaries may seek to influence their policy making power through a multiplicity of various apparatuses.

1. **Foreign Contributions:** Foreign governments or actors may contribute to third party groups, such as corporations or charity organizations, who can then use those funds to make financial contributions to parties. Foreign governments may also use charities as conduits to advance its preferred policy narrative, where foreign funded groups could lobby government officials or release reports that could be to the benefit of a political party.

2. **Spearfishing** has been successfully demonstrated as an effective means to gain access to critical information to both party and voter data. It is also used as technique to gain backdoor access to critical infrastructure.
3. **Espionage** is a highly effective tactic to gain access to crucial information, where information could then be used to the benefit of an adversary. This would include activities such as backdoors in information technologies or traditional methods of manipulating actors to willingly provide intel.
4. **Embarrassment** is a useful tactic to discredit a politician or political party. Foreign governments may release disinformation or information regarding previously incriminating behaviour on political affiliates in an effort to sabotage their campaign.
5. **Blackmail** in a similar vein to embarrassment, foreign adversaries could acquire damaging information on a political target, which could then be used to coopt their policy making powers or political agenda.
6. **Data Theft** foreign adversaries could acquire sensitive information regarding political parties or politicians, which could then be used to create targeted campaigns.
7. **Statecraft** is an effective tactic to subvert the free decision making powers of politicians, political parties, or prominent elites who are tangentially related to the party. These efforts could include foreign funded visits, economic coercion, or diplomatic sanctions which may impact their ability to make “bias free” judgements regarding the foreign entity.

Voters

Voters are the crux of the democratic process, where their voting decision ultimately sets the stage for the state. Voters are a significant target for foreign governments as they can be easily targeted and manipulated with relative low costs. Foreign governments focus on two outcomes when targeting voters: convince them to vote for a party that would benefit its preferred policy, or convince them not to vote. The following tactics can be used to achieve either outcome:

1. **Data Theft** is used to acquire sensitive information regarding the voter, which could then be applied to a targeted campaign designed to coopt the voter's belief system or instil a sense of malaise where they would not turn out to the polls. Observed during the 2016 US presidential campaign, where DNC voter data was stolen and publicized by hacker Guccifer 2.0. Data could be acquired through a multiplicity of nexuses, where the data controller may sell information to a foreign adversary or the user could willingly provide data by using certain applications or websites.
2. **Trolls/Bots** are highly effective in promulgating disinformation or information online, where the data capabilities of foreign adversaries allow these actors to target populations who are most receptive to influence campaigns. Voters could either be receptive to the campaign and in turn decide to vote along those lines or become dissuaded by the democratic failings and decide not to vote.
3. **Deepfakes** can be leveraged to manipulate voter belief systems through the creation of fake content designed to mimic prominent elites. Unable to accurately decipher the occurrence of an event, voters may be manipulated into the preferred narrative of a foreign adversary. At this stage deepfakes are early in the development process, however,

recent demonstrations by CannyAI for a project called ‘Spectre’ displayed one the most hyper realistic illustrations in their portrayal of Kim Kardashian in an Instagram video (Posters 2019).

4. **Universities** are a highly effective apparatus to circulate belief systems. Knowing the influential power of the university as a breeding ground for discourse, foreign adversaries have an interest in ensuring its narrative promulgates throughout the university. Students, who are potential voters, may have their belief systems coopted under the guise of a legitimate institution. The pervasiveness of ‘Confucius Institutes’ in Canadian Universities deliberately undercut the teachings of Liberal values, such as human rights, where these institutes do not serve the interests of the countries hosting them.
5. **Media** is the most effective means of transmitting information to the general public. Knowing this, foreign adversaries may coopt or purchase outlets to promulgate its narrative, where information could appear legitimate from the view of the uninformed voter. Observing Karen Woods articles in *the Star* or propaganda networks broadcasting in Canada such as ‘Chinese Radio International’ in Vancouver.

Based on the relevant literature, I postulate that foreign adversaries who attempt a non-linear warfare against Canada during the period leading up to and over the course of the 2019 election will engage in a campaign that follows these general tactics and focus on three targets listed previously: the electoral process, parties and politicians, and voters themselves. The remainder of this paper will analyze Canada’s defence mechanisms that would prevent an effective non-linear warfare campaign.

Canadian Safeguards to Democracy

Following Russian actions against the United States in 2016, there has been a compendium of policy responses from Western democracies. Canadian efforts have been productive in this area, passing the *Elections Modernization Act* (2018) as an update to the *Elections Canada Act* (2000), in addition to other non-legislative measures. The following section will identify existing Canadian safeguards to defend against foreign intervention in the 2019 election. These safeguards can be separated into six non-exclusive categories, listed below and discussed in more detail in subsequent pages: 1. *Infrastructure Protections*; 2. *Information Security*; 3. *Prohibitive Mechanisms*; 4. *Detection Mechanisms*; 5. *Social Media Regulation*; 6. *Voter Resiliency*.

Infrastructure Protection

Voting procedure in federal elections is entirely paper based. Sections 114 to 116 of the *Canada Elections Act* (2000) requires voters to physically transcribe their vote on the provided ballot, which is then placed into a secure ballot box. Part 12 of the *Canada Elections Act* also identifies the procedure for counting the votes, specifically sections 283 to 289 have legislated this counting procedure. In addition to these sections, section 290 outlines the procedure to deliver ballot boxes from the polling stations to the Electoral Officer. Moreover, section 292 identifies the safekeeping of the ballot boxes by the Electoral officer. Canada's antiquated technologies, ironically, provide an effective safeguard against identified threats to physical election tampering, whereby, the use of paper and pen mitigate the risk that votes may be physically manipulated.

While the federal voting procedure is secure, there is still risk associated with voter registration. Elections Canada allows online voter registration (Elections Canada 2019), which

creates a risk around two scenarios: *first*, hostile elements could pollute the voter registration database with false records, resulting in difficulties for electoral officers on polling day; *second*, hostile actors could also use manipulate the voter registration website, either rendering it inaccessible from a DDoS attack or deface the website, having it display misleading information to voters. In both cases, democratic freedoms have been interrupted and undue stress has been placed on Canada's election infrastructure.

Lastly, the process of disseminating results from the polling station to the public, which can be transmitted either by hand, phone, or the internet (Elections Canada 2019). In the case where votes are transmitted online, foreign meddlers may have the capabilities to intercept and alter the results using a redirect attack, however, Elections Canada has safeguarded against this with the use of paper and pen ballots. While there is potential for adversarial actors to capture and alter the results during transmission, the physical ballots can be recounted, mitigating the risk. In a worst-case scenario, an adversarial actor could induce short-run "panic" in voters by displaying illegitimate results, however, this can be easily and readily countered by Elections Canada.

Information Security

Section 385.1 of the *Canada Elections Act* (2000) requires registered political parties to provide the Chief Electoral Officer with the party's independent policy on the protection of personal information. However, this legislation does not specify guidelines as to how parties must protect voter's personal information. While official legislation is lacking, the Office of the Privacy Commissioner has provided a series of best practices that provide a guideline for parties to establish effective privacy policies. These guidelines follow 10 directives, which I will briefly describe (Guidance for Federal Political Parties 2019): *Accountability*, each registered party must

have written policies that can be readily demonstrated; *Identifying purposes*, parties need to be transparent in the collection and use of personal information; *Consent*, needs to be meaningful and valid with regards to collection, use, and disclosure of personal information; *Limiting collection*, personal information should only be collected and used as it is defined under the *Privacy Act* (1985) and should not include opinions; *Limiting use*, personal information should only be used for the purposes stated by the party in its collection; *Accuracy*, all information is up to date, where parties must be mindful in attempts to draw inferences from said information; *Safeguards*, parties need to protect personal information from unauthorized access, where safeguards should have forms of encryption to limit access and all employees or volunteers must be aware of the sensitive nature of personal information; *Openness*, practices need to be clear and transparent; *Individual access*, upon request, individuals should be given access to information that has been collected and have the right to correct false information; and *Challenging compliance* ensure all complaints are readily investigated and take heed of concerns from citizens.

Although the Privacy Commissioner has provided a detailed list of best practices and parties claim to have sufficient safeguards to protect voter's personal information, there may still be a risk. During the 2016 US presidential election, the Democratic National Committee voter database was hacked by an alleged agent of the Russian state, known as Guccifer 2.0. The result illustrated the capabilities of the DNC for voter quantification, which may have contributed to malaise and apathy towards the democratic process. While safeguards are in place it is not improbable that a similar case could occur at the expense of a political parties computer security.

Prohibitive Mechanisms

Following the *Lortie Commission* in 1991 and the subsequent recommendations and changes regarding election financing, the use of foreign contributions to fund political activities, including parties or campaigns, has been explicitly prohibited (Reforming Electoral Democracy 1991, 321). However, there are other means by which foreign entities could influence the Canada's elections.

Provisions in the *Canada Elections Act* (2000) prohibit undue influence from foreigners. Under section 282.4 (1), “no person shall during an election period unduly influence an elector to vote or refrain from voting, or to not vote for a particular candidate.” Where “unduly” means, a foreign entity has knowingly expensed or endorsed a registered party or candidate. However, there are exceptions in this legislation that allows for foreign entities to express an opinion of the desired outcome, if their only action is one of the following: presenting a statement that encourages the elector to vote or refrain from voting, or transmit through broadcast an editorial, debate, speech, interview, column, letter, or commentary regarding the preferred outcome of the Canadian election.

I express concerns to this particular section on two accounts: *first*, the legislation only applies during the “election period,” which is defined as “the period beginning with the issue of the writ and ending on polling day” (Canada Elections Act 2000, 4). This does not prevent foreign entities from conducting influence campaigns during the “pre-election period”. *Second*, is the allowance of *some* commentary from foreign entities with regards to Canada's election. While there may be legitimate reasons to allow these provisions, such as the promotion of functional democracy and get-out-the-vote campaigns, there is leeway for a foreign government

or actor to unduly influence an election. However, I will note there would be difficulties both in a capacity to monitor and enforce the concerns I have expressed.

Section 349.02 of the *Canada Elections Act* (2000) prohibits the use of foreign funds by third parties, where “no third party shall use funds for a partisan activity, for fundraising, for election advertising or for an elections survey if the source of the funds is from a foreign entity.” Third parties represent a significant source of electoral financing, contributing over \$37 million of a total of \$135 million in funding during the 2015 federal election (Postmedia 2019)⁴. Prohibiting the use of foreign funds by third parties is a necessary mandate to secure Canada’s democratic infrastructure.

Continuing with the *Canada Elections Act* (2000), section 482 (1) specifies provisions relating to unauthorized use of a computer, where any means that could be used to directly or indirectly alter or destroy data or obstruct, interrupt, or interfere with data with the “intention of affecting the results of an election” is subject to an offence. This provision implements a safeguard that can be used to hold foreign entities responsible in the event of a cyber campaign to influence Canada’s election. While foreign entities often utilize plausibly deniable methods to conduct cyber operations to subvert culpability, this legislation is necessary to create a deterrence effect.

Detection Mechanisms

The first line of defence is knowing that a problem exists. Canada’s security and intelligence agencies – Canadian Security Intelligence Service, Royal Canadian Mounted Police, Communication Security Establishment, and Global Affairs Canada – have formed a joint task

⁴ These contributions may be greater than \$37 million due to the use of “conduits” by corporations, unions, or other groups who can subvert the limits on financial contributions by providing employees or group members with the funds to make donations on behalf of the third party.

force known as SITE (Security and Intelligence Threats to Elections). The task force is responsible for preventing potential acts of non-linear warfare that would affect Canada's democratic process (Combatting Foreign Interference 2019). Beyond the responsibilities set forth in the SITE task force, agencies conduct independent monitoring and assessments of potential foreign intervention. The CSE's mandate, as defined by the *Communications Security Establishment Act* (2018) in part 3 *National Defence Act* (2018), requires the agency to acquire and use information to aid foreign intelligence; provide guidance and services to protect information infrastructures; and provide assistance to federal law enforcement agencies. CSE's role in this process is to ensure Canada's government systems and networks are protected against cyber-attacks. Defined by the *Canadian Security Intelligence Service Act* (2017), CSIS's duties extend to counteract any particular activity that constitutes a threat to national security, so long as that response is reasonable and proportional. To this, they are actively monitoring and reporting threats to the government and political parties. The RCMP's responsibility in this area is to investigate and disrupt undue influence by foreigners pertaining to Canada's democratic infrastructure.

These agencies, along with the joint SITE task force are a necessary and effective means to detect foreign interference in Canada's democratic process, whereby appropriate precautions have been taken by the federal government to detect and inform necessary actors in the event of a foreign interference campaign.

Social Media Regulations and Advertising Restrictions

The *Elections Canada Act* (2000) defines *election advertising* under section 2 as "Transmission to the public by any means during an *election period* of an advertising message that promotes or opposes a registered party or the election of a candidate, including by taking a

position on an issue with which a registered party or candidate is associated.” Section 2 also defines *partisan advertising*, which is identical to *election advertising*, however, partisan advertising refers to that during the *pre-election period*. Both definitions do not include the transmission of editorials, speeches, interviews, columns, letters, or commentary; book publications; sharing political documents; or making phone calls to voters. Furthermore, subsection (7) references advertising as the promotion or opposition of a party by its name or identification, or the promotion or opposition of a candidate through name, photos, cartoons, drawing, or logos. While these definitions are necessary, they are not sufficient to protect against potential hostile actions by foreign entities, whereby advertising takes form in a variety of differing means, resulting in a gap that would allow for ideological references.

To this, the *Elections Canada Act* (2000) under section 325.1 (2) requires online platforms who sell advertising space for the purposes of partisan or election advertising to publish the financier as one of: the registered party, registered association, nomination contestant, potential candidate, or a third party. Where online platforms who are subject to legislation are defined under 325.1 (1) by the average visitation numbers by Canadians, being 3 million users if content is primarily available in English, 1 million if content is primarily French, or 100 thousand if content is primarily in a language other than English or French. This definition fails to address a fundamental issue as it only pertains to “mainstream” sites. While this is a necessary update to address the changing technological environment, it does not encapsulate “fringe” sites. Hostile adversaries routinely utilize fringe sites such as China Daily or InfoWars in foreign influence efforts, because of their susceptible or radical user base. These populations are highly vulnerable to targeted advertisements, where foreign entities could target these networks with advertisements to manipulate belief systems.

Furthering the efforts of Elections Canada, the ministry of Democratic Institutions has published a *Declaration on Electoral Integrity Online*. Together with online platforms, the ministry hopes to ensure integrity, transparency, and authenticity online with respect to the 2019 federal election (Canada Declaration on Electoral Integrity Online 2019). In this declaration, the government has set forth a series of responsibilities for both online platforms and the Canadian government. With respect to online platforms these responsibilities are as follows (Canada Declaration on Electoral Integrity 2019):

- Combat disinformation through increased transparency and understanding, while informing Canadians about new safeguards
- Apply the latest technology that would aid in the protection of democracy
- Promote safeguards that promote security with ensuring privacy protection
- Advertisements are transparent in nature and well regulated
- Terms and conditions are easily accessible with language that is readable
- Will work towards removing fake accounts and inauthentic content
- Will work towards removing malicious bots

Alongside guidelines for platforms, the declaration also establishes procedures for the government of Canada to take with respect to online platforms:

- Ensure policy is readily communicated to platforms
- Implement the Critical Election Incident Public Protocol
- Promote lawful information sharing
- Collaborate with civil society to support efforts of critical thinking
- Support the sharing of information on emerging developments related to threats against democratic institutions

The Declaration set forth, along with the revised statutes in the *Election Canada Act*, has forced some online platforms to update policies regarding political advertisements. Twitter has stated it will comply with these new guidelines, the site will no longer allow *partisan* advertisements and has developed an advertisement registry (Thompson 2019a). Twitter has also taken measures to reduce automated content that could be malicious, developing a site integrity team to facilitate user feedback on these issues (Thompson 2019a). However, it should be noted that Twitter will still allow *election* advertisements during the writ period, so long as those advertisements comply with Elections Canada regulations.

Facebook has also decided to comply with these guidelines and regulations, updating its policies on partisan and electoral advertisements. While Facebook will allow both, advertisements must be pre-approved by the platform having to abide by legislation set forth by Elections Canada. Advertisements will also have a link that displays the financier and targeting settings (Facebook 2019). It should be noted that Microsoft (Bing) has decided to ban political advertisements across all jurisdictions, and Alphabet (Google) has decided they will not comply with legislation, claiming the company was not provided with ample time to develop new policy guidelines (Thompson 2019b).

While these companies have updated policies to conform with government legislation, there are still myriad problems left unaddressed. These policies only pertain to paid content, so advertisements that are unpaid are left unregulated. The most concerning aspect of this is the failure to address algorithmic manipulation of feed populations, where botnets and influencers can rapidly disseminate content to unsuspecting populations. Another concern is the Government of Canada's failure to understand opinion formation and bias, that hostile actors have effectively mastered. The requirement to have registries tied to advertisements, displaying the financier and

origin of content presupposes how vulnerable or those least sophisticated process information. These populations do not fact check or seek additional qualifiers for new information, meaning that the new policies will place an overwhelming onus on users. The last immediate concern is the failure to address deepfakes, where online platforms do not currently have policies that restrict the posting of these materials. Given that current legislation allows for political candidates to give speeches as source of partisan or election advertisements, deep fakes allow advertisement regulations to be subverted.

Voter Resiliency

The first step in safeguarding Canadian elections is to ensure voters have sufficient information to make informed decisions. Both the CSE and CSIS have published extensive documents, outlining cyber threats, potential targets, and actors who may conduct influence campaigns during the 2019 election (CSE 2019; CSIS 2018). These reports provide an accurate and transparent depiction of the current geo-political landscape as it pertains to potential influence campaigns, which the public may consult to reinforce or update their belief systems.

On January 30th, 2019, Karina Gould, Harjit Sajjan, and Ralph Goodale, ministers for Democratic Institutions, National Defence, and Public Safety respectively, gave a speech outlining the potential for a foreign influence campaign to be conducted over the course of the 2019 federal election. Their speech assured Canadians that the federal government has acknowledged the threat and has prepared a plan to combat threats against democracy (Gould, Sajjan, and Goodale 2019). Minister Gould would go on to say that “the strongest defence against threats to democracy is an engaged and informed public” (Gould, Sajjan, and Goodale 2019), to her remark the federal government has committed \$7 million towards digital literacy programs to assist Canadians critically assess information, understand how actors can manipulate

algorithms, and acquire necessary skill to prevent manipulation online (Gould, Sajjan, and Goodale 2019).

In the event of a critical incident related to the election, the ministry of Democratic Institutions has established a public protocol. Upon being made aware of a threat the ministry will share information through the relevant agencies who can then critically assess the potential damage, where the public will then be made aware of the current facts and measures they can take to protect themselves (Critical Election Incident Public Protocol 2019).

This last section has outlined the state of Canadian election security. I will now turn to a detailed analysis of specific risks, focusing on the aforementioned groups at risk – election infrastructure, political parties and politicians, and voters – attempting to delineate the hazards Canada faces for the 2019 federal election.

What's the Risk?

Following an in-depth analysis of non-linear warfare, Canada's security environment, and Canadian safeguards to defend elections, this section proposes a risk analysis for the 2019 federal election based on the previously identified threats and safeguards.

- **Threat:** Threats are identified as anything that would create an effect of tampering, destruction, or interruption around the elections infrastructure, political parties, politicians, or voters.
- **Group at Risk:** Identifies whom is at risk to the threat. In the case where there are multiple groups listed, groups are ranked by the potential impact of the threat.
- **Tactics:** This category ascribes the potential tactics used by hostile actors to achieve a strategic goal, or ensure the threat comes to fruition. In the case where there are multiple tactics, these are not ranked.

- **Worst Case Scenario:** If a hostile actor successfully follows through with the threat, what would be the worst-case scenario as it pertains to the 2019 federal election. This section does not make assumptions to the larger societal impacts that may occur, it exclusively focuses on the election period leading up to the 2019 federal election.
- **Safeguards:** This category briefly identifies what safeguards are currently in place, as described in the previous section.
- **Hazard Classification:** Ranks the severity of the threat based on the worst-case scenario on a scale of 1-5, where:

Severity	Description
1	Threat requires significant effort to exploit. The resulting scenario would cause minimal to no harm
2	Threat requires significant effort to exploit. The resulting scenario would cause moderate harm.
3	Threat requires many resources to exploit. The resulting scenario would cause moderate harm.
4	Threat requires some resources to exploit. The resulting scenario would cause moderate harm.
5	Threat requires few resources to exploit. The resulting scenario would cause significant harm.

- **Likelihood of Occurrence:** This category assigns a subjective probability to the likelihood that the threat would be realized at some point during the pre-election and election periods. Likelihood is ranked from 1-5, where

Likelihood	Description
1	Occurrence of threat is low. Threat was sparingly realized in other interference campaigns.
2	Occurrence of threat is low. Threat has been realized in other interference campaigns.
3	Occurrence of threat is moderate. Threat has been realized in other interference campaigns.
4	Occurrence of threat is high. Threat has been realized in other interference campaigns.
5	Occurrence of threat is high. Threat has been used abundantly in other interference campaigns.

- Risk Level:** This category ascribes the level of risk based on a subjective interpretation of the safeguards in place, hazard classification, and likelihood of occurrence. I weight the significance of safeguards as greater importance than hazard classification and likelihood of occurrence. If safeguards are not sufficient then a threat could be readily exploited. As Hazard classification is based on a subjective worst-case scenario, likelihood is also weighted with more significance. Based on this valuation of the prescribed variables, risk is then ranked from 1-10, where:

Risk	Description
1	There are numerous effective safeguards to counter interference efforts; Hazard classification is defined as 1; Likelihood of occurrence is defined as 1
2	There are numerous effective safeguards to counter interference efforts; Hazard classification is defined as 1-2; Likelihood is defined as 1-2
3	There are effective safeguards to counter interference efforts; Hazard classification is defined as 2-3; Likelihood is defined as 2-3
4	There are safeguards to counter interference efforts; Hazard classification is defined as 2-3; Likelihood of occurrence is defined as 2-3

5	There are safeguards to counter interference efforts; Hazard classification is defined as 2-4; Likelihood is defined as 2-4
6	There are some safeguards to counter interference efforts; Hazard classification is defined as 2-4; Likelihood is defined as 2-4
7	There are some safeguards to counter interference efforts; Hazard classification is defined as 3-4; Likelihood is defined as 3-4
8	There are minimal safeguards to counter interference efforts; Hazard classification is defined as 3-5; Likelihood is defined as 3-5
9	There are minimal safeguards to counter interference efforts; Hazard classification is defined as 4-5; Likelihood is defined as 4-5
10	There are minimal or no safeguards to counter interference efforts; Hazard classification is defined as 5; Likelihood is defined as 5

The following two tables place the elements as a risk matrix, where risks are listed from the most concerning to least concerning for the 2019 federal election.

Table 1
Most Concerning Risk Factors and Potential Targets in the 2019 Canadian Federal Elections

Threat	Group at Risk	Tactics	Worst Case Scenario	Safeguards	Hazard Classification	Likelihood of Occurrence	Risk Level
Fake News	1.Voters 2.Parties & Politicians	1.Trolls/Bots 2.Deepfakes 3.Media Ownership 4.Defacing Website	Long-run social instability resulting in moral panics, hysteria, and distrust towards fellow Canadians and democratic institutions.	Online platforms are expected to abide by the Declaration on Electoral Integrity and the Elections Canada Act has legislation on partisan and election advertisements Ultimately voters are responsible for their own actions.	5	5	10
Biased News	1.Voters 2.Parties & Politicians	1.Trolls/Bots 2.Media Ownership	Long-run ideological divisions that may result in a decline in social and political trust between Canadians	Voter information campaigns would assist Canadians in detecting biased content. Ultimately voters are responsible for their own actions.	4	5	9
Political Scandals and Embarrassment	1.Parties & Politicians	1.Spearfishing 2.Hacks	A foreign actor could co-opt a politician, constraining their ability to make policy decisions that are in the best interest for Canadians.	Politicians and parties are responsible for their own actions. There are no institutional safeguards	2	5	8
Coopting Elites	1.Parties & Politicians	1.Spearfishing 2.Hacks 3.Foreign Funding 4.Espionage 5.Blackmail	A foreign actor could co-opt a politician, constraining their ability to make policy decision that are in the best interest for Canadians.	There are safeguards to defend against cyber espionage and mechanisms in the Elections Canada Act to prohibit foreign contributions, however, individuals are responsible for their own actions.	3	5	7
Personal Information Theft	1.Voters	1.Spearfishing 2.Trolls 3.Social Media Sites	A foreign actor would gain access to Canadian's critical infrastructure. In this event, foreign actors could use this information in the future to have more precise attacks.	Online platforms are regulated as to who can acquire personal information and the federal government has programs to ensure voter resiliency against spearfishing.	2	4	7
Coopting Media Institutions	1.Voters	1.Foreign Funding 2.Economic Coercion	Media companies could produce fake news or biased news, which would result in a similar scenario as the news itself.	There are regulations on the advertisements organizations can publish, however, there are no regulations prohibiting foreign ownership of media.	3	4	7

Table 2
Other Risk Factors and Potential Targets in the 2019 Canadian Federal Election

Threat	Group at Risk	Tactics	Worst Case Scenario	Safeguards	Hazard Classification	Likelihood of Occurrence	Risk Level
Voter Database Theft	1. Voters 2. Parties & Politicians	1. Spearfishing 2. Hacks	A foreign actor would gain access to Canada's critical infrastructure. In this event, foreign actors could use this information in the future to have more precise attacks.	The Office of the Privacy Commissioner has provided parties with appropriate steps to protect information from hacks, however, parties are independently responsible.	2	4	6
Coopting Think Tanks/ Universities	1. Voters	1. Foreign Funding 2. Economic Coercion	Trust in academic institutions would decline, resulting in diminished belief in scientific objectivity and undermine expert opinion.	There are no current safeguards	3	2	6
Inhibiting Voter Turnout	1. Election Infrastructure 2. Voters	1. DDoS Attacks 2. Defacing Websites 3. Trolls/Bots	Results would not accurately reflect the views of the population.	The Ministry of Democratic Institutions provides voter information campaigns.	3	3	5
Prevention of Voter Registration	1. Election Infrastructure 2. Voters	1. DDoS Attacks 2. Defacing Websites 3. Trolls/Bots 4. Deepfakes	Undue stress would be placed on Elections Canada Officials and voters, this may result in longer waiting times during pre-election registration or at the polls on election day.	Voter registration can be conducted in person, over the phone, or by mail.	2	3	3
Foreign Contributions to Political Parties	1. Parties & Politicians	1. Donations to Political Parties	A foreign actor could co-opt a politician or party, constraining the ability to make policy decision that are in the best interest for Canadians.	Foreign contributions to political parties and 3rd parties are prohibited	3	2	3
Tampering with Election Results	1. Election Infrastructure 2. Voters	1. Redirect Attacks 2. Trolls/Bots	A short-run fear in the general population, which could result in riots, hysteria, or moral panics.	Elections are conducted with pen and paper.	1	1	1

Modern Problems Require Modern Solutions

Canada and other Western democratic states must recognize and adapt to an evolving foreign policy environment. The Liberal Democratic Order has been challenged by hostile adversaries desiring to undermine its fundamental tenants, while employing all available resources to achieve their strategic goals. In this regard, disinformation and covert measures of influence are here to stay. Canada must accept this new environment and design policies that will allow effective pushback against hostile states and safeguards against new tactics, such as non-linear warfare. To complement a changing international environment, Canada's domestic sphere has also undergone a fundamental change, where the notion of Post-Truth has emerged, functionally undermining the belief in objective truth and eroded our shared moral values, resulting in a decline in our ability to strive towards a uniform objective – a rules based system founded on the principles of human rights and equal opportunity. Recognizing these two central shifts in Canada's policy landscape, there is sufficient grounds to argue that Canadian policy should also undergo a directional shift. While many Canadian policy responses have focused on reactive measures, such as reforming the Elections Canada Act or advertisement restrictions on social media sites, the response moving forward should focus on proactive measures that would mitigate the effectiveness of non-linear warfare and attacks on democracy.

Policy Recommendation

Based on this capstones' risk analysis, the most pressing concerns to Canada's elections centers on disinformation and misinformation, spearfishing and hacks, and co-optation of elites and media. Canada has done well in its efforts to combat foreign interference; however, there are gaps in the current regulation and security environment. To effectively combat these persistent threats, I would like to improve on the recommendation proposed by Marcus Kolga (2019) of the

MacDonald-Laurier Institute, which calls for the creation of a “National Centre for Strategic Communications and Digital Democracy.” This Centre would bring together the Ministries of Public Safety, Democratic Institutions, Foreign Affairs, and National Defence, in addition to the four security agencies (CSE, CSIS, RCMP, and Global Affairs), to develop cohesive strategies to safeguard democracy in Canada against foreign influence campaigns, cyber-attacks, and disinformation. The Centre for Strategic Communications and Digital Democracy would be tasked with four responsibilities:

1. Enhanced Measures to Monitor, Detect, and Identify Disinformation and Influence Campaigns

The first line of defence is knowing a problem exists and where that problem emanates. While Canada security nexus of CSE, CSIS, RCMP, and Global Affairs are rigorous in their operations, there is always room for improvements. To successfully identify and monitor information requires significant resourcing and staff by specialists who understand active non-linear warfare operations, including types of propaganda, its sources, where hostile actors operate, and its targets. As this process is often extremely difficult, even for the most experienced, I suggest three objectives: *first*, there must be an initiative to define “propaganda” that establishes a uniform understanding of various strategies, the distinction between overt, overt, and grey propaganda, and what populations are most at risk.

Second, the Centre should collaborate with internet browser providers to implement machine learning techniques that would identify sources of disinformation and misinformation online, based on the previously defined set of terms. Private organizations such as “FakerFact” or “FakeBox” have developed programs that analyze text and speech online, which can distinguish

various types of text based on its composition (FakerFact 2019; MachineBox 2019). After the text is identified, a code would be assigned to the article that places it into one of six categories: *Journalism, Information, Satire, Sensational, Opinion*, or, *agenda-driven*. The ideal outcome would be for browsers that have a fixed extension built in, that would display a “pop-up” each time a new page was opened, displaying the articles categorization and why it is coded as such. While these technologies are in early stages of development, technological progress follows “Moore’s Law,” where the number of transistors in an integrated circuit doubles every 18 months, which essentially means that technological progress increases exponentially every 18 months (Moore 1965, 115). The federal government should work with browser providers to develop a categorical interpretation of article definitions that effectively identifies credible and non-credible sources of information.

Third, following a similar approach to detecting and identifying categories of information, the Centre should further analytics development around network analysis to identify where sources of propaganda and influence campaigns originate. Identification efforts should draw on experts in the field of data and network sciences in addition to enhanced collaboration with fellow G7 and NATO members to readily share information on influence efforts. This information must be made publically available in a digital and searchable repository to ensure citizens have easy and ready access.

2. Active Measures to Combat Disinformation

I. *Creation of an Office of Information*

The West managed to defeat the Soviet Union during the Cold War largely in part to the West’s abundance of “Soft Power” - a transparent or overt means of persuasion,

to attract and inspire actions (Nye 2004, 5). The advent of blue jeans, rock music, and consumerist ideologies inspired a public infatuation with Western lifestyle in the Soviet Union, ultimately contributing to its demise. The primary focus of Russian influence campaigns centers on the polarization of society by undermining the key tenants of Liberal democracy, in this regard, Canada should actively combat influence efforts with its own strategy of influence directed at its citizens in a transparent manner. The office's focus should be creating and demonstrating Canadian and Liberal values to the public, both domestic and abroad, in a digital environment. This could take the form of targeted content on social media sites that promote acts of civic virtue.

II. *Targeted Social Efforts*

Recognizing the impact of disinformation on certain vulnerable populations, the harm from digital influence efforts have led to tragic real world consequences, such as the emergence of radical ideological networks in “ANTIFA” (Anti-Fascists) and the “Alt-Right,” “Anti-Vaxers,” and climate change deniers. These community's memberships are growing, causing harm not only in their actions but also in the visceral response by onlookers who often despise their beliefs and actions. In both cases polarization increases and democracy is negatively impacted.

The federal government has created a program to combat its domestic terror threats through anti-radicalization efforts with the creation of the “Canada Centre for Community Engagement and Prevention of Violence.” To effectively counter act harmful radical ideologies these communities often require in depth, one-on-one efforts to combat their radicalization, similar to the effect of social work. However,

due to the nature of these populations there is often a great deal of distrust towards elites and legacy institutions. Rather than simply expand the Centre for Community Engagement and Prevention of Violence, I propose the federal government work with non-governmental organizations, non-profit groups, and ex-members of harmful radical groups that could provide anti-radicalization or anti-disinformation counseling to victimized communities.

3. Collaborate with Social Media and Tech Companies

The *Declaration on Electoral Integrity Online* was a critical first step in combating influence efforts on social media; however, there is still room for improvements. The Centre should first be tasked with ensuring that social media companies comply with the existing declaration, requiring that these companies provide a monthly report on troll and bot accounts they have removed, recent efforts to mitigate targeted propaganda campaigns, and transparency on their feed population algorithms. Expanding on the declaration, the Centre should work with social media platforms to display a public “audit” feature on all account pages that would display the following:

- I. A page’s followers separated between genuine and bot accounts,
- II. A count and percentage of a page's posts that are original content, reposts from genuine accounts, reposts from automated or bot driven accounts, posts with redirect links to other sites,
- III. An interactive web that displays a page’s network and the centrality of that page in relation to its larger network,

An audit feature would allow for users to better understand where their information comes from and whether that information is genuine or automated content. This feature could mitigate the effectiveness of bot driven accounts and the ability for hostile actors to leverage algorithmic vulnerabilities on social media platforms, while maintaining an individual's responsibility for action.

The Centre should also ensure that users personal information is protected by requiring social media companies to adopt transparency measures to provide users reports on request regarding the collection, storage, user, and sale of personal information. Finally, the Centre should collaborate with other jurisdictions and governments who are working with social media and tech companies in a similar manner, to share information and strategy to protect citizens online.

4. Create an Accessible Database on the Financing of Universities and Non-Profit Organizations

On average, Canadian Universities receive 50% of its financing from federal and provincial governments and another 25% from tuition fees, the remaining 25% is derived from donations and private grants (Statistics Canada 2017). Universities receive millions of dollars from private funding and in some cases these donations come from foreign entities. Non-profit groups have also been charged with receiving large amounts of funding from foreign sources. These institutions are recipients of foreign funding (in some capacity) and advocates for domestic policy reform, where they often reflect the donor's priorities. To mitigate the effect that foreign contributions may have on Canada's domestic policy environment, I propose the Centre creates and publishes, in a digital, searchable, and accessible form, a database on the financial

contributions from private sources. While this does not prohibit contributions, it will provide transparency to the public and members of government, who could be lobbied for policy reform by these institutions.

Conclusion

Like the Maginot Line in France, Canada's democratic institutions have been fundamentally subverted by hostile actors who developed new means of warfare. Technological developments along with the conditions of Liberal society has allowed for hostile foreign actors to conduct targeted interference campaigns against Canada's democratic institutions. The result of these campaigns has been less disastrous in Canada than other Western Liberal states, such as the USA or United Kingdom, largely in part due to Canada's relative lesser standing in the international environment and effective safeguards. While the effect may be less catastrophic, there is still a great deal to worry about. The behaviour of hostile foreign actors have attempted to fundamentally undermine Canadian institutions through coordinated non-linear warfare campaigns designed to polarize Canadians and coopt the sovereign policy decisions of government officials. As actors in the international environment continue to push-back against a rules-based system, Canada and other states will continue to be a target for these interference campaigns.

Canadian policymakers have indicated a willingness to move in a direction that would quell the efforts of these hostile states, however, their actions have not been sufficient to effectively mitigate risk. Due to a lack of safeguards and current tensions with Russia and China, Canada will be a target for interference campaigns in the 2019 federal election. Russia's campaign will continue to focus on polarizing Canadian society through disinformation campaigns, while China is more likely to focus on creating biased content and coopting political

and economic elites. In both cases, the fundamental tenants of free and fair elections will be eroded leading up to the 2019 election. While it is too late to implement these policy suggestions for the upcoming election, Canada should explore proactive policy solutions in the future that could suppress a threat prior to occurring. In addition, voters should attempt to inform themselves on tactics employed by these actors and how to prevent falling victim to influence campaigns by foreign governments. The Canadian security environment has undergone a fundamental shift due to new actors and new tactics, in order for Canada to effectively defend itself against future non-linear warfare campaigns, Canada's policy environment must also undergo a fundamental change; focusing on subduing attacks prior to a threat coming to fruition.

References

- Albright, Johnathan. 2016a. "#Election2016: Propagandalytics & Weaponized Shadow Trackers." *Medium*. Accessed May 17, 2019. <https://medium.com/@d1gi/election2016-propaganda-lytics-weaponized-shadow-trackers-a6c9281f5ef9>
- 2016b. "The #Election2016 Micro-Propaganda Machine," *Medium*. Accessed May 17, 2019. <https://medium.com/@d1gi/the-election2016-micro-propaganda-machine-383449cc1fba>
- Bartles, Charles K. 2016. "Getting Gerasimov Right." *Military Review*, January-February: 30-38.
- Banasik, Mirosław. 2016. "Unconventional War and Warfare in the Grey Zone: The Spectrum of Modern Conflict," *Journal of Defense Resources Management*, 1(1): 37-46.
- Blackwell, Tom. 2017. "Russian Fake-News Campaign Against Canadian Troops in Latvia Includes Propaganda About Litter, Luxury Apartments." *National Post*, November 17. <https://nationalpost.com/news/canada/russian-fake-news-campaign-against-canadian-troops-in-latvia-includes-propaganda-about-litter-luxury-apartments>
- Brady, Anne-Marie. 2015. "China's Foreign Propaganda Machine." *Journal of Democracy*, 26(4). 51-59.
- 2017. "Magic Weapons: China's Political Influence Activities under Xi Jinping." Conference Paper presented at The Corrosion of Democrat Under China's Global Influence. Arlington, Virginia. September 16-17.
- 2018. "Exploit Every Rift: United Front Goes Global." *Party Watch Annual Report*. 34-40.
- Bowe, Alexander. 2018. "China's Overseas United Front Work: Background Implications for the United States." *U.S-China Economic and Security Review Commission*. August 24.
- Broniatowski, David, Amelia M. Jamison, SiHua Qi, Lulwah AlKulaib, Tao Chen, Adrian

- Benton, Sandra C. Quinn, and Mark Dredze. 2018. "Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate," *American Journal of Public Health*, 108(10): 1378-1384.
- Burke, Eugene. 2017. "Big Data and Predictive Analytics: Opportunity or Threat to the Future of Tests and Testing." In *Psychometric Testing*, edited by Barry Cripps, 43-58. Wiley-Blackwell.
- Canada. 2019. Communications Security Establishment (CSE). *2019 Update: Cyber Threats to Canada's Democratic Process*. Ottawa: Ont.
- 2019. Special Economic Measures Act: Canadian Sanctions Related to Russia (SOR/2019-71). Ottawa: Ont. April 12. Last modified on April 12, 2019.
https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/russia-russie.aspx?lang=eng#a6_1
- 2019. Ministry of Democratic Institutions. *Combatting Foreign Interference*. Ottawa: Ont. January 30. Last modified on July 9, 2019.
<https://www.canada.ca/en/democratic-institutions/news/2019/01/combating-foreign-interference.html>
- 2019. Ministry of Democratic Institutions *Critical Election Incident Public Protocol*. Ottawa: Ont. February 7. Last modified July 9, 2019. <https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/public-protocol.html>
- 2019. Ministry of Democratic Institutions *Canada Declaration on Electoral Integrity Online*.

Ottawa: Ont. May 27. Last modified May 27, 2019.

<https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/declaration-electoral-integrity.html>

--- 2019. Office of the Privacy Commissioner. *Guidance for Federal Political Parties on Protecting Personal Information*. Ottawa: Ont. April 1. Last modified April 1, 2019.

https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/gd_pp_201904/

--- 2018. Canadian Security Intelligence Service (CSIS). *Who Said What? The Security Challenges of Modern Disinformation*. Ottawa: Ont. February 2018. Last modified May

4, 2019. <https://www.canada.ca/en/security-intelligence-service/corporate/publications/who-said-what-the-security-challenges-of-modern-disinformation.html>

--- 2018. *Operation UNIFER*. Ottawa: Ont. Retrieved from Current Operations list of National Security and Defence. Ottawa: Ont. December 3. Last modified December 3, 2018.

<https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-unifier.html>

--- 2017. Communications Security Establishment (CSE). *Cyber Threats to Canada's Democratic Process*. Ottawa: Ont.

--- 1991. Royal Commission on Electoral Reform and Party Financing. *Reforming Electoral Democracy*. Ottawa: Ont. Volume 1.

Canada Elections Act, Statutes of Canada (2000, c. C-9). Retrieved from the Justice Laws website: <https://laws-lois.justice.gc.ca/PDF/E-2.01.pdf>

Canadian Security Intelligence Service Act, Revised Statutes of Canada (1985, c. C-23).

Retrieved from the Justice Laws website: <https://laws-lois.justice.gc.ca/PDF/C-23.pdf>

- Carty, Victoria. 2011. *Wired and mobilizing*. London: Routledge.
- Castels, Manuel. 2001. *The Internet Galaxy*. London: Oxford University Press.
- Chakravorti, Bhaskar, Christopher Tunnard, and Ravi Shankar C. 2015. “The Way to Estonia: How to Reach Digital Nirvana.” *Foreign Affairs*, March 24.
<https://www.foreignaffairs.com/articles/global-commons/2015-03-24/way-estonia>
- Chanda, Nayan. 2015. “The Silk Road – Old and New.” *YaleGlobal Online*, October 26.
<https://yaleglobal.yale.edu/content/silk-road-old-and-new>
- Charvet, John and Elisa Kaczynska-Nay. 2008. *The Liberal Project and Human Rights: The Theory and Practice of a New World Order*. New York: Cambridge University Press.
- Chesney, Robert and Danielle Citron. 2019. “Deepfakes and the New Disinformation War: The coming Age of Post-Truth Geopolitics,” *Foreign Affairs*, January/February.
<https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war>
- China Association for International Friendly Contact (CAIFC). 2019. “About the China Association for International Friendly Contact (CAIFC).” March 27.
<http://www.caifc.org.cn/en/content.aspx?id=616>
- Chivvis, Christopher. 2017. “Understanding Russian “Hybrid Warfare” And What Can Be Done About It,” *Testimony presented before the House Armed Services Committee*, March 22.
- Davis, Susan (*Rapporteur*). 2018. “Russian Meddling in Elections and Referenda in the Alliance,” *NATO Parliamentary Assembly, Science and Technology Committee*,
- Deibert, Ronald. 2015. “Cyberspace Under Siege.” *Journal of Democracy*, 26(3): 64-78.
- DiResta, Renée. 2018a. “The Digital Maginot Line.” *Ribbonfarm.com*. November 28, 2018.

- <https://www.ribbonfarm.com/2018/11/28/the-digital-magnot-line/>
- 2018b. "Computational Propaganda: If You Make It Trend You Make It True." *Yale Review*, 106(4):12-29.
- 2017. "There are Bots. Look Around," *Ribbonfarm.com*, May 23.
- <https://www.ribbonfarm.com/2017/05/23/there-are-bots-look-around/>
- Duckworth, Grant. 2018. "A Made-in-Canada China Strategy for 2018?" *Canadian International Council*, September 10. https://thecic.org/en/a-made-in-canada-china-strategy-for-2018/#_ftn8
- Elections Modernization Act, Statutes of Canada (2018, c. C-31). Retrieved from the Justice Laws website: https://laws-lois.justice.gc.ca/eng/annualstatutes/2018_31/page-1.html
- Entman, Robert and Andrew Rojecki. 1993. "Freezing Out the Public: Elite and Media Framing of the U.S. Anti-Nuclear Movement." *Political Communication* 10(2): 155-173.
- EU vs. Disinfo. 2018. "Top 3 Ways to Spread Disinformation About Military Exercises." October 25. <https://euvdisinfo.eu/top-3-ways-to-spread-disinformation-about-military-exercises/>
- Facebook. 2019. "Advertising Policies: Restricted Content." https://www.facebook.com/policies/ads/restricted_content/political
- FackerFact. 2019. "About." *FackerFact.org*. <https://www.fakerfact.org/about>
- Finlay, Sean. 2014. *Predictive Analytics, Data Mining and Big Data*. Basingstoke: Palgrave Macmillan.
- Fredkin, Kim and Patrick Kenney. 2012. "Impact of Negative Campaigning on Citizens' Actions and Attitudes." In *The Sage Handbook of Political Communication*, edited by Holi Semetko and Margaret Scamelli, London: Sage Publishers.

- Gamson, William. 1992. *Talking politics*. New York: Cambridge University Press.
- Gibson, Rachel and Stephen Ward. 2012. "Political Organizations and Campaigning Online." In *The Sage Handbook of Political Communication*, edited by Holi Semetko and Margaret Scamelli, 62-74. London: Sage.
- Giles, Keir. 2016. "Russia's New Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power," *Chatham House, Russia and Eurasia Program*.
- Gould, Karina, Harjit S. Sajjan, and Ralph Goodale. 2019. "The Government of Canada's Plan to Safeguard Canada's 2019 Election. *Speech*, January 30.
- <https://www.canada.ca/en/democratic-institutions/news/2019/03/speech-the-government-of-canadas-plan-to-safeguard-canadas-2019-election.html>
- Green, Joshua and Sasha Issenberg, 2016. "Inside The Trump Bunker, With Days To Go." *Bloomberg.com*, October 27. https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go?utm_content=business&cmpid=socialflow-twitter-business&utm_campaign=socialflow-organic&utm_source=twitter&utm_medium=social
- Greitens, Sheena Chestnut. 2013. "Authoritarianism Online: What Can We Learn from Internet Data in Nondemocracies?" *Political Science and Politics* 46(02): 262–70.
- Harrell, Peter, Elizabeth Rosenberg, and Edoardo Saravalle. 2018. "China's Use of Coercive Economic Measures." *Center for a New American Security*. Energy, Economics, and Security, June 11.
- Han, Rongbin. 2015. "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army.'" *Journal of Current Chinese Affairs* 44(2): 105–34.
- Helmus, Todd, Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua

- Medelsohn, William Marcellino, Andriy Bega, and Zev Winkelam. 2018. "Russian Social Media Influence," *Rand Corporation*.
- Higgins, Tory and Gillian King. 1982. "Individual Construct Accessibility and Subjective Impressions and Recall." *Journal of Personality and Social Psychology*, 43(1): 35-47.
- Hersh, Eitan. 2015. *Hacking the Electorate*. Cambridge: Cambridge University Press.
- Hoffman, Frank. 2007. "Conflict in the 21st Century: The Rise of Hybrid Wars," Potomac Institute for Policy Studies, Virginia.
- Holden, Michael, and Jack Stubbs. 2019. "Five Eyes Will Not Use Huawei in Sensitive networks – Senior US Official." *Reuters*. April 24.
<https://ca.reuters.com/article/companyNews/idCAL5N2263UN>
- Joye, Christopher. 2013. "Transcript: Interview with Former CIA, NSA Chief Michael Hayden." *Financial Review.com*. July 19.
- Kahneman, Daniel and Amos Tversky. 1984. "Choices, Values, and Frames." *American Psychology Association*, 39(4): 341-350.
- King, Gary, Jennifer Pan, and Margaret E. Roberts. 2017. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument." *American Political Science Review*, 111(3): 434-501.
- Kleemola, Katie, and Seth Hardy. 2013. "Surtr: Malware Family Targeting Tibetan Community." *CitizenLab and Munk School of Global Affairs*.
<https://citizenlab.ca/2013/08/surtr-malware-family-targeting-the-tibetan-community/>
- Kreiss, Daniel. 2016. *Prototype Politics*. New York, NY: Oxford University Press.
- Kolga, Marcus. 2019. "Stemming the Virus: Understanding and responding to the threat of Russian Disinformation." *Macdonald-Laurier Institute*. January.

- Kosinski, Michael, David Stillwell, and Thore Graepel. 2013. "Private Traits and Attributes are Predictable from Digital Records of Human Behavior." *Proceedings of The National Academy of Sciences*, 110(15): 5802-5805.
- Kurlantzick, Joshua. 2007. *Charm Offensive: How China's Soft Power is Transforming the World*. New Haven: Yale University Press.
- Kynge, James, Lucy Hornby, and Jamil Anderlini. 2017. "Inside China's Secret 'Magic Weapon' for Worldwide Influence." *Financial Times*, October 25.
<https://www.ft.com/content/fb2b3934-b004-11e7-beba-5521c713abf4>
- Lanoszka, Alexander. 2016. "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe," *International Affairs* 92(1): 175-195.
- Lepido, Daniele. 2019. "Vodafone Found Hidden Backdoors in Huawei Equipment." *Bloomberg.com*. April 30. <https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment>
- MachineBox. 2019. "FakeBox." *MachineBox.io*.
<https://machinebox.io/docs/fakebox#usesforfakebox>
- Marland, Alex. 2017. *Brand Command*. Vancouver: UBC Press.
- Mattis, Peter. 2018. China's 'Three Warfares' in Perspective." *War on the Rocks*, January 30.
<https://warontherocks.com/2018/01/chinas-three-warfares-perspective/>
- McCombs, Maxwell and Daniel Shaw. 1972. "The Agenda-Setting Function of Mass Media." *Public Opinion Quarterly* 36(2): 176-187.
- McCulloh, Timothy and Richard Johnson. 2013. "Hybrid Warfare," *Joint Special Operations University, Report* 13-4.
- Miller, Greg. 2018. *The Apprentice: Trump, Russia and the Subversion of American Democracy*.

- New York: Custom House Publishing.
- Moore, Gordon E. 1965. "Cramming More Components onto Integrated Circuits." *Electronics* 38(8): 114-118.
- National Defence Act, Revised Statutes of Canada (1985, c. N-5). Retrived from the Justice Laws website: <https://laws-lois.justice.gc.ca/PDF/N-5.pdf>
- Natsional Sluzhba Novostey. 2015. "Potomki Galichan Prevratili Kanadu v Zhupel Rusofobii v 'Semerke'?" June 5, 2015. <https://nsn.fm/in-the-world/in-the-world-potomki-galichan-prevratili-kanadu-v-glavnogo-rusofoba-bolshoy-semyerki->
- North Atlantic Treaty Organization (NATO). 2018a. "Confucius Institutes." *NATO Strategic Communications*.
- 2018b. "Chinese Public Diplomacy in Taiwan." *NATO Strategic Communications*.
- Nye, Joseph. 2004. *Soft Power: The Means to Success in World Politics*. New York: Public Affairs.
- Ottis, Rain. 2008. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." Paper presented at the Conference Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth: Massachusetts.
- Paul, Christopher and Miriam Matthews. 2016. "The Russian Firehose of Falsehood Propaganda Model," *Rand Corporation*.
- Pomerantsev, Peter. 2015. "Authoritarianism Goes Global (II): The Kremlin's Information War," *Journal of Democracy* 26(4): 40-50.
- Pomerantsev, Peter and Michael Weiss. 2014. "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture, and Money," *Institute of Modern Russia and The Interpreter*, November 17.

Porup, J.M. 2019. “How and Why Deepfake Videos Work – and What is at Risk.”

CSOonline.com. Accessed June 15, 2019.

<https://www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html>

Posters, Bill (Bill_Posters_UK). 2019. “When There’s So Many Haters...” *Instagram*. June 1.

<https://www.instagram.com/p/ByKg-uKlP4C/>

PostMedia. 2019. “Follow the Money.” *National Post*. Accessed on June 28, 2019.

<https://special.nationalpost.com/follow-the-money/feature>

Privacy Act, Revised Statutes of Canada (1985, c. P-21). Retrieved from the Justice Laws

website: <https://laws-lois.justice.gc.ca/eng/acts/p-21/>

Proctor, Jason. 2019. “‘Poor Canada’: Will Meng Wanzhou Extradition Hearing Threaten

National Interest?” *CBC*, May 3. [https://www.cbc.ca/news/canada/british-](https://www.cbc.ca/news/canada/british-columbia/meng-wanzhou-extradition-chinese-huawei-1.5089840)

[columbia/meng-wanzhou-extradition-chinese-huawei-1.5089840](https://www.cbc.ca/news/canada/british-columbia/meng-wanzhou-extradition-chinese-huawei-1.5089840)

Qing, Koh Gui and John Shiffman. 2015. “Beijing’s Covert Radio Network Airs China-Friendly

News Across Washington, and the World.” *Reuters*, November 2.

<https://www.reuters.com/investigates/special-report/china-radio/>

Radin, Andrew. 2017. “Hybrid Warfare in the Baltics: Threats and Potential Responses.” *Rand Corporation*.

Repnikova, Maria. 2018. “How Chinese Authorities and Individuals Use the Internet.” *Hoover Institute: Stanford*. Fall Series: 218.

Schnauffer II, Tad. 2017. “Redefining Hybrid Warfare: Russia’s Non-Linear War Against the West,” *Journal of Strategic Security* 10(1): 17-31.

- Shen, Foyuan. 2004. "Chronic Accessibility and Individual Cognitions: Examining the Effects of Message Frames in Political Advertisements." *Journal of Communication* 54(1): 125-137.
- Sigur Center for Asian Studies. 2019. "Countering China's Sharp Power" Disinformation and Social Media in Taiwan." *Asia Report*. 44: January.
- Snow, David, E. Burke Rochford, Jr., Steven Worden and Robert Benford. 1986. "Frame Alignment Processes, Micromobilization, and Movement Participation," *American Sociological Review* 51(4): 464-481.
- Sukhankin, Sergey. 2019. "Canada and the Western alliance in the face of Russian (dis)information onslaught." *The School of Public Policy Publications* (forthcoming - fall 2019).
- Thompson, Nicholas and Issie Lapowsky. 2018. "How Russian Trolls Used Meme Warfare to Divide America," *Wired.com*, December 17. <https://www.wired.com/story/russia-ira-propaganda-senate-report/>
- Tilly, Charles. 2006. *Regimes and Repertoires*. Chicago: University of Chicago Press.
- Tilly, Charles and Sidney Tarrow, 2005. *Contentious politics* (1st ed.). Oxford: Oxford University Press.
- Timberg, Craig and Tony Romm. 2018. "These Provocative Images Show Russian Trolls Sought to Inflamm Debate Over Climate Change, Fracking and Dakota Pipeline," *Washington Post*, March 1. <https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/congress-russians-trolls-sought-to-inflame-u-s-debate-on-climate-change-fracking-and-dakota-pipeline/>
- Thaler, Richard and Cass Sunstein. 2008. *Nudge*. Penguin Books: London.

- Thompson, Elizabeth. 2019a. "Twitter Banning Political Ads in Canada Until Election Campaign." *CBC*, June 26. <https://www.cbc.ca/news/politics/twitter-online-advertising-election-1.5190465>
- 2019b. "Facebook Rolls Out High-Tech Ad Registry with a Low-Tech Twist." *CBC*, June 10. <https://www.cbc.ca/news/politics/facebook-political-ad-registry-canada-1.5167413>
- Thornton, Rod. 2015. "The Changing Nature of Modern Warfare." *The RUSI Journal*: 160(4), 40-48.
- Towers-Clark, Charles. 2019. "Mona Lisa and Nancy Pelosi: The Implications of DeepFakes." *Forbes.com*, May 31. <https://www.forbes.com/sites/charlestowersclark/2019/05/31/mona-lisa-and-nancy-pelosi-the-implications-of-deepfakes/#613052a54357>
- Tufekci, Zeynep. 2014. "Engineering the public: Big data, Surveillance and Computational Politics." *Firstmonday.org*: 19(7). <https://firstmonday.org/article/view/4901/4097>
- U.S. 2014. *Joint Publication 3-05: Special Operations*, (Washington: July 16, 2014): II-9
- U.S. Department of the Army, 2008. "Special Operations Forces Unconventional Warfare." *FM 3-05.130*. September 2008: 6-1-2.
- U.S. Department of Justice, 2014. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." *Office of Public Affairs*. Monday, May 19. <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>
- U.S.- China Economic and Security Review Commission. 2018. "U.S.- China Economic and Security Commission." *Report to Congress*. November 14.
- Von Clausewitz, Carl. 1832. *On War*. Baltimore: Penguin Books.

- Walker, Christopher and Jessica Ludwig. 2017. "The Meaning of Soft Power." *Foreign Affairs*. November 16. <https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power>
- Woolley, Samuel and Philip Howard. 2016. "Political Communication, Computational Propaganda, and Autonomous Agents," *International Journal of Communication* 10: 4882-4890
- Woods, Karen. 2018. "Huawei Crises Has Chinese Canadians Worried." *The Star*, December 2018. <https://www.thestar.com/opinion/contributors/2018/12/18/huawei-crisis-has-chinese-canadians-worried.html>
- Wortzel, Larry M. 2014. "The Chinese People's Liberation Army and Information Warfare." *United States Armywar College Press*. Strategic Studies Institute.
- Yang, Yuan. 2017. "China's Communist Party Raises Army of Nationalist Trolls." *Financial Times*, December 29. <https://www.ft.com/content/9ef9f592-e2bd-11e7-97e2-916d4fbac0da>
- Zhang, Ketian Vivian. 2019. "Chinese Non-Military Coercion – Tactics and Rationale." *Brookings*, January 22. <https://www.brookings.edu/articles/chinese-non-military-coercion-tactics-and-rationale/>