Western
University

Visualizing Canada's Future in the Fifth Dimension

A Project by Western University's
International Relations Class of 2019

Authors

Bridget Collrin
Marisa Coulton
Alana Cress
Cassandra DiFelice
Davide DiTaranto
Jared Forman
Lena Gahwi
Omar Ghanie
Maxwell Gill
Kelsey Hierlihy
Jihwan Steven Kim
Abby MacDonald
Hilary Koum Njoh
Mark Omenugha
Ian Orr
Matt Sparling
Monika Stolarski
Ariela St-Pierre-Collins
Lyndsay-Marie Talon
Lucas Tersigni
Amy Timmerman
Joshua Tong
Jacob VanderBurgt
Gabriella Yankowich

Supervisors

Professor Francine McKenzie
Department of History
University of Western Ontario

Professor Dan Bousfield
Department of Political Science
University of Western Ontario

Table of Contents

Executive Summary

This report assesses the major challenges and risks associated with cyberspace and how the Government of Canada can navigate these issues through a new regulatory framework. The goal for this new framework is for Canada and the international community to develop an international cyber regime that promotes innovation; facilitates access to credible information; protects individual and state well-being; brings about government and corporate transparency and accountability; and engenders stability, trust and cooperation among all major stakeholders.

This report begins with an introduction that outlines the importance of regulating cyberspace, especially given the recent push from New Zealand after the Christchurch Mosque Massacre. That event, which was broadcast live on Facebook by the shooter himself, shows that both Canada and the rest of the international community need to make major changes to cyber-related policies to ensure that such an event cannot happen again. As a result, this report has been broken into six different sections which examines a wide range of issues that face both domestic and international regulators. These parts are: International Development, Corporate Considerations, Individual Privacy Rights, Canada's 5G Networking, Information Warfare, and Election Interference.

Each section will examine relevant cases and highlight the regulatory risks and challenges associated with these specific issues.

Additionally, they will make a recommendation based on these findings that coincide with the goals outlined above. Section-specific recommendations are as follows: the International Development section will recommend that Canada and IGOs incorporate cyber-capabilities and cryptocurrencies into their delivery of development aid; the Corporate Considerations section will recommend that governments regulate channels through which corporations interact with the internet to ensure that these interactions are secure and direct self-interested behaviour to benefit the public good; the Individual Privacy Rights section will recommend that governments and corporate actors work to protect the individual's right to personal privacy and control over the collection and use of individual private data, and prevent the misuse of this information; the section on Canada's 5G Networking will recommend that the Government of Canada explore alternatives to Huawei's 5G technology to maintain Canada's relationship with the US and its position in the Five Eyes network; the Information Warfare section will recommend that governments mitigate the ability of non-state actors to weaponize information and utilize information warfare tactics; and, the Elections Interference section will recommend that states should assist corporate, civil society, and individual actors to mitigate the spread of mis/disinformation that can be harmful to democratic processes. At the conclusion of the case studies, we have provided a full reflection of all of the recommendations as well as an audit of each section using international relations theory will be provided.

Introduction

On Friday March 15th, 2019 an assailant equipped with an assault rifle covered with hate slogans live-streamed the massacre of over fifty innocent civilians gathered in a mosque in Christchurch, New Zealand. In the aftermath of the shooting, one of the first conversations New Zealand's Prime Minister had was with Facebook executive, Sheryl Sandberg, in a plea to the social media giant to stop the spread of hate speech and remove all instances of the video.

Australian Prime Minister Scott Morrison reacted to the event by penning a letter to Japan's Prime Minister Shinzo Abe, urging him to bring internet regulations to the forefront of the upcoming June 2019 G-20 summit in Osaka. In the letter, Morrison called it "unacceptable to treat the internet as an ungoverned space," calling for world leaders to lay out "clear consequences" for those individuals who proliferate extremism online, as well as those companies which facilitate terrorism and the spread of extremist ideas.[1]

This year marks the 30th anniversary of the internet and there has never been a greater urgency for the development of cyber regulations in the form of a cyber regime. Since its inception, regulation of the internet has been limited, making it emblematic of a lawless space akin to the Wild West. The tragedy at Christchurch highlights the stark reality of the lack of regulations online. Twenty-four hours after the event occurred, there were over 1.5 million versions of the video portraying the massacre circulating on Facebook's platform. However, by the time Facebook took action and deleted many of these instances, there were already millions more of the video circulating across the web through alternative websites.[2]

Considering the upcoming G-20 summit, Prime Minister Morrison's call to action indicates the timeliness of this report. The research and findings of this report lay out the guiding principles necessary for Canada to lead these discussions of cyber regulations at the G20, and take a leadership role in developing a subsequent international cyber regime. The recommendations in this project address the concerns and interests of various stakeholders in cyberspace, including individuals, civil society groups, private corporations, non-profit organizations, state actors and international organizations. This report provides a set of recommendations based on an analysis of the major challenges, risks, and benefits of cyberspace. They will better position Canada and the international community to develop a cyber regime that promotes innovation, facilitates access to credible information, protects individual and state well-being, encourages government and corporate transparency and accountability, while finally engendering trust and cooperation among people, non-state actors, the private sector, and states.

Cyberspace is omnipresent. It is a tangible extension of the human experience, in which both the negative and positive aspects of humanity can be either amplified or suppressed. This project is founded on the belief that the development of norms through effective cyber governance is able to promote the potentially beneficial elements of cyberspace while tempering its negative impact.

Definitions

5G: 5G or the "Fifth Generation," the newest iteration of wireless technology, is specifically engineered to significantly increase speed and responsiveness. The speed at which the 5G functions is fast enough to support innovative technology such as self-driving cars and Artificial Intelligence.

Anti-Intellectualism: Anti-intellectualism is discourse against largely accepted scientific ideas and literature. It is propagated through online mediums, specifically utilizing information warfare to spread their message. This includes the anti-vaccination movement and climate denial, and also can include general attacks on those who are highly educated.

Blockchain: Blockchain is the main book of all Cryptowatch (see definition below) transactions. Blockchain records individual transactions and ownership of all cryptocurrencies which are in circulation, and this system is managed by the blockchain 'miners' who have to update all transactions that have occurred and ensure the accuracy of the information. In this way, the security of the transaction is confirmed.

Censorship: Censorship is the monitoring, suppression, or regulation of what can be accessed, consumed, or published on the basis that it is considered harmful, false, or misleading. Internet censorship can be enacted in reaction to political concerns such as opposition to the government, minority oppression and human rights violation, or social concerns regarding sexual content, illegal substances, or other topics perceived as offensive or sensitive. It can be carried out by governments, private actors, or corporations.

Civil Society Actors: Civil society actors are groups of people that are distinct from the government and business sectors. Civil society actors are tasked with working in the best interests of citizens and act to hold governments and corporations accountable for their actions.

Cryptocurrency/Digital Currency: Cryptocurrency is a digital asset designed to work as a medium of exchange in return for goods, services, and/or national currencies. Cryptocurrency functions with the help of a technique called cryptography which is a process that translates legible information into codes that cannot be broken. Bitcoin is an example of a cryptocurrency.

Cryptowatch: Cryptowatch is comparable to a stock exchange, but for cryptocurrency. Cryptowatch is a website wherein users can see real-time pricing for different cryptocurrencies which are tradeable.

Cyber Literacy: This is defined as the ability to use technological devices that have access to the internet effectively while understanding both the opportunities as well as the implications that result from this form of engagement. The promotion of cyber literacy is critical to society's growing dependence on technology as it is a necessity to better protect themselves and others while interacting with cyberspace. This includes being aware of disinformation campaigns, identifying reliable sources, and preventing the propagation of fake news (see definition).

Cyberspace: An “amorphous, supposedly ‘virtual’ world created by links between computers, Internet-enabled devices, servers, routers, and other components of the Internet’s infrastructure.” In the 1990s, cyberspace was a term used to describe the “location” in which people interacted with each other while using the Internet. Today, the definition of Cyberspace is broader: “the ubiquitous space that exists in relation to the Internet”, as well as “a dynamic broad domain ranging from Internet and its infrastructures to social networks.”[3]

Cyber Technology: Cyber technology is the blanket term used in this report to define online services, technologies, and products, including but not limited to: social media platforms, computer servers, mobile phones, streaming services, online banking and record keeping, personal computers, email, cryptocurrency, and internet provision infrastructure.

Data Processing, or Processing: Data processing is any action taken utilizing personal data, either manually or automatically, including but not limited to: collecting, recording, organizing, structuring, storing, deleting, transferring, altering, using, or disclosing this data.

Data Profiling, or Profiling: Data Profiling is the automated processing of individual data, for the purposes of identifying specific aspects about the individual in question, either for a single use or for retention as part of a collection of data on said individual.

Data Sovereignty: Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located.
In states with developed internet infrastructure, this is not an issue, however, in states that are reliant on external internet infrastructure, this can be difficult to attain.

Digital Weapons/Arms: Digital weapons/arms are exploits (see definition) that pose security risks. They may cause serious breaches of classified data, a calamitous breakdown in the functionality of essential infrastructure, and may provide unfettered control of remote computer software and networks.

Disinformation: Disinformation is the deliberate act by a state, collective group, or individual actor to spread information that is completely or partially false with aspirations of convincing citizens of untruth. It is often used in propaganda campaigns to influence the public and obscure the truth. Disinformation should not be confused with misinformation, information that is unintentionally false.

Election Interference: Election Interference has been an issue which dates back prior to the introduction of cyber technology. It has evolved as a consequence of the cyberspace. Presently, election interference concerns go beyond tampering with votes and hacking into systems to change results. It consists of several tactics to mislead users online and target them with mis/disinformation about adversarial political parties and their leaders. This is done to try to influence voters to change their voting preferences or abstain from voting in general. Election interference may manifest in the form of fake news articles, forged political party social media accounts, and targeted advertisements that build upon algorithms to reinforce an echo chamber.

Exabyte: Exabyte refers to an enormous size of data; one exabyte is equivalent to one billion gigabytes. In 2018, total world cellular data usage was calculated at 15.8 exabytes.

Exploits: Exploits are packets of computer code that allow hackers to capitalize on vulnerabilities and shortcomings in otherwise inaccessible computers, networks, and software.

Fake News: Fake news is the term used to describe content containing disinformation which is deliberately spread on traditional news and/or online social media platforms. It is used in reference to traditional media outlets like CNN and Fox News, as well as online blogs and websites, spreading false information for political ends.

Formal Channels of Terrorism Information Operations: Formal channels of Terrorism Information Operations include formally released communiqués, platforms such as billboards in areas that terrorist groups control, online publications (such as Dabiq magazine for IS), and officially sponsored videos. The goal of formal channels is to deprive populations from reliable sources of information and instead amplify and support a group's narratives and ideological positions while simultaneously creating perceptions of legitimacy for the group.

Individual Data: Individual Data is data generated by the actions of a single online user, relating to a single identifiable individual, ranging from: metadata about their device and network, online address access history, information, and keystrokes entered while online, messages sent and received, or any other form of data generated by their online actions.

Individual Data Profile: Individual Data profile is a collection of individual data collected about a single user and compiled into a single location, file, or server. This can be processed via any means, and enables any actor to view much or all of the individual data collected by the actor in question from a single source.

Informal Channels of Terrorism Information Operations: Informal channels of terrorism information operations refers to terrorist members' use of mobile phones and social-media forums like Twitter, Diaspora, Reddit, and Facebook to send text, photo, and video messages in an unofficial capacity in an effort to spread their group's message. Informal channels aim at covertly disrupting narratives provided by adversaries.

Information Warfare: Information warfare refers to the development and use of synthetic technologies with the intent of influencing and managing mass opinion in a rival or opponent state.

Internet Backbone: The internet backbone refers to the major networks provided by Internet Service Providers (ISPs).

Internet Exchange Point (IXP): Also referred to as Internet Exchanges (IXs) or Network Access Points (NAPs), Internet exchange points allow for the transfer of data from one network to another. Therefore, the presence of IXPs is required for interaction between two different networks.

Internet Infrastructure: Internet infrastructure is the current physical infrastructure through which computers can connect with the internet and with other computers.

Internet of Things: The Internet of Things refers to the interconnection via the internet embedded in everyday devices that allows individuals to transmit and receive data rapidly. This includes devices such as smartphones, smart watches, and tablets.

Internet Service Providers (ISPs): ISPs create the infrastructure which allows consumers to connect to other individuals on their network, often for a fee.

Knowledge Product: According to the Inter-American Development Bank, a knowledge product is a publication of research that is conducted through funding from IGOs.

Metadata: Data about specific pieces of individual data, including but not limited to: timestamps, location tags, keystrokes, networks or devices used to generate said data, or the operating system used by said device.

Misinformation: Misinformation is false information spread without deliberate intent. Individuals can become misinformed and start to spread that information thinking it is factual.

New Media: New media refers to the forms of media that are native to computers and that rely on computer technology for redistribution. This can include the internet, smartphones, and computers. It is usually interactive as opposed to traditional media.

Terrorist Information Operations: Terrorist information operations refers to the central strategic mechanism through which terrorist groups frame politico-military activities. These operations are often multi-dimensional, targeting both “friend and foe” through the same content and messages. These messages are perpetuated through both formal and informal channels.

Traditional Media: Traditional media refers to sources from where most people historically received information. This includes television (cable and satellite), print (newspapers, magazines, and periodicals), and radio.

Troll or Opinion Agent: When referring to the internet, a ‘troll’ is someone who purposely posts provocative, incorrect, or offensive content with the purpose of garnering a reaction. By eliciting reactions, trolls exert immense power over actors as they can often cause their respondents to make a mistake or reveal certain information. Trolls also use tactics such as abuse, doxxing, spamming, and/or mimicking. Doxxing is a practice by which “trolls” will publish sensitive or compromising information about a person on the internet, usually with malicious intent. In terms of mimicking, trolls will often pretend to be a different actor representing a specific brand to discredit members of specific groups.

Vehicle-to-Vehicle (V2V): V2V pertains to the sharing of data between automobiles relative to traffic warnings.

Vision

Mission: Our vision for this project is to provide recommendations to develop a cyber regime that promotes innovation, facilitates access to credible information, protects individual and state well-being, brings about government and corporate transparency and accountability, and engenders stability, trust and cooperation among people, non-state actors, the private sector, and states.

Audience: The primary audience of the report is the Government of Canada, for the purpose of creating effective and updated approaches to a rapidly developing cyberspace. The report may also be of interest to various stakeholders in cyberspace and cyber governance. This can include, but is not limited to: individuals, civil society groups, private corporations, non-profit organizations, state actors or international organizations.

Intent: This report will examine the major challenges, risks, and benefits related to cyberspace, highlighting specific cases and providing recommendations for how to address the cases. These recommendations may take the form of state level policy recommendations, best practices for corporate actors, possible protective measures taken by individuals, or international-level institutions, and agreements. Any interested party can determine which areas of cyber governance warrant their attention and concern, and may potentially act upon these recommendations in order to address these concerns.

Guiding Principles: While each segment of this report will address the implications of a single area of focus in cyber governance in depth and provide recommendations to address any challenges associated with this area, the recommendations made will all be informed by the theoretical groundings outlined in the following section of this report:

A. **International Development:** Incorporate cyber-capabilities and cryptocurrencies into the delivery method of international development, with a focus on investment in internet infrastructure.
B. **Corporate Considerations:** Regulate channels through which corporations interact with the internet to ensure these interactions are secure and direct self-interested behavior to benefit the public good.
C. **Individual Privacy Rights:** Protect the individual's right to personal privacy and control over the collection and use of their own private data, and prevent misuse of this information.
D. **5G Network:** Enhance Canada's national cybersecurity capabilities, and explore 5G alternatives that will help Canada maintain its position in the Five Eyes network and as a US ally.
E. **Information Warfare:** Mitigate the ability of non-state actors to weaponize information and utilize information warfare tactics
F. **Election Interference:** Assist corporate, state, civil, and individual actors in taking a larger role within cyberspace in order to mitigate the threat of election interference, and implement regulations to better protect the election process and prevent the spread of mis/disinformation related to elections.

Cyberspace and International Relations Theory

The purpose of this report is to understand the role of cyber-technologies in relation to the state, and non-state actors; those including individuals, corporations, non-governmental agencies, or civil society. This section of the report will provide the theoretical understanding and critique of the subject matter discussed, and the reasons for this discussion. This framing is essential for understanding and expanding this complex field which plays an imperative role in contemporary human experience and alters the very realities of state and non-state relations with cyber technologies.

The following section will explore several theoretical frameworks as they problematize and support the claims and recommendations made in each section of the report. This section will present a constructivist conception of cyber-technologies, the realist and neoliberal assumptions throughout the report, the possible reality of an anarchical cyberspace, and finally it will offer solutions informed by critical theories of constructivism, postcolonialism, feminism, and queer theory.

For constructivists, all thoughts, perceptions, and images are constructed from the reality in which states and people within them choose to perceive. Some scholars have taken this position further in arguing that the predominant international relations (IR) theories have become self-fulling prophecies for states. Constructivism is a concept that borrows equally from the rationalism of realism and liberalism, while maintaining the ability to take from the postcolonial and feminist critiques of postmodern thought.[4] The framework for constructivism is simply to understand the reasons for interpretations and distortions of reality in the relations between nations.[5] This report will also highlight the concept of trust, which constructivists have often focused on in relation to relations between states since it is constructed and deconstructed.[6] Alexander Wendt's works are crucial to constructivist theory and understanding. In particular, he offered the strongest criticism of realist realities and theories. He suggested that "anarchy is what states make of it," and once states and actors within states believe this premise they fall into a self-fulling prophecy in which all actors are self-interested.[7] As a result, Wendt concluded that "…self-interest is not sustained by practice, it will die out."[8] He meant that states can avoid the over-securitization of politics, and the realist principles of self-help and self-interest, and instead produce constructive dialogues in their place.

Applying this framework to cyberspace in relation to international relations, the state must understand that the internet can be constructed into different frameworks. From a place of entertainment to one of communication, as well as one that perpetuates insecurity as corporate entities or governments gather information on individuals. Nevertheless, the internet exists and has the potential to accomplish unspeakable harm and the greatest benefit to the world. For instance, the Christchurch mosque attacker used the internet as a way to convey his message as he spread his manifesto on social media websites and also live streamed the mass killing on Facebook. As a result, his ideas have been spread across the world fueling his rhetoric and resulting in calls for governments to regulate social media corporations to prevent the spread of these views.[9]

Upon reading the academic scholarship on the internet and international relations, it is easy to discern that the internet has been over-securitized. Scholars and individuals view it in Rumsfeldian terms as a place with more "unknown unknowns" rather than "known knowns." However, this has not prevented the perpetual application of theoretical frameworks onto the internet. International relations scholar, Joseph Nye, perpetuates this securitization in his “Regime Complex for Managing Global Cyber Activities.” He states that “Governments and non-state actors cooperate and compete for power in this complex arena. Cyberpower can be defined in terms of set resources that relate to the creation, control and communication of electronic and computer-based information.”[10] This reflects the realist perspective of international relations, in which the world and relations between states is defined by power and the self-interest of the actors involved. There are other critical reflections within the scholarship that seek to provide an understanding of the role of non-state actors who utilize the internet to their advantage. These concepts have led to studies, such as “The Arab Digital Vanguard: How a Decade of Blogging Contributed to a Year of Revolution,” where Jillian York provides the analysis and role of the internet in providing the reasons that fueled the Arab Spring.[11]

Taking this critique into account and examining the recommendations and written works produced, predominant and perpetual interpretations and narratives are apparent in these works. Firstly, the entire report carries a liberal orientation as it seeks to understand the implications of the cyber technologies on the state, as well as the individual, and even corporations. Secondly, examining individual reports, realist narratives are predominantly offered instead of constructive dialogue. For example, the 5G Report provides a relevant critique and information on the risks for the Canadian government in relation to adopting Huawei technologies. However, it is also anti-Chinese and seeks to rationalize China as an untrustworthy actor, whereas the United States is seen as a trustworthy state. The language is similar to that of the twentieth-century, in which Japan and China were viewed as threats to the Western world, and it was known as the “Yellow Peril.” Upon reading the recommendations offered, we see the inherent obsession with critiquing China’s immoral or unjust actions, however, the scholarship does not seem to place such emphasis on the acts of other Western nations. Constructivism seeks to understand the reasons behind this by asking questions: Why do we fall into realist traps of securitization with the internet? Why is liberalism the inherent ideology and perception of this study?

There is a core set of assumptions that govern the philosophy of realist thinkers dating back from Thucydides to the modern age. These scholars can agree that first, the state is the dominant actor, second, the dominant actor acts rationally to fulfill the national interest, and third, power and security are the core values of the state.[12] More modern figures of realist thought, Hans J. Morgenthau and Kenneth Waltz, have made attempts to find a deeper coherence beyond these three assumptions. Specifically, the inherent self-interest of human nature, in which “laws of politics have their roots” is seen as consistent throughout all of human history.[13] In addition, Waltz asserts that realists view anarchy as the general condition of international relations, which acts as the catalyst for the problems states must deal with.[14] The ‘condition’ of anarchy is central to what realists refer to as the security dilemma, where the self-interested pursuit of power is rewarded with greater security and success compelling other states to do the same.[15]

Realist scholars find no reason to amend these core beliefs to conform to the digital age.[16] The state remains as the dominant actor, and the pre-eminence of security and power defined in terms of military capacity is maintained, which prevents non-state actors from accumulating any capacity to exercise power. It is not to say that cyberspace is seen as insignificant, but is instead viewed as part of the continuity of evolving military and strategic planning such as with the introduction of psychological and electronic warfare.[17] Ultimately, the impact of the digital age is uncontroversial among realist thinkers. It will undeniably affect domestic policy and the structure of states, but it will have little ramification on the primacy of the state in international affairs.

Constructivists critique this realist framework for its use of ‘perpetualism’ within its international relations theory.[18] By prioritizing the state and not attempting to look beyond it, realism cannot properly address the power of cyber technologies. Instead, it will always be viewed as a new tool to aid the state in its pursuit of its national interests. Wendt described realism as rational forces, which seek to understand behaviour, and consequently offers a change to behaviour, but not identities and interests.[19] As such, realism is unable to properly grapple with the benefits and harms provided by cyber technologies, since it is either one or the other for those theorists. Following a realist framework results in two reinforcing and perpetual realities. The first of which is that the internet will remain securitized and a place for exploitation. As such, the second is the state and non-state actors will exploit and securitize the internet. Ultimately, realism neglects the reality that cyber technologies are beneficial in ways that are highlighted by other critical theories.

Liberalism is one of the two most influential approaches to international relations in the modern day. In contrast to realism, the core tenets of liberalism can be summarized as: (1) the emphasis on a plurality of international actors; (2) the importance of domestic political factors in determining the international behavior of states; (3) the role of international institutions in establishing (although not enforcing) rules of behavior (or regimes) for state actors; and (4) expanding the agenda of international studies.[20] New non-state international actors (transnational corporations, social movements, pressure groups, political party networks, migrants, and terrorists), they argue, can play key roles in world politics.[21] Overall, liberalism tends to emphasize the positive outcomes of interdependence and interconnectedness at the international level.

With regards to cyber politics and national security, liberal theorists have tended to focus their attention on the positive rather than the negative aspects of actor plurality in the digital age. Modernization, and subsequently technological development, is generally seen as peaceful change amongst liberals and they have supported their stances by promoting notions such as collective and cooperative security to respond to the emergence of cyber threats. In alignment with the core tenets of liberalism, influential scholar Joseph Nye has analyzed the impact of the information revolution on international relations and argues that soft power is becoming increasingly important in the digital age, as multiple channels of global communication are evolving which easily transcend sovereign boundaries.[22] In the following report, liberal theory is used in Corporate Considerations to emphasize the important role corporations play in cyber politics, and it is further argued that right incentives for business are important to encourage them to take on this role. Alternatively, in Information Warfare, seldom is liberal theory referenced except in the recommendation section which then calls for international commitments and agreements to achieve various aims. Ultimately, liberal theory contributes to scholarship on cyber politics in the digital age by taking a critical stance against addressing issues labelled as threats to state “security”, by emphasizing the plurality of world actors in cyberpolitics, and by advocating for a “soft power” approach to facilitate cooperation, democratization, and peace.[23]

In considering the realities of cyber technologies and the space which exists online, a key question arises: what if the cyber sphere remains unregulated, and ungoverned? Cyber-anarchism (or more commonly known as Crypto-anarchism) first coined by Timothy May, is a theory which advocates for a selfgoverned cyberspace and rejects a government controlled centralized monopoly over the internet.[24] In crypto-anarchism, there is no set of policies established and there is no single leader; it is those who choose to participate in the cyber domain who dictate their own restrictions and policies.[25]

Crypto-anarchists often implement encrypted software which protects them from domestic and international laws, in order to evade censorship. The goal of the participants is to encourage privacy and increase freedom of speech/cyber action outside the purviews of the traditional political sphere.[26] The software allows crypto-anarchists to privately send and receive information that otherwise would be detected by governments or intelligence agencies. Given the anonymity of the participants, many establish online reputations in which they hold a significant amount of control and power within cyberspace that can disrupt prior implemented laws pertaining to technology. Despite law enforcement's lack of knowledge in the field, these agencies continue to struggle to maintain control and enforce the law, but with difficulty.[27] However, given that anarchy presents a challenge to good governance, one of the clear aims of this report, cyber anarchy is considered in the recommendations of this report.

Similar to the constructivist view, there are various other critical views which seek to better address cyber technologies as well as the gaps left by realist and neoliberal theories which are core theories present throughout this report. Critical perspectives of IR seek to challenge what appears to be familiar and natural.[28] Postcolonialism, for example, is a non-mainstream theory which focuses on the intersections of class, race, and gender in a hierarchical world order. Postcolonialism problematizes critical IR theory by seriously considering these factors on the order of states, and not naturalizing them as critical IR does.[29] As Choudhry and Nair highlight, postcolonial thought maintains that in a postcolonial world, "national identities are constructed in opposition to European ones, and come to be understood as Europe's 'others'," thus arguing that there is a continuous systematic racialized bias in critical IR theory.[30]

This theory is particularly reflected in the section on development. As will be proven later, there is a lack of infrastructure when it comes to the innovation of development aid in the forms of untied cash aid and the use of cryptocurrencies in delivering aid. This report will highlight the United Nations Sustainable Development Goals and apply cyber innovations to proposed solutions to aid in the completion of these goals. The idea of the expansion of cyber technologies to help more people gain access to the internet is applied to these solutions, and the inherent benefits of access to the internet are shown in relation to achieving these goals.

Postcolonial thought can perhaps best be seen in the development section when trying to expand upon Mao Zedong's "Three World Concept." The very language that it used mirrors critical IR theory, but perpetuates the postcolonial imperialist language of the "West versus the rest." The language of the three worlds lends itself easily to the discussion of development, but contains an inherent racialized and gendered bias that must be acknowledged. This can also be extended to the types of humanitarian and developmental aid that are currently supplied. Most aid has been in-kind aid, whereas it is suggested that untied cash aid as non-profits such as GiveDirectly are implementing can be synthesized with cryptocurrency to ensure the safe transfer and quick delivery of cash aid.

Additionally, feminist critiques also succeed in addressing certain issues in realist and liberal assumptions present in this report. Feminist theory seeks to study the ways in which systems of power aim to marginalize certain groups of individuals and aims to highlight that these different systems of power do not exist in isolation of one another.[31] Within the discipline of IR, the intersectional feminist critique argues that it is necessary to broaden what is considered to be the main units of analysis, such as state actors and state relations. Given the expansion of cyber technologies, and cyber communication in particular, feminist anthropologist Sophie Bjork-James writes that there is a "… significant expansion of social life along with a proliferation of new identities and communities," all of which must be a consideration.[32] Within the context of cyber technologies, a feminist critique argues for the decentralization of states, as this form of analysis fails to take into view the myriad of other dynamics online. It seeks to include the embodied experiences of women, racialized individuals, sexual minorities, and all those of varying intersectional identities as a site of knowledge and ways in which cyber-technologies are experiences.[33] Realism tends to assign 'ideal' male characteristics to the 'ideal' state: feminist IR expert Jill Steans states that, "…to be a 'man,' one had to be self- reliant, autonomous, [and] avoid dependence on others."[34] The only way to understand normative theories like realism, and liberalism, is by looking not only at their ideal and abstract universalizing claims, but to also consider their non-ideal implementation in reality.[35] Liberalism, for example, is hailed as a theory that seeks justice and freedom for all, however, only a select few white men in particular are able to fully access this freedom.

Within dominant cyber rhetoric, the internet is hailed as an equalizer, or as Christine Ann Nguyen-Fredrick terms it, a social utopia. However, as Nguyen-Fredrick asserts, "research has shown that [computer-mediated communication] (CMC) has many of the same power issues found in other communities and other forms of communication. Many studies have shown that CMC is not democratic, particularly in the area of gender. For example, women and other minorities generally have less access to computers, and therefore less access to CMC."[36] Evidence for this claim is present throughout this report, in case studies such as Access to the Internet, or Anti-Intellectualism. More broadly, considerations of the individual experience, with issues such as privacy of marginalized individuals at the forefront, these dynamics are of consideration in this research.

A dynamic untouched by any of the aforementioned theories is the queer experience with cyber technologies. However, as asserted by Queer theorists such as Chris Ashford or Simona Rodat, the identities and experiences of LGBTQ2+ communities are shaped online through CMC. Ashford writes that, "Sexual minority groups, and/or those groups deemed sexually deviant, limited by the constraints of space, are able to interact through virtual media."[37] This dynamic is specifically referred to in the Individual Privacy portion of this report.

Given the realist and liberal foundations of this report, constructivist, postcolonial, feminist and queer analyses are present; however, they are lacking throughout the research presented. This is the result of both the presented report and the literature that was consulted to create the report, as the literature predominantly reflects liberal and realist theories. These critical analyses are an important consideration to the recommendations of this report and are essential to keep in mind while learning more about the expansive possibilities of cyber technologies. There is inherent value in the use of a variety of theoretical perspectives when discussing cyber-technologies. The complexity presented by challenges online cannot be thoroughly tackled using one theoretical view. As such, this report is directed at the Canadian government which is best interpreted through liberal and realist lenses. These theories are also best representative of the current international system. Therefore, in attempting to speak to the Canadian government, international actors, and corporations, it was essential for the natural progression of the report to have realist and liberal foundations. Nevertheless, it was important to deconstruct this perpetual framework through the use of constructivist, post-colonial, feminist, and queer theories so as to highlight the inherent flaw of solely using similar theoretical lenses.

[1] Karen Gilchrist, “Australia's Prime Minister Calls for Global Social Media Restrictions After Christchurch Shootings” *CNBC,* March 18, 2019, https://www.cnbc.com/2019/03/19/australias-pm-restrict-social-media-after-christchurch-mosque-attack.html

[2] Karen Gilchrist, “Australia's Prime Minister Calls for Global Social Media Restrictions After Christchurch Shootings” *CNBC,* March 18, 2019, https://www.cnbc.com/2019/03/19/australias-pm-restrict-social-media-after-christchurch-mosque-attack.html

[3] Gang Li, Wenji Niu, Li Guo, Lynn Batten, Yinlong Liu, and Guoyong Cai, “Editorial: Securing Cyberspace,” *Concurrency and Computation: Practice and Experience* 28 (2016): 1870-1871. DOI: 10.1002/cpe.3753.

[4] Johan Eriksson and Giampiero Giacomello, “The Information Revolution, Security, and International Relations: (IR)relevant Theory?,” *International Political Science Review* 27, no. 3 (2006): 232-233.

[5] Johan Eriksson and Giampiero Giacomello, “The Information Revolution, Security, and International Relations: (IR)relevant Theory?,” *International Political Science Review* 27, no. 3 (2006): 233; Hiski Haukkala, Carina van de Wetering, and Johanna Vuorelma eds., *Trust in International Relations: Rationalist, Constructivist, and Psychological Approaches* (New York: Routledge, 2018), 3.

[6] Asli Ilgit and Binnur Ozkececi-Taner, “Identity and Decision Making: Toward a Collaborative Approach to State Action,” *Psychology and Constructivism in International Relations: An Ideational Alliance*, ed. by Vaughn P. Shannon and Paul A. Kowert (Ann Arbor: The University of Michigan Press, 2012), 92; Hiski Haukkala, Carina van de Wetering, and Johanna Vuorelma eds., *Trust in International Relations: Rationalist, Constructivist, and Psychological Approaches* (New York: Routledge, 2018), 1.

[7] Stefano Guzzini, and Anna Leander eds., *Constructivism and International Relations: Alexander Wendt and His Critics* (London and New York: Routledge, 2006), 5-8.

[8] Stefano Guzzini, and Anna Leander eds., *Constructivism and International Relations: Alexander Wendt and His Critics* (London and New York: Routledge, 2006), 7.

[9] David D. Kirkpatrick, “Massacre Suspect Traveled the World but Lived on the Internet,” *New York Times*, March 15, 2019, https://nyti.ms/2FbCtGS.

[10] Joseph S. Nye Jr., “The Regime Complex for Managing Global Cyber Activities,” in *Centre for Internet Governance Innovation*, May 2014, https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf, 5.

[11] Jillian York, “The Arab Digital Vanguard: How a Decade of Blogging Contributed to a Year of Revolution,” *Georgetown Journal of International Affairs* 13, no. 1 (2012): 33-42.

[12] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?," International Political Science Review 27, no. 3 (2006): 228, doi:10.1177/0192512106064462.

[13] Hans J. Morgenthau, Politics Among Nations: The Struggle for Power and Peace (New York: Alfred A. Knopf, 1954), 4.; Jack Donnelly, Realism and International Relations (Cambridge: Cambridge University Press, 2000), 57.

[14] Kenneth N. Waltz, Realism and International Politics (New York: Routledge, 2008), 79-80.

[15] Jack Donnelly, Realism and International Relations (Cambridge: Cambridge University Press, 2000), 49.

[16] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?," International Political Science Review 27, no. 3 (2006): 229, doi:10.1177/0192512106064462.

[17] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?," International Political Science Review 27, no. 3 (2006): 229, doi:10.1177/0192512106064462.

[18] Stefano Guzzini, and Anna Leander eds., *Constructivism and International Relations: Alexander Wendt and His Critics* (London and New York: Routledge, 2006), 2.

[19] Alexander Wendt, “Anarchy is What States Make of It: The Social Construction of Power Politics,” *International Organization* 46, no. 2 (1992): 391-392, https://www.jstor.org/stable/2706858.

[20] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?," International Political Science Review 27, no. 3 (2006): 229, doi:10.1177/0192512106064462.

[21] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?," International Political Science Review 27, no. 3 (2006): 230, doi:10.1177/0192512106064462.

[22] Joseph S. Nye, JR, *Power in the Global Information Age: From Realism to Globalization*. London: Routledge: Ch. 7.

[23] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?," International Political Science Review 27, no. 3 (2006): 231, doi:10.1177/0192512106064462.

[24] Timothy May, “The Crypto Anarchist Manifesto," In *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*, 1992, 2.

[25] Timothy May, “The Crypto Anarchist Manifesto," In *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*, 1992, 2.

[26] Peter Ludlow, *Crypto Anarchy, Cyberstates, and Pirate Utopias* (MIT Press, 2001), 5.

[27] Peter Ludlow, *Crypto Anarchy, Cyberstates, and Pirate Utopias* (MIT Press, 2001), 6.

[28] Sandra Harding as referenced in: Ann Tickner, "You Just Don't Understand: Troubled Engagements Between Feminists and IR Theorists," *International Studies Quarterly* 41, no. 4 (1997): 623.

[29] Geeta Chowdhry, and Sheila Nair, *Power, Postcolonialism and International Relations: Reading Race, Gender and Class* (Routledge, 2013), 2.

[30] Geeta Chowdhry, and Sheila Nair, *Power, Postcolonialism and International Relations: Reading Race, Gender and Class* (Routledge, 2013), 2.

[31] Sandra Harding as referenced in: Ann Tickner, "You Just Don't Understand: Troubled Engagements Between Feminists and IR Theorists," *International Studies Quarterly* 41, no. 4 (1997), 622.

[32] Sophie Bjork-James, "Feminist Ethnography in Cyberspace: Imagining Families in the Cloud," *Sex Roles* 73, (2015), 113.

[33] Sandra Harding as referenced in: Ann Tickner, "You Just Don't Understand: Troubled Engagements Between Feminists and IR Theorists," *International Studies Quarterly* 41, no. 4 (1997), 622.

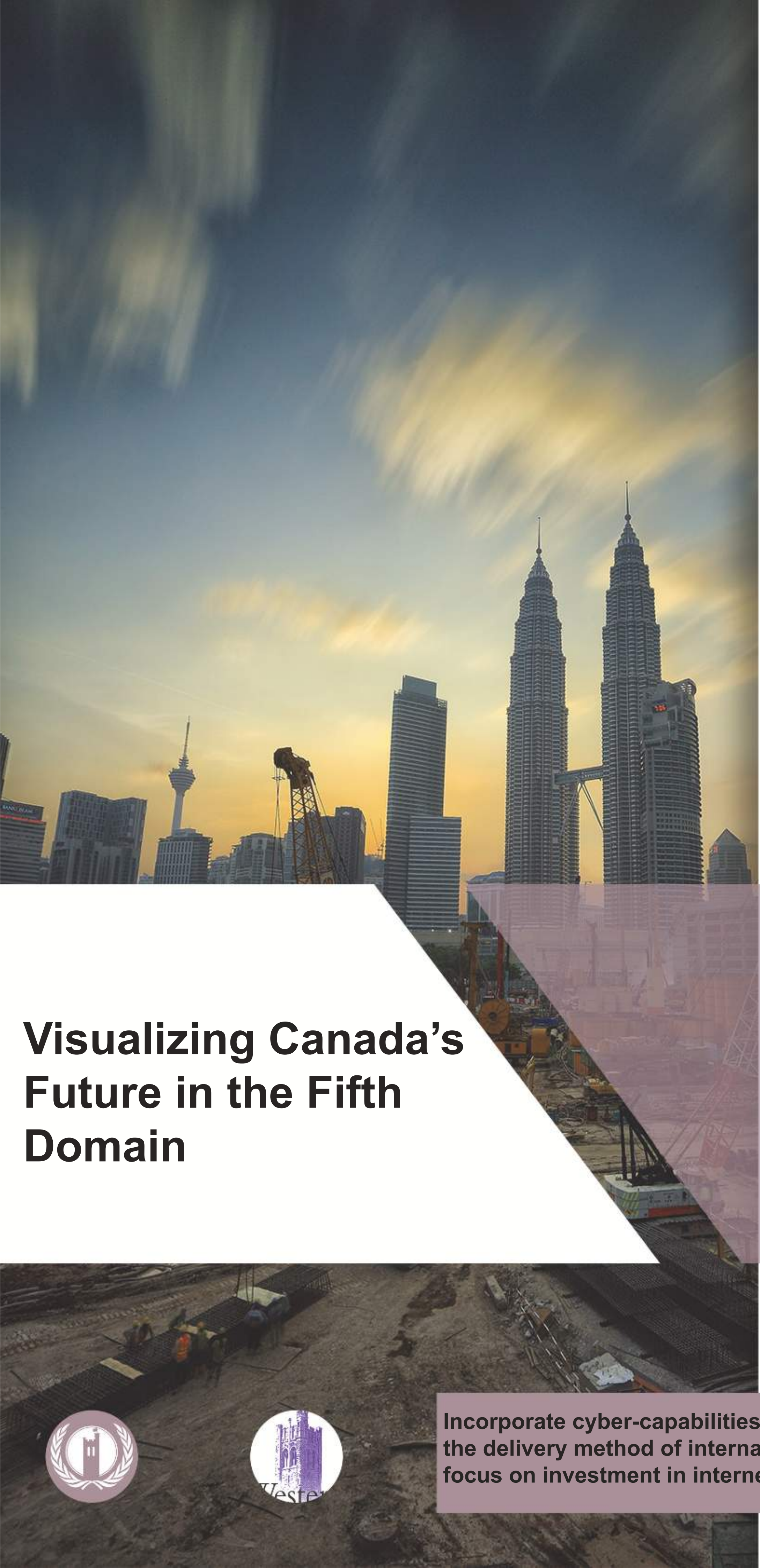
[33] Sophie Bjork-James, "Feminist Ethnography in Cyberspace: Imagining Families in the Cloud," *Sex Roles* 73, (2015), 113.

[34] Jill Steans, *Gender and International Relations: Issues, Debates and Future Directions*, (2009), 47.

[35] Charles Mills, "Racial Liberalism," *Black Rights/White Wrongs,* (2017), 1381.

[36] Christine Ann Nguyen-Fredrick, "Feminist Rhetoric in Cyberspace: The Ethos of Feminist Usenet Newsgroups," The Information Society, 15, no. 3, (1999), 187.

[37] Chris Ashford, "Queer theory, cyber-ethnographies and researching online sex environments," *Information & Communications Technology Law* 18, no. 3 (2009), 299.



International Development

Visualizing Canada's Future in the Fifth Domain

Incorporate cyber-capabilities and cryptocurrencies into the delivery method of international development, with a focus on investment in internet infrastructure.

International Development

Cryptocurrency & Internet Access

Background

International development has been an evolving field that links key areas in the realm of IR including politics, economics, security, and social climates. The primary goal of international development is for developed nations to work in tandem with non-state actors and other developed nations to develop strategies to aid in the advancement of underdeveloped and developing countries. This section will begin by analyzing the history and background of International Development including the role of Global Affairs Canada (GAC), as well as international organizations, such as the International Monetary Fund (IMF), and the World Bank. Moreover, it will provide background information on cash transfers as a form of foreign aid. This section will also focus on the evolution of international development focusing on challenges and successes relating to development through the use of cryptocurrency and internet access.

Canada continues to be an influential global actor in areas of international development and foreign aid.[38] Internationally, the Canadian government through GAC is currently placing a strong focus on a gender equality initiative, specifically its recent enactment of Canada's Feminist International Assistance Policy.[39] The goal of Canada's Feminist International Assistance Policy is to demonstrate that "Canada firmly believes [in the promotion of] gender equality and empowering women and girls in the most effective approach to achieving this goal."[40] In particular, Canada is seeking to provide more inclusive international assistance by "invest[ing] in innovation and research, deliver[ing] better reporting on results, [and] develop[ing] more effective partnerships," in order to aid women and girls. [41]

Moreover, there are international institutions that play a key role in international development, principal among them are the World Bank and the IMF. The World Bank is a development institution that provides fiscal and technical assistance to the governments of developing nations. Such assistance is often co-financed with other international development institutions, commercial banks, credit institutions, and private sector investors.[42] Financial aid takes the form of low-interest loans and grants.[43] The World Bank allocates funding and technical assistance to projects in support of public health, education, infrastructure, private sector stimulation, and agricultural/environmental initiatives.[44] The World Bank has two primary development goals that they seek to reach by 2030. First, to decrease the number of people living on less than a $1.90/day to 3% or lower and second, promoting the growth of income for the bottom 40% earners in every nation.[45] The 2030 Agenda of the World Bank ties in with completing the Sustainable Development Goals, as explained below.

The International Monetary Fund is dedicated to international development worldwide, supporting various global development projects that focus on an array of social issues such as, poverty, inequality, education, sustainable development, and post-conflict reconstruction.[46] An example of this is seen in their support for the United Nations Sustainable Development Goals (SDGs), in which they have funded and facilitated several projects that focus on specific SDGs. The 'Infrastructure Policy Support Initiative' is an example in which the IMF advocates for more public investment into resilient and inclusive infrastructure projects (SDG 9).[47] This initiative deepens the IMF's macroeconomic policy and its capacity building efforts by supporting infrastructure projects, without pushing states towards financial collapse. In general, the IMF's new debt limits policy provides room for countries to grow and invest, without putting a strain on the state economies or domestic policies. The IMF has also worked to reform its debt sustainability framework, providing pertinent information and guiding low-income developing nations, when borrowing money or paying off public debt responsibly.[48] The IMF has publicly committed to supporting the UN's SDGs, helping initiate global development projects and make them financially feasible.

Cryptocurrencies and International Development

Information and communication technologies (ICTs) have been utilized globally as a method for mitigating poverty and fast-tracking development. In Chile, they have been formally integrated in the nation's development strategy.[49] Chile currently plans to reach economic development levels of Southern European countries by utilising high-impact initiatives, such as online tax payments, issuance of Civil Registry Certificates and the launching of an online public procurement system called ChileCompra have been implemented thus far.[50] However, there are various institutional barriers for nations like Chile. Barriers such as political and banking institutions can be overcome via cryptocurrencies which represent the perfect merger of financial and technological innovation. Saifedean Ammous argues that Bitcoin offers a 'blueprint' to people living in countries lacking 'supportive modern institutions,' allowing them to partake in worldwide contemporary capitalism.[51] This blueprint is a viable solution or alternative to traditional state or commercial banking institutions, fiscal services such as currency issuance and credit provision, as well as issues relating to judicial practice.[52]

Cryptocurrencies are encrypted and stored in a decentralized fashion. This technology enables digital financial transactions without an intermediary.[53] This is crucial for international development as it is often the case that developing nations bear the highest costs for financial services and the institutions delivering such services are corrupt and lack accountability.[54] Eliminating the role of such intermediary institutions allows those involved in the transaction to pay less for it to occur and avoid corrupt influence.

The limited availability of Bitcoin may be perceived as a weakness of that cryptocurrency, but Ammous argues that this is actually an asset.[55] Blockchain is a technology that would require a certain amount of capacity building on the part of nations receiving aid to address the risks of institutional exploitation.[56] The state must decide that if the 'mass adoption' of bitcoin does not occur, having a monetary alternative not subject to forces such as inflation or tied to any physical currencies is essential and would present a real challenge to state-issued physical currency.[57] For example, the Chinese government has banned digital currencies due to the risks associated with their use, however, it has considered future adoption.[58]

The use of cryptocurrencies does come with some risks, but Jan Lansky argues that the benefits outweigh the risks. He asserts that the onus is on the individual nation to understand the perils associated with cryptocurrencies and to mitigate them by educating the users of cryptocurrencies while also utilizing Anti-Money Laundering (AML) and Know Your Customer policies.[59] Perhaps the greatest risks with cryptocurrencies in developing nations are transactions that cannot be altered or reversed once completed, as well as the fact that state authorities cannot withdraw funds from a crypto account.[60] In the event of a theft or seizure of "illegally gained funds," democratic countries require the consent of the criminal to return what was taken.[61]

Cryptocurrencies also present an interesting opportunity in regards to the distribution of development aid. Humanitarian and developmental organizations are playing a key role in combining efforts from governments and the private sector, incorporating Blockchain technology to increase the efficiency, accountability, and transparency of delivering humanitarian aid.[62] Sudzina argues that while there are advantages and disadvantages to using cryptocurrencies as a vessel to distribute international development aid, the idea must be considered and not immediately dismissed.[63] Such considerations include the amount of energy cryptocurrencies utilize and the sustainability implications associated which include logistical factors such a transaction fees/timing and ledger transparency, as well as the general acceptance of cryptocurrencies in commercial establishments.[64]

The Use of Technology and Cyberspace in the Facilitation of International Development

International Development and cyberspace are growing increasingly linked as cyberspace becomes more essential for successful integration in the global economy. In particular, Canada's Feminist International Assistance Policy is oriented toward technological development as evidenced by the programs funded by the government through the International Development Research Centre (IDRC).[65] The IDRC argues that through the focus on technology and development, we can begin to tackle the key actions of Canada's Feminist International Assistance Policy as well as UN Sustainable Development Goal #5, "Gender Equality: Achieving gender equality and empowering all women and girls."[66]

One of the programs currently being supported by the IDRC is *Prospera* Digital. *Prospera* (previously known as *Progressa* or *Oportunidades)* is an anti-poverty conditional cash-transfer program that began in rural Mexico. It is the biggest social program in Mexico and the second largest cash transfer program in the world.[67] In Mexico, an estimated 50% of the population is affected by poverty. Moreover, "up to half of the economically active population depends upon the informal sector for its income, and has access to few benefits."[68] This program was established in 1997 in order to deal with the poverty epidemic in the nation and has inspired similar initiatives across Latin America. The main focus of the program is to improve human development by focusing on children's education, nutrition, and health.[69] It takes form in bi-monthly cash transfers, made up mostly of scholarships for children's schooling as well as additional cash to improve nutrition. *Prospera* Digital is an initiative that is aimed to "improve, through digital technologies, the way beneficiaries receive, access, and use conditional cash transfers and financial services… [and] foster a system of electronic transactions, facilitating access to financial services through digital banking solutions, and promoting financial education among women."[70] This initiative, which began in 2016, will ease access to the cash transfers by the families receiving it and is set to cut costs of transfer for the Mexican government. Overall, it seems to be a cheaper and more effective way of transferring essential cash to those who need it.

Meanwhile, technology has made cash transfers more effective as a humanitarian tool. Less money can be spent to help individuals in need, reducing costs and increasing accountability mechanisms to track the flow of cash.

NGOs such as Free the Children and GiveDirectly have capitalized on the ease through which the internet has made cash transfers easy, reliable, and safe. Cyber-technologies have allowed NGOs to reach hostile areas, delivering aid effectively and quickly. Further research has shown that cash transfers reduce tension between host communities and cash-aid recipients by stimulating local markets.[71]

GiveDirectly (GD) is an NGO that is committed to ending severe poverty by providing un-tied cash transfers to people in need and works to convince governments and organizations to use more un-tied cash aid. Following a study by Amartya Sen, GD highlights the pitfalls of in-kind aid and the potential dangers of flooding local markets with food aid and goods. A comparative study in Ethiopia found that cash-aid was 25-30% more effective and cheaper. Another study done in Somalia showed that when cash aid was used, more than double the aid budget went directly toward recipients.[72] Cash aid has not only proven to be an effective humanitarian tool, but it also helps quell tension between local communities and displaced people by stimulating the local market economies. However, less than 6% of all humanitarian aid is used as cash aid.[73]

GD capitalizes on the ease through which the internet and cellphones have simplified money transfers. Cash aid sent through secured money transfer systems ensures accountability and transparency. Corruption and fraud are significantly reduced because money can be easily tracked.[74] Moreover, cash aid to remote or hostile environments where organizations cannot operate is made possible.[75] However, cash aid does have its limitations. Inflation, weak markets and unsupportive governments are all variables that hinder cash aid from being effective.[76] GD is revolutionizing humanitarian work by gathering valuable research data on the successes and failures of its operations. This data can be shared with other organizations to make improvements or comparisons to different regions or states.[77]

Challenges

There are significant challenges regarding the use of cryptocurrencies. First, digital currencies are not viewed equally from country to country, depending largely on their stage of economic and social development as defined by Mao Zedong's "Three World Concept." The First World nations tend to be more accepting of cryptocurrency technology, while their Second World counterparts are more hesitant to widely accept or are blatantly against cryptocurrency technology. Members of the Third World hold mixed opinions as some accept it and some do not. The reasons for Third World countries' hesitation range from fears of black market usage for digital currencies or taxation scams. Employing stricter policies regarding middle-man interactions as well as AML can stifle these concerns. Second, cryptocurrencies require an incredible amount of energy to be sustained. If cryptocurrencies are to be used in the context of international development aid, ways to sustainably host, use, and mine such currencies must be investigated and invested in to avoid wasteful practices.

The most significant challenge with internet infrastructure in developing and underdeveloped countries is the stark socioeconomic divide. As such, it is important that when money is invested in improving access to internet in developing and underdeveloped countries that this divide is bridged instead of widened.

When determining what recommendations are appropriate, one must consider not just the challenges associated with cyber-technology, but the goals of international development in relation to

United Nations' mandates. In particular, the SDGs are a set of 17 goals that every member-state of the United Nations agreed to in 2015.[78] While all are important, the most relevant ones for the purposes of this report are: (1) No Poverty; (2) Zero Hunger; (3) Good Health and Well-Being; (4) Quality Education; (8) Decent Work and Economic Growth; (9) Industry, Innovation and Infrastructure; (10) Reduced Inequalities; (12) Responsible Consumption and Production, and (16) Peace, Justice and Strong Institutions.[79]

Recommendations

1.1. Research Methods to Reduce the Environmental Impacts of Cryptocurrencies

Actors: UN, IMF, World Bank, GAC, non-state actors
Type of Recommendation: Regulatory
Main Cyber Issues Involved: Environmental impact posed by the mining of crypto-currencies, pace of technological change
Main IR Issues Involved: Multilateralism, development, and cooperation

Explanation: International development institutions such as, the IMF, World Bank, and IDB must work to mitigate the environmental impact of cryptocurrencies by conducting research and development in the form of knowledge products. Non-state actors such as independent researchers, scientists, and experts in digital currencies would be able to provide beneficial contributions to this.

Challenges: The use of cryptocurrencies requires a lot of energy, so much so that the use of them in their present form would result in a negative impact on the environment if adopted to the extent necessary to be effective. Numerous actors have looked at the benefits of using cryptocurrencies as a substitute for certain types of humanitarian aid, but little research has been done on best practices to mine and distribute cryptocurrencies sustainably. In addition, few, if any, policies or frameworks exist that incentivize these actors to switch to using cryptocurrencies as a form of humanitarian aid. Lastly, the recent development of cryptocurrency technology has been met with hesitation by several countries, who do not acknowledge cryptocurrencies as being legitimate forms of currency. In order to successfully serve as a form of humanitarian aid, states and institutions must be willing to adopt practices that incorporate cryptocurrencies and recognize its monetary value.

Justification: If cryptocurrencies are used as development aid, this would result in aid being distributed easier and faster, furthering SDGs (8), (9), and (10). It would also help reshape how developmental aid has been given historically, which in turn harnesses the power of the internet and our reliance on smartphone technology. Moreover, if this is not done sustainably, progress on SDG (12) as well as SGD (11) Sustainable Cities and Communities would be at risk. Thus, the development of sustainable methods through which cryptocurrencies can be used would improve aid without imposing greater costs on the environment.

1.2. Reducing Neglectful Practices in Distribution of Aid

Actors: Government of Canada, other state actors, NGOs, international development institutions such as IDB, IMF, World Bank, etc.
Type of Recommendation: Legal/Legislative, Regulatory
Main Cyber Issues Involved: Dark web, Trust/mistrust, Governance, Fraud, Corruption
Main IR Issues Involved: Reach of International Law, Governance, Cooperation, Compliance

Explanation: By using existing frameworks already in use by NGOs utilizing cash-aid, national governments and NGOs intending to implement cryptocurrencies in the aid process must develop strict policies regarding taxation and AML in order to mitigate the risk of crimes related to the use of cryptocurrencies. Canada should lobby the UN and its member states to reduce the use of tied aid and in-kind aid.

Challenges: A large portion of humanitarian aid has been in-kind aid (food aid, medical supplies, etc). This poses a significant challenge because a major shift towards the use of cryptocurrencies as a humanitarian tool requires time, resources, and support from the international community to back these efforts. Frameworks and policies regarding the distribution of developmental aid must be reconfigured if there is to be to be a global shift towards incorporating cryptocurrencies as humanitarian aid. These changes require a global consensus, in which all states recognize cryptocurrencies as a legitimate form of currency. Currently, several countries such as China, Russia, Columbia and Bolivia do not recognize Bitcoin, which poses a problem for the use of cryptocurrencies as a humanitarian tool.

Justification: Actors considering the use of digital currencies for international development purposes must develop strict policies regarding taxation and AML in order to mitigate the risk of crimes related to the use of cryptocurrencies. Furthermore, actors must also look to existing frameworks set up by NGOs and states already distributing cash aid, in order to further strengthen cyber capabilities that will distribute cryptocurrencies as humanitarian aid efficiently, safely, and transparently. These efforts will work towards achieving SDGs (8), (9), and (16).

1.3. Increase Investment Towards Access to Internet Through Foreign Aid

Actors: Canada (GAC), developed nations, international development institutions, and UN
Type of Recommendation: Normative
Main Cyber Issues Involved: Lack of uniform cyber-related infrastructure and access throughout the world, development, governance, social dependence, social division, access, network
Main IR Issues Involved: Multilateralism, governance, regionalism, development, human rights, cooperation

Explanation: Canada, alongside developed nations and international development institutions must research and invest more in expanding internet infrastructure for the developing and underdeveloped world in a safe and sustainable manner. This recommendation is aimed at Canada specifically, as it is relevant to Canada's Feminist International Assistance Policy in relation to international development. The policy looks to invest more in women and girls, creating equitable policies that empower all genders on a global scale with the support of the Canadian government.

Challenges: The main issue is changing perceptions of the cybersphere, increased access to the internet and its relevance to humanitarian aid and development. The idea of getting more people connected to the internet merely sounds like adding more Facebook accounts to the networking giant's repertoire, however, in reality, there is more to this than instant connectivity. Access to cyber-technologies, including and beyond the scope of the internet, can help increase access to education, health care, and promote local businesses; because the perception of developmental aid has been historically associated with medical or food aid, hence, the benefits of access to the internet are less tangible and harder to measure. Thus, less funding and awareness are allocated to efforts increasing the accessibility of the internet globally for developmental purposes.

Justification: The support of the SDGs by the Canadian government, specifically SDG (9), harnesses Canada's Feminist International Assistance Policy by increasing access to the internet which will help women. Greater access to the internet has proven to help people in the developing world, giving them greater opportunity to access resources regarding education, health care and humanitarian aid. Greater access to the internet would help existing NGOs' already streamlining developmental aid like un-tied cash grants to people in the developing world. In doing so, increased investment in more resilient and sustainable internet infrastructure would help create more transparent and quicker money transfer systems, giving recipients the dignity and autonomy to use the un-tied cash grants for their individual needs. Recent research done by the UN and NGOs distributing un-tied cash grants have seen a reduction of tension between host communities and refugees receiving un-tied cash grants, as they stimulate local economies, increase health and well-being, reduce poverty and hunger and increase access to education - SDGs (1), (2), (3), (4), (8), (9), (10) and (16).

[38] Canada, Global Affairs Canada, *Priorities of Global Affairs Canada.* https://www.international.gc.ca/gac-amc/priorities-priorites.aspx?lang=eng

[39] Canada, Global Affairs of Canada. Our Priorities in International Assistance*, Canada's Feminist International Assistance Policy*, (Ottawa, CA: Our Priorities in International Assistance, 2017) https://international.gc.ca/world-monde/assets/pdfs/iap2-eng.pdf.

[40] Canada, Global Affairs of Canada. Our Priorities in International Assistance*, Canada's Feminist International Assistance Policy*, (Ottawa, CA: Our Priorities in International Assistance, 2017), 8, https://international.gc.ca/world-monde/assets/pdfs/iap2-eng.pdf.

[41] Canada, Global Affairs of Canada. Our Priorities in International Assistance*, Canada's Feminist International Assistance Policy*, (Ottawa, CA: Our Priorities in International Assistance, 2017), 65, https://international.gc.ca/world-monde/assets/pdfs/iap2-eng.pdf.

[42] *About the World Bank*. March 13, 2019, http://www.worldbank.org/en/about.

[43] *About the World Bank*. March 13, 2019, http://www.worldbank.org/en/about.

[44] *About the World Bank*. March 13, 2019, http://www.worldbank.org/en/about.

[45] Mike Kelleher, "Sustainable Development Goals (SDGs) and the 2030 Agenda," In *World Bank Programs*. March 13, 2019, http://www.worldbank.org/en/programs/sdgs-2030-agenda.

[46] International Monetary Fund. "IMF and the Sustainable Goals." In *IMF Factsheets*. March 8, 2018, https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/16/46/Sustainable-Development-Goals.

[47] International Monetary Fund. "IMF and the Sustainable Goals." In *IMF Factsheets*. March 8, 2018, https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/16/46/Sustainable-Development-Goals.

[48] International Monetary Fund. "IMF and the Sustainable Goals." In *IMF Factsheets*. March 8, 2018, https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/16/46/Sustainable-Development-Goals.

[49]Carlos Alvarez, "ICT as a Part of the Chilean Strategy for Development: Present and Challenges," in *The Network Society. From Knowledge to Policy*, ed. Manuel Castells and Gustavo Cardoso (Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2005), 383.

[50]Carlos Alvarez, "ICT as a Part of the Chilean Strategy for Development: Present and Challenges," in *The Network Society. From Knowledge to Policy*, ed. Manuel Castells and Gustavo Cardoso (Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2005), 384-386.

[51] Saifedean Ammous. "Economics beyond Financial Intermediation: Digital Currencies' Possibilities for Growth, Poverty Alleviation and International Development." *Journal of Private Enterprise* 30, no. 3 (2015): 42-43. http://link.galegroup.com/apps/doc/A426900749/AONE?u=lond95336&sid=AONE&xid=ed506d10.

[52] Saifedean Ammous. "Economics beyond Financial Intermediation: Digital Currencies' Possibilities for Growth, Poverty Alleviation and International Development." *Journal of Private Enterprise* 30, no. 3 (2015): 42-43. http://link.galegroup.com/apps/doc/A426900749/AONE?u=lond95336&sid=AONE&xid=ed506d10.

[53] Saifedean Ammous. "Economics beyond Financial Intermediation: Digital Currencies' Possibilities for Growth, Poverty Alleviation and International Development." *Journal of Private Enterprise* 30, no. 3 (2015): 46. http://link.galegroup.com/apps/doc/A426900749/AONE?u=lond95336&sid=AONE&xid=ed506d10.

[54] Saifedean Ammous. "Economics beyond Financial Intermediation: Digital Currencies' Possibilities for Growth, Poverty Alleviation and International Development." *Journal of Private Enterprise* 30, no. 3 (2015): 46. http://link.galegroup.com/apps/doc/A426900749/AONE?u=lond95336&sid=AONE&xid=ed506d10.

[55] Saifedean Ammous. "Economics beyond Financial Intermediation: Digital Currencies' Possibilities for Growth, Poverty Alleviation and International Development." *Journal of Private Enterprise* 30, no. 3 (2015): 49. http://link.galegroup.com/apps/doc/A426900749/AONE?u=lond95336&sid=AONE&xid=ed506d10.

[56] Mircea Constantin Scheau and Pop Stefan Zaharie, "The Way of Cryptocurrency," *Economy Informatics* 18, no. 1 (2018): 33-34, https://search.proquest.com/docview/2172009989/fulltext/A6C9A3BE06904C6FPQ/1?.

[57]Saifedean Ammous. "Economics beyond Financial Intermediation: Digital Currencies' Possibilities for Growth, Poverty Alleviation and International Development." *Journal of Private Enterprise* 30, no. 3 (2015): 47. http://link.galegroup.com/apps/doc/A426900749/AONE?u=lond95336&sid=AONE&xid=ed506d10.

[58] Mircea Constantin Scheau and Pop Stefan Zaharie, "The Way of Cryptocurrency," *Economy Informatics* 18, no. 1 (2018): 35, https://search.proquest.com/docview/2172009989/fulltext/A6C9A3BE06904C6FPQ/1?.

[59] Jan Lanksy. "Possible State Approaches to Cryptocurrencies." *Journal of Systems Integration* 9, no. 1 (2018): 22. https://doaj.org/article/47ca1fef31254a5e8b1c9b62cad59c03.

[60] Jan Lanksy. "Possible State Approaches to Cryptocurrencies." *Journal of Systems Integration* 9, no. 1 (2018): 25. https://doaj.org/article/47ca1fef31254a5e8b1c9b62cad59c03.

[61] Jan Lanksy. “Possible State Approaches to Cryptocurrencies.” *Journal of Systems Integration* 9, no. 1 (2018): 25-27, https://doaj.org/article/47ca1fef31254a5e8b1c9b62cad59c03.

[62] Andrej Zwitter and Mathilde Boisse-Despiaux, “Blockchain for Humanitarian Action and Development Aid,” *Journal of International Humanitarian Action 3*, no. 1 (2018): 1, doi:10.1186/s410118-018-0044-5.

[63] Frantisek Sudzina. "Distribution of Foreign Aid in Cryptocurrencies: Initial Considerations." *International Advances in Economic Research* 24, no. 4 (2018): 387, http://link.galegroup.com/apps/doc/A563359711/AONE?u=lond95336&sid=AONE&xid=3405f7a3.

[64] Frantisek Sudzina. "Distribution of Foreign Aid in Cryptocurrencies: Initial Considerations." *International Advances in Economic Research* 24, no. 4 (2018): 387, http://link.galegroup.com/apps/doc/A563359711/AONE?u=lond95336&sid=AONE&xid=3405f7a3.

[65] International Development Research Centre, “INTERNET5: Shaping an Internet for Women’s Empowerment.” In *International Development Research Centre*. December 8, 2017, https://www.idrc.ca/en/research-in-action/internet5-shaping-internet-womens-empowerment.

[66]United Nations, “Sustainable Development Goals,” 2015, https://sustainabledevelopment.un.org/?menu=1300.

[67] J.R. Behrman, E. Skoufias, “Mitigating Myths about Policy Effectiveness: Evaluation of Mexico’s Antipoverty and Human Resource Investment Program,” *The ANNALS of the American Academy of Political and Social Science*, 606 (2006): 247, https://journals.sagepub.com/doi/pdf/10.1177/0002716206288956.

[68] Maxine Molyneux, “Mothers at the Service of the New Poverty Agenda: Progresa/Oportunidades, Mexico’s Conditional Transfer Programme,” *Social Policy & Administration* 40(2006): 432, http://resolver.scholarsportal.info/resolve/01445596/v40i0004/425_matsotapmctp.

[69] J.R. Behrman, and E. Skoufias, “Mitigating Myths about Policy Effectiveness: Evaluation of Mexico’s Antipoverty and Human Resource Investment Program,” *The ANNALS of the American Academy of Political and Social Science*, 606 (2006): 248, https://journals.sagepub.com/doi/pdf/10.1177/0002716206288956.

[70] International Development Research Centre, “Prospera Digital Phase II: Financial inclusion for low-income women in Mexico,” 2016, https://www.idrc.ca/en/project/prospera-digital-phase-ii-financial-inclusion-low-income-women-mexico

[71] Center for Global Development, “Doing Cash Differently: How Cash Transfers can Transform Humanitarian Aid” In *Overseas Development Institute*, September 2015, https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9828.pdf.

[72] Center for Global Development, *Doing Cash Differently: How Cash Transfers can Transform Humanitarian Aid, 10.*

[73] Center for Global Development, *Doing Cash Differently: How Cash Transfers can Transform Humanitarian Aid*, 15.

[74] Center for Global Development, *Doing Cash Differently: How Cash Transfers can Transform Humanitarian Aid*, 20.

[75] Shannon Doocy, Hannah Tappis, and Emily Lyles. “Are Cash-Based Interventions a Feasible Approach for Expanding Humanitarian Assistance in Syria?” *Journal of International Humanitarian Action* 1, no.1 (2016): 10, https://link-springer-com.proxy1.lib.uwo.ca/content/pdf/10.1186%2Fs41018-016-0015-7.pdf.

[76] UNHCR, *Operational Guidelines for Cash-Based Interventions in Displacement Settings* (Geneva, United Nations Refugee Agency, 2015), 31.

[77] “Joe Huston: ‘GiveDirectly: Cash Transfers, Basic Income, and Hurricane Relief’ | Talks at Google,” Youtube video, 25:35, posted by “Talks at Google,” February 8, 2018, https://www.youtube.com/watch?v=iyeIsVXjMzU.

[78] United Nations, *Sustainable Development Goals*, March 13, 2019, https://sustainabledevelopment.un.org/?menu=1300.

[79] United Nations, *Sustainable Development Goals*, March 13, 2019, https://sustainabledevelopment.un.org/?menu=1300.

Corporate Considerations

Visualizing Canada’s Future in the Fifth Domain

Regulate channels through which corporations interact with the internet to ensure these interactions are secure and direct self-interested behavior to benefit the public good.

Corporate Considerations

Commodification, Infrastructure & Corporate Security

Background

Corporations and the internet are intimately intertwined. Corporations are involved in the creation and maintenance of the infrastructure required to keep the internet running and connected, the creation of new commodities, and the transfer of traditional trade onto the internet. The presence of the internet as a medium creates the possibility for cyber attacks to steal intellectual property (IP).

The emergence of cyberspace has commodified a brand-new dimension of goods and services. Vulnerabilities within corporations' online databases and software have spawned an online black market where any individual, acting in either public or private interest, can bid for the control of these vulnerabilities or 'exploits.' This new plane of business has catalyzed the development of legitimate businesses and firms who not only sell vulnerabilities, but also broker exploit transactions. Businesses that deal in cyber protection have also appeared. They can be hired to investigate shortcomings and leaks in company software. Ultimately, cyberspace has been both a source of insecurity and a source of great financial opportunity.

Corporate security concerns and state-sponsored corporate espionage predate the advent of the internet and cyberspace. Cyberspace has broadened the scope of corporate insecurity, allowing the perpetration of espionage by a hacker half a world away. The losses from these attacks can be unimaginably costly, such as in the case of US Steel, where a cyber attack resulted in the loss of proprietary technology to a competitor and caused an estimated loss of $1.5 billion USD.

Corporations are integral to the operation of the internet. However, since corporations seek profit, they do not always act in the public good. As such, it is necessary for governments to regulate and incentivize these corporations to modify corporations' understanding of their interests and responsibilities. This includes incentivizing infrastructure development in areas which are not likely to generate profits and regulating data transfers when cost-effective measures may compromise the privacy of data. In the physical manifestations of cyberspace, cooperation between national governments and private corporations are required to pursue the public interest.

Commodification of Digital Arms

In the past few years there has been an exponential increase in demand for software and packets of computer code which allow hackers to capitalize on vulnerabilities and shortcomings in otherwise inaccessible computers and networks.

[80] These programs, commonly referred to as "exploits," are notoriously difficult to prepare against and present a threat not only to the privacy of individuals, but also to financial institutions, multinational corporations, and other sensitive sources of information. According to Kenneth Geers, a cyber-security specialist at America's Naval Criminal Investigative Service, the main difficulty in countering these cyber-

based weapons is the confidential way they are designed, sold, and used making it difficult to develop preventative measures.[81]

The scale and destructive capabilities of these exploits were put on display in 2010 when a joint Israeli-American endeavor, project "Olympic Games," developed a computer worm called "Stuxnet" which infiltrated uranium enrichment facilities in Iran, damaging over one thousand centrifuges.[82] Stuxnet was a discernible turning point in the commodification of digital arms. By developing this weapon, the United States initiated a digital arms race akin to the nuclear arms of the Cold War. Another distinction of this cyber-arms race in comparison to the Cold War is that cyber weapons are not limited to states; there exists instead a widespread, multilateral investment in cyber weapons.[83] The United States, China, and Iran all boast cyber warfare expenditures of more than a $1.5 billion USD between 2013 and 2017, with plans to increase the budget annually.[84] Furthermore, private firms that deal in digital arms, and corporations that want to prevent large-scale attacks are stockpiling digital weapons. The online demarcation between the public and private sphere are blurred as digital capabilities once owned by states more easily find their way into the hands of private actors.

The commodification of exploits originates in 'bug bounty programs,' which were initiatives by websites and software developers offering monetary compensation to those who reported, mitigated, or fixed vulnerabilities, with exchanges being insured through official firms.[85] However, there has been a gradual shift away from the bug bounty system; instead of reporting these vulnerabilities to the original vendor, they are instead auctioned off indiscriminately to the highest bidder.[86] The most lucrative of these vulnerabilities are 'zero-day vulnerabilities', with 'zero' referring to the amount of days the original vendor or developer was aware of this exploit. For example, if the vulnerability had been recognized for one day, it would be termed a 'one-day vulnerability.'[87] Zero-day vulnerabilities present the highest threat, as corporations have no time to protect themselves and their users. Currently, it is difficult to enforce regulations to prevent freelance programmers from selling these vulnerabilities to potentially dangerous actors.

Despite the malevolent and precarious nature of these exploits, their sale and purchase are legal. There are legitimate firms and businesses that develop their own exploits and act as middlemen, buying exploits from freelance hackers to sell to both private and state actors.[88] Moreover, in the realm of digital arms, state-sponsored actors do not have a monopoly over the best cyber weapons, and some of the most advanced cyber technology belongs to private firms.[89] Though state actors may have the advantage of funding, the gap in expertise between state and private actors continues to shrink, and state actors need to continue to develop protective measures at a fast pace if they want to stay ahead of the race.[90] The markets for these exploits have multiplied fivefold since 2004 and are appraised depending on the complexity of the code itself, the number of computers the exploit will grant access to, and the value of the computers it can infiltrate. Some of these exploits range from $50,000 USD, if the exploit can crack an older model running Windows XP to $500,000 USD, if the exploit can provide individuals access to Internet Explorer.[91] In extreme cases the market can be even more lucrative. In July 2018, a former employee of the Israel-based cyber technology firm NSO Group, was caught attempting to sell stolen exploits to foreign buyers at the cost of $50 million USD worth of bitcoin.[92] Though the details of what was being sold have not been disclosed, the price tag of this specific exploit suggests it was linked to a program with serious ramifications.

China provides a case study in the commodification of digital arms, specifically in the sphere of surveillance technology. Surveillance and the monitoring of public opinion is the norm throughout the Chinese government. As surveillance has embedded itself in the daily life of Chinese citizens, surveillance software has become a necessary expenditure for government.[93] With this increased demand in the Chinese market, surveillance technology has become increasingly efficient, requiring just a quick installation on a computer or phone to completely make available all comments, discussion, and search history on the device.[94] An offshoot of the demand for surveillance technology is online opinion reporting (輿情报告). Online opinion reporting is essentially a consulting service provided by private firms which advise on the best possible strategies to monitor opinion, assess risks, and repair possible deficiencies in public opinion.[95]

China vs. United States: Sinovel Wind Group vs. AMSC and US Steel vs. Baosteel

The "trade war" between the United States and China is foregrounding corporate espionage and the theft of Intellectual Property (IP). Given the storage of IP and other sensitive information online, it is much more difficult to protect against theft or unauthorized access.[96] There are two useful cases to demonstrate the dangers of IP theft and corporate espionage for the private sector. The first case is the conflict between the American company AMSC (American Superconductor Corporation) and the Chinese firm Sinovel Wind Group during which the Chinese were given codes by a former American employee to access IP. Sinovel noticed the higher returns earned by AMSC, who provided higher value-added components. Sinovel specialized in low-cost manufacturing, and thus earned lower profit margins and wages. Sinovel's solution was to offer a large payout to a former AMSC engineer who provided proprietary source codes, allowing Sinovel to copy the AMSC system.[97] This was a devastating blow to AMSC since Sinovel was its biggest customer, accounting for roughly two-thirds of the AMSC's revenue. This IP theft resulted in total damages exceeding $60 billion USD, and job losses of more than sixty percent of AMSC employees. Stock values fell by ninety percent, and the legal battle was also incredibly costly.[98]

In the second case between US Steel and several Chinese steel companies including Baosteel, a Chinese corporation directly hacked and stole IP from the computer of a US Steel employee. It had taken the American firm around a decade and millions of dollars of investment to develop their product, and after the alleged hacking, Baosteel took only a couple of years to produce the same quality steel at far less cost. US Steel is estimated to have lost $1.5 billion USD over this theft and filed a complaint with the US International Trade Commission, although there has been no true resolution.[99]

Both of these scenarios demonstrate how vulnerable IP is online, the devastating effect of IP theft on corporations and employees, and the lack of defence against or effective punishment for IP theft. The reasons for a lack of response are numerous: areas of jurisdiction and the reach of international law, a lack of enforcement mechanisms, and cyber security abilities.[100]

Internet Infrastructure

Internet infrastructure refers to the current physical infrastructure through which computers connect with the internet and other computers. Internet backbone refers to the major networks provided by Internet Service Providers (ISPs). These ISPs create the infrastructure which allows consumers to connect to other individuals on their network, often for a fee. However, the networks created by each ISP often only allow individuals to connect to other individuals on their network; one individual connected to a network created by Company A, and a second individual connected to a network created by Company B would not be able to interact with each other online without an Internet Exchange Point (IXP). These IXPs, also referred to as Internet Exchanges (IXs) or Network Access Points (NAPs), allow the transfer of data from one network to a different network. Therefore, the presence of IXPs is required for interaction between two different networks.

The creation of internet infrastructure is a complex process, often evolving out of previously existing telephone infrastructure. The primary, and frequently most expensive work is usually completed by the government, such as in USA, Germany, and Argentina.[101] After the base level infrastructure is created, the creation of internet infrastructure usually shifts to the private sector. One of the primary motivators is the perception that innovation is better produced by the private sector.[102] The private sector, as ISPs, then usually develops networks in response to perceptions of demand. However, this demand does not occur evenly across geographies, and thus networks are built in a patchwork manner. Furthermore, IXPs are often built in a similar patchwork manner, in response to demand. Sometimes, governments respond to this by creating incentives for private businesses to build infrastructure in areas which need it, but may not be cost effective or rational from a cost-benefit standpoint. Alternatively, if these incentives are not in place, then issues of 'data sovereignty' can occur.[103]

Data sovereignty refers to the fact that data is usually subject to the laws and regulations of the country in which it exists. In states with developed internet infrastructure, this is not an issue; in states which are reliant on external internet infrastructure, this becomes problematic. When a state is reliant on external infrastructure, any transfer of data which utilizes external infrastructure is subject to the laws of all states it passes through at different points in its journey. This becomes an issue when states have different national laws on data and privacy; as law is prima facie territorial, this extension puts data at risk.[104]

Data sovereignty refers to risks from state actors in particular, because national governments often legislate around data and how it can be used. These laws, however, do not apply to states, only to private actors. Facebook could be reprimanded for its handling of personal data, as proven by the recent implementation of General Data Protection Regulation (GDPR) in the European Union (EU). However, the USA could not be reprimanded to the same extent for its treatment of data under the Patriot Act.[105]

Solutions have thus been primarily to increase the capabilities of the state; in particular, this can be observed in reactions toward mass surveillance in the USA. Under the Patriot Act, the USA allows itself unlimited access to data it deems critical to the security of the state. This has provoked reactions internationally, including from Canada, the EU, and international organizations. Canada preceded by legislating data sovereignty, requiring domestic transfers of data to remain within Canadian territory. It has supported this by increasing the number of IXPs from three to twelve in recent years.[106] In another example, when the USA subpoenaed financial information and began mining it from the Society for Worldwide Interbank Financial Telecommunications (SWIFT), the organization responded by moving their cloud network from the USA to Switzerland.[107] Lastly, when the EU experienced what it saw as violations of their citizens' data in the USA due to EU cloud networks based in the US, they responded by commissioning an EU-based cloud.[108] Cloud networking has been an important topic in the EU, referred to in Privacy Briefs as one of the key challenges which need to be addressed by policy developers.[109]

Recommendations

2.1 Institutionalizing the Practice of Hackers for Hire

Actors: Private Corporations, National Governments, International Organizations
Type of Recommendation: Normative
Main Cyber Issues Involved: Security Threat, Corporate Espionage, Commodification of Digital Arms
Main IR Issues Involved: Security

Explanation: The black market for exploits will not fade away any time soon. With a market this lucrative, preventing the trade of exploits through legal means would be challenging as it would require heavy state interference and international cooperation. However, the legal route to criminalize and prosecute exploit traders is unproductive. Corporations and governments with a stake in securing their software and code should invest heavily in 'hackathons,' where groups of freelance hackers are given carte-blanche to infiltrate security measures and are compensated for every zero-day vulnerability they find. Hackathons have been very successful in the past, with the 2018 Pentagon-sponsored hackathon revealing over 130 vulnerabilities in the Pentagon's system.[110] A smaller scale version of these 'hackathons' are possible for corporations through the recruitment of private firms hired to uncover corporate spies or vulnerabilities. Essentially, the legal aspect of the exploits commodification should be as lucrative as the illegal black market.

Challenges: The main challenge to this recommendation is the cost. It is expensive to hire private cyber security firms and it is even more expensive to incentivize freelance hackers to commit to a less profitable bug bounty model.

Justification: Spending the money to have regular interval 'audits' through hackathons and private security firms would be comparably cheaper than having sensitive information linked to finances, health, conventional weapons and energy compromised. Furthermore, with the commodification of digital arms being a relatively new phenomenon, private firms capable of dealing with these threats remain few. If these firms are hired more often, and the demand increases, these firms will inevitably increase in securitization capabilities.

2.2 Promotion of Data Sovereignty Through Domestic Infrastructure Development

Actors: Private Corporations, National Governments
Type of Recommendation: Normative

Main Cyber Issues Involved: Data Sovereignty, Internet, Infrastructure
Main IR Issues Involved: Security, Domestic Capabilities, Extra-territorial Nature of Cyber

Explanation: By increasing domestic investment in ICT infrastructure, the requirement for infrastructure supplied by other states to domestically transmit data would decrease. This would increase the self-sufficiency of individual states. It also has the added benefit of increasing the internet capabilities of the state, which can be used to provide the public good of the internet. This would likely be undertaken through one of three methods; infrastructure development by the state, development by the private sector, or a combination of public and private investment. Development pursued by a combination of the public and private sector would allow for cost-effective development spurred by the state, without imposing the requirements of maintenance and innovation on the state.

Challenges: There are two main challenges to this recommendation. First, the creation of domestic infrastructure including IXPs and networks by ISPs can be expensive, especially when there are large geographical spaces between small population groups. Secondly, this would only protect data which is domestically transferred, not data which is transferred to corporate actors in a different state. Thus, while data sovereignty can be protected domestically, this does not tackle the issue of multinational corporations and the extent to which they can provide data sovereignty.

Justification: This would provide states with the ability to maintain territorial control of the internet exchanges that happen within their borders, and reduce the reliance on non-domestic infrastructure.

2.3 . Employee Training and Education

Actors: Private Corporations
Type of Recommendation: Normative
Main Cyber Issues Involved: Cyber Literacy, Cyber Security
Main IR Issues Involved: Governance, Leadership

Explanation: Most employees do not know much about cybersecurity. Thus, their individual actions, such as passwords and internet activity on company computers, may inadvertently have a negative impact on the company's security. For example, the most common passwords remain simple, such as "123456," and many firms allow employees to connect personal devices to the company's network.[111] Corporations must ensure that everyone has some basic knowledge of the risks and necessary mitigation, not only those in Information Technology (IT) or cyber-relevant positions. Mandatory training every quarter for all employees to update changes in practice could work to achieve this recommendation.

Potential Challenges: Depending on the size of the business and its location, it may be very difficult to ensure that all employees get the training and supervision that they require.

Justification: With more important information being stored online, all employees must understand the risks and challenges and how to mitigate them. Corporations must ensure their employees receive the necessary training to understand their security online, clearly define acceptable and unacceptable online practices, and have a clear risk management strategy outlined for employees to follow.[112]

[80] The Economist, "The Digital Arms Trade," The Economist, last modified March 30, 2013, https://www.economist.com/business/2013/03/30/the-digital-arms-trade.

[81] The Economist, "The Digital Arms Trade".

[82] Virgilio A. Almeida, Danilo Doneda, and Jacqueline De Souza Abreu, "Cyberwarfare and Digital Governance," IEEE Internet Computing 21, no. 2 (March/April 2017): 69, doi:10.1109/mic.2017.23.

[83] Amit K. Maitra, "Offensive Cyber-Weapons: Technical, Legal, and Strategic Aspects," Environment Systems and Decisions 35, no. 1 (November 2014): 177, doi: 10.1007/s10669-014-9520-7.

[84] Maitra, "Offensive Cyber-Weapons," 177.

[85] Matthew J. Schwartz, "Weaponized Bugs: Time For Digital Arms Control," Information Week, last modified March 9, 2019, https://www.darkreading.com/attacks-and-breaches/weaponized-bugs-time-for-digital-arms-control/d/d-id/1106686.

[86] Matthew J. Schwartz, "Weaponized Bugs: Time For Digital Arms Control," Information Week, last modified March 9, 2019, https://www.darkreading.com/attacks-and-breaches/weaponized-bugs-time-for-digital-arms-control/d/d-id/1106686.

[87] Matthew J. Schwartz, "Weaponized Bugs: Time For Digital Arms Control," Information Week, last modified March 9, 2019, https://www.darkreading.com/attacks-and-breaches/weaponized-bugs-time-for-digital-arms-control/d/d-id/1106686.".

[88] The Economist, "The Digital Arms Trade".

[89] Neri Zilber, "Hackers for Hire: What Happens When the Best Cyberweapons are Controlled by the Private Sector?," *Foreign Policy* 230 (Fall 2018): 63, http://link.galegroup.com/apps/doc/A556838653/AONE?u=lond95336&sid=AONE&xid=d8dc27d8.

[90] Neri Zilber, "Hackers for Hire: What Happens When the Best Cyberweapons are Controlled by the Private Sector?," *Foreign Policy*230 (Fall 2018): 63, http://link.galegroup.com/apps/doc/A556838653/AONE?u=lond95336&sid=AONE&xid=d8dc27d8.

[91] The Economist, "The Digital Arms Trade".

[92] Neri Zilber, "Hackers for Hire: What Happens When the Best Cyberweapons are Controlled by the Private Sector?," *Foreign Policy*230 (Fall 2018): 63, http://link.galegroup.com/apps/doc/A556838653/AONE?u=lond95336&sid=AONE&xid=d8dc27d8.

[93] Rui Hou, "Neoliberal Governance or Digitalized Autocracy? The Rising Market for Online Opinion Surveillance in China," Surveillance & Society 15, no. 3/4 (2017): 420, doi:10.24908/ss.v15i3/4.6610.

[94] Rui Hou, "Neoliberal Governance or Digitalized Autocracy? The Rising Market for Online Opinion Surveillance in China," Surveillance & Society 15, no. 3/4 (2017): 421, doi:10.24908/ss.v15i3/4.6610.

[95] Rui Hou, "Neoliberal Governance or Digitalized Autocracy? The Rising Market for Online Opinion Surveillance in China," Surveillance & Society 15, no. 3/4 (2017): 421, doi:10.24908/ss.v15i3/4.6610.

[96] Committee on Homeland Security, Economic Espionage: A Foreign Intelligence Threat to American Jobs and Homeland Security, (Washington: United States Government Printing Office, 2012), http://www.govinfo.gov/content/pkg/CHRG-112hhrg79843/pdf/CHRG-112hhrg79843.pdf?fbclid=IwAR1-GFgUM-ulWOVK2banlsHZY1d3xbxYl998-PP3gJGvA94BGda1by07iKI.

[97] Melanie Hart, "Criminal Charges Mark New Phase in Bellwether U.S.-China Intellectual Property Dispute," Center for American Progress, last modified June 27, 2013, https://www.americanprogress.org/issues/security/news/2013/06/27/68339/criminal-charges-mark-new-phase-in-bellwether-u-s-china-intellectual-property-dispute/.

[98] [98] Melanie Hart, "Criminal Charges Mark New Phase in Bellwether U.S.-China Intellectual Property Dispute," Center for American Progress, last modified June 27, 2013, https://www.americanprogress.org/issues/security/news/2013/06/27/68339/criminal-charges-mark-new-phase-in-bellwether-u-s-china-intellectual-property-dispute/.

[99] Claude Barfield, "China Exposed on Steel Technology Cyber Theft: Why No Indictments?" *American Enterprise Institute* (March 2016): http://www.aei.org/ publication/china-exposed-on-steel-technology-cyber-theft-why-no-indictments/.

[100] Andrew F. Popper, "More than the Sum of All Parts: Taking on IP and IT Theft Through a Global Partnership," Northwestern Journal of Technology and Intellectual Property 12, no. 4 (November 2014): 254-255.

[101] Hao Xiaoming and Chow Kay, "Factors Affecting Internet Development: An Asian Survey," First Monday 9, no. 2 (2004): 8, doi:10.5210/fm.v9i2.1118.

[102] David R. Johnson and David Post, "Law and Borders: The Rise of Law in Cyberspace," Stanford Law Review 48, no. 5 (1996): 3, doi:10.2307/1229390.

[103] Louise Amoore, "Cloud Geographies," Progress in Human Geography 42, no. 1 (2016): 8, doi:10.1177/0309132516662147.

[104] David R. Johnson and David Post, "Law and Borders: The Rise of Law in Cyberspace," Stanford Law Review 48, no. 5 (1996): doi:10.2307/1229390.

[105] Primavera De Filippi, and Internet Policy Review. "Foreign Clouds in the European Sky: How US Laws Affect the Privacy of Europeans." Internet Policy Review 2, no. 1 (2013), 2.

[106] "Canada's Internet Factbook," CIRA | Canadian Internet Registration Authority - FACTBOOK 2014 | The Canadian Internet, January 11, 2019, , https://cira.ca/factbook/canada's-internet-factbook-2018.

[107] Louise Amoore, "Cloud Geographies," Progress in Human Geography 42, no. 1 (2016): 8, doi:10.1177/0309132516662147.

[108] Louise Amoore, "Cloud Geographies," Progress in Human Geography 42, no. 1 (2016): 8, doi:10.1177/0309132516662147.

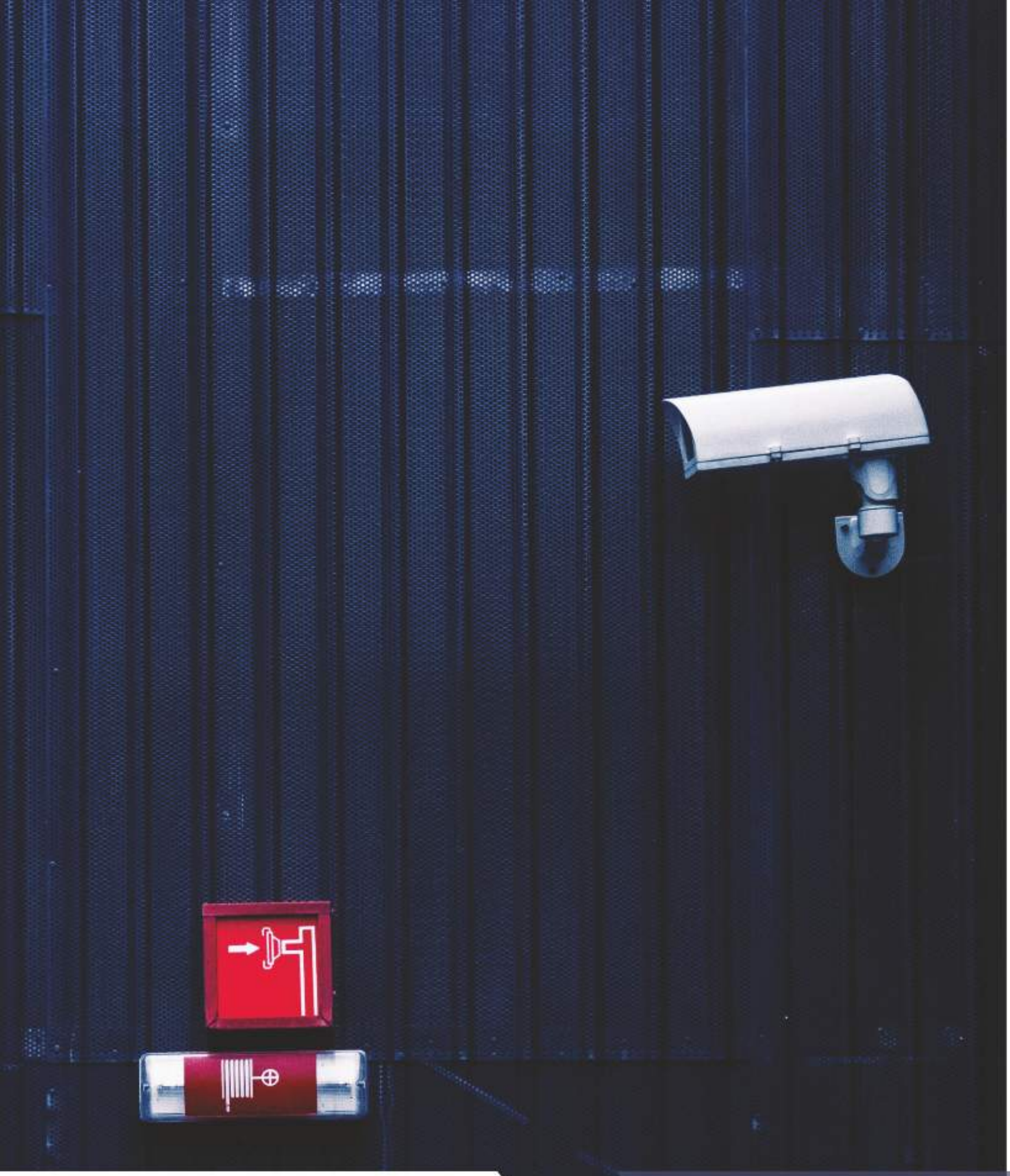
[109] "Policy Brief: Privacy," In *Internet Society*, October 30, 2015. https://www.internetsociety.org/policybriefs/privacy/.

[110] Claude Solnik, "Hackers for Hire," Long Island Business News, last modified October 4, 2018, https://libn.com/2018/08/24/hackers-for-hire/.

[111] Scott J. Shackelford. "Business and Cyber Peace: We Need You!" *Business Horizons* 59, no. 5 (2016): 543, doi:10.1016/j.bushor.2016.03.015.

[112] Scott J. Shackelford. "Business and Cyber Peace: We Need You!" *Business Horizons* 59, no. 5 (2016): 543, doi:10.1016/j.bushor.2016.03.015.

Individual Privacy Rights



Visualizing Canada's Future in the Fifth Domain

Protect the individual's right to personal privacy and control over the collection and use of their own private data, and prevent misuse of this information.

Individual Privacy Rights

Commodification of Data & Data Profiling

Background

In 2017, there were an estimated 3.65 billion recorded internet users active, with access to the internet reaching 89% of the population in North America.[113] With recent advancements in internet technologies, the average consumer can access everything from clothes to food from their homes, relatives and friends around the world have become an email away, and everything from recipes to banking information is available with the press of a button. However, this convenience comes at a cost, one which many are ignorant or indifferent towards. Cyber technologies and the internet have revolutionized much of our lives, yet in doing so, our lives have also become increasingly dependent on these same technologies.[114] While the individual user is happy to enjoy the benefits of cyber technologies, very few realize the extent to which these same advancements have jeopardized individual security and privacy.[115] By its very nature, the internet runs through the collection and use of points of data, sending and receiving information between devices connected in networks, but what happens to this information after its initial use?

While using any application that is connected to the internet, thousands of individual pieces of data are generated, which tracks specific keystrokes, browsing history, and which device is facilitating this activity. When the individual accesses the internet from a mobile device, such as a cellular phone or personal computer, data such as the location of the device and its movements may also be logged when on the move. In short, every action taken online, from which advertisements are seen to the exact content of a personal message sent or received represents a point of data generated by the individual. Each piece of data can be traced back to its source, tied either to the device it originates from, its IP address or, as is increasingly the case, the personal user account of the individual.[116] These personalized pieces of data are called individual data.[117]

It is the status and use of this data after its initial purpose which poses a myriad of risks to the privacy and rights of the individual. While some services or websites may discard this individual data after its initial use, many more retain this data, collecting statistics regarding the activity of each user online.[118] Many companies use this data for general improvement purposes, such as navigation programs' usage of average travel speeds along routes to calculate traffic speeds for its users, or streaming services flagging frequently viewed content to highlight on its homepage for users. But often, the collection and profiling of this data is much more specific than the collection of general statistics, with each individual user's activity being catalogued. This practice is referred to as data profiling, which can range from broad uses such as determining which advertisements will prove effective at catching the interest of groups or individuals, to tracking the usage or movement patterns of a specific user.[119] While some states or bodies, such as the European Union, have enacted restrictions of the collection of individual data and its profiling, in many cases, these regulations are minimal at best, and often the individual user has little formal protections against the collection of this information, its profiling or its usage. [120] Even when companies or organizations do not misuse these data profiles, their very existence poses a threat to the security of the individuals profiled, with sensitive information like personal messages, banking records and personal details often included in these profiles. Even data profiles compiled by government agencies pose threats to individual security, as was demonstrated in 2015 when the Office of Personnel Management in the USA was targeted by hackers, resulting in over 5 million fingerprint files being compromised.[121]

While the existence of these profiles poses a significant risk to the individual, there has been a positive trend in recent years, with consumers in Canada, the United States, and Europe, among others, calling on their governments for more detailed protections to individual privacy and for regulations regarding this individual data.[122] Yet these protections alone have not had the desired impact, and as large corporations have increasingly absorbed smaller firms, large technology giants have developed a form of online monopoly, circumventing the need for consent to data profiling by simply making agreement to their terms the price of entry to large portions of the online space.[123] While steps have been taken to address the implications of these detailed individual data profiles, the truth of the matter is that their existence and current uses pose significant risks to the individual. From targeted breaches by single hackers, to corporate sales of thousands of profiles, and law enforcement monitoring of suspected criminals using data profiles, there is evidently a need for a comprehensive framework to address and mitigate these risks moving forward. While recent years have seen groundbreaking regulations introduced in numerous states to regulate the creation and misuse of these data profiles, the unfortunate reality is that in many cases, these regulations are only marginally effective. Without a more detailed understanding on the part of users, regulations designed to protect the individual, such as required consent or the option to prevent data retention are largely ineffective, and even when users may wish to opt out, many services have made the provision of consent a requirement to utilize services.

Hacking and Personal Use of Individual Data

The most obvious form of individual data profiles are those created by each individual willingly, user accounts with services like Facebook, Google and other social media platforms. User accounts are regularly hacked, and have become major sources of personal data used in the generation of data profiles. One of the major risks posed by these profiles are breaches to the servers of these services, usually as a result of targeted hacking attempts. In these cases, the central area of concern is the lack of information available to users regarding the risks posed by offering up this amount of personal information to these services, and subsequent failures on the part of these services to disclose these breaches. Often, the information accessed by these hacks is banking information, from websites that facilitate online transactions, such as Marriott International, which had the data of 500 million customers stolen between 2014 and 2018 and included contact information, passport numbers and travel history of rewards members.[124] Other instances, such as the 3 billion Yahoo user accounts compromised between 2013 and 2014 saw dates of birth, phone numbers, full names, and shared files stolen.[125] Social Security and credit card information for 143 million users were lost by Equifax in 2017, through a “vulnerability in their website.”[126] Many of these data breaches are to gather information for sale to a third party, to access accounts for misuse and to gather access to banking information and accounts. However, there are other more insidious examples of hacking leading to bullying, blackmail and permanent harm.

When compromised, these accounts pose significant security threats to users, as information provided to trusted sources is often accessed by unauthorized parties, and can be released or misused without consent. The hacking of the website Ashley Madison has been one of the large scale data breaches that has gained the most attention from the media and public. The website, marketed as a service for extramarital affairs had data leaked by a group titled “The Impact Team,” and was discovered when partial data leaks were released and messages were left on employees’ desktops by the hacking group.[127] The company was threatened with the release of the information of approximately 40 million users, largely from the US and Canada, who were using the site to conduct secretive, “discreet” affairs, if the company did not permanently shut down its websites.[128] Information supposedly accessed by the group included full names, addresses, credit card information, and profiles with intimate sexual details. After the company ignored these demands, The Impact Team periodically released partial leaks of profiles, emails, company files and credit transactions, including notable figures such as Joshua J. Duggar who came under fire, as well as approximately 15,000 American military and government employee emails.[129] Ashley Madison was remarkable, as the information released severely damaged reputations, and sparked interest in sites such as trustify.info, which claims to check if your personal email has been part of a data breach. Furthermore, divorces, work issues/dismissals and even suicides were theorized to be connected to the release of the information, although, it is difficult to definitively attribute such events to this leak.[130] Furthermore, phishing emails continue to use threats of sensitive or embarrassing information to attempt to coerce payments from affected individuals. This case highlights how user profiles, including data willingly provided can be permanently harmful, with no option for reversal despite once this information is put online.

An additional example of this type of risk comes from 2018, when Canadians found their bank accounts at risk with the breach of two major banks, Bank of Montreal and Simplii Financial (owned by CIBC). This breach is estimated to have affected up to 90,000 customers who may have faced fraudulent activity, stolen data and frozen accounts.[131] While both banks were quick to state that they would reimburse all fraudulent transactions, many of these accounts lost thousands of dollars, and until their claims were investigated customers were unable to access online accounts and to use their debit cards in many instances.[132] For online based bank Simplii, this crippled services for affected customers. Hacking into bank accounts can have extreme consequences, revealing sensitive data such as financial history, contact information, security questions and social security number. These all contribute easily to accessing other accounts, and creating fake identities using stolen data. Further, the money lost in these breaches can impact credit scores, ability to pay bills while waiting for reimbursement, assuming reimbursement is possible, and destroys trust in banking institutions. This is especially true services increasingly transition toward online access.

Over 105 million adults in America alone are aware of receiving at least one data breach notification in their lifetime, however 44% said they found out through alternative sources first.[133] The growth of sites such as “haveibeenpwned.com,” Breachalarm and DeHashed, which check email addresses, passwords and personal information to see if it is in any known lists of data breaches is indicative of the increasing acceptance on the part of users regarding the potential of data breaches as a central part online activities. Similar sites appeared following Ashley Madison, creating a searchable list, or an easy way to check if you were part of the leak. These sites fill a gap right now, as many sites and companies fail to inform consumers when a breach has occurred, even if their information might be part of the breach, often in order to prevent backlash or loss of business. However, this creates difficulty for an individual on the web to know if they need to update accounts to protect their information in the future and leaves them vulnerable especially as a common phishing tactic is to claim an account or password has been compromised and some of this information can be used for identity theft given enough time. Furthermore, one study shows that customer loyalty was not strongly influenced by a data breach when the customer was informed promptly.[134] This not only shows that individuals are aware of the commonality of breaches, but also that they are comforted by a company that appears to be responding to the threat with their interests in mind. If websites begin disclosing data breaches promptly, this also leaves room for those that fail to disclose, or that are inadequately protecting data to be shamed by the public and the media, as many companies already find occurring during data breaches given that there is no proper procedure which might allow for redemption.

In general, the increasing amount of personal information being provided and collected online has allowed a strong hacking community to thrive, both for positive security efforts, and for misuse and data breaches. It is no longer enough for users to use false information and cover their webcams when seeking to remain anonymous. When online companies are breached, information is accessed from user accounts, but also increasingly from users who may have never willingly or knowingly entered any data, such as search histories or location services. The increasing frequency of these breaches pose new questions regarding how best to govern the cyberspace. How can individuals protect their information online? How much trust can individuals put in business, while still protecting themselves? What forms of recourse do consumers have when their information is breached? This topic relates to both government and business violations of individual privacy, as data profiles collected by both are vulnerable to these targeted breaches and struggle to keep pace with the developing technology to get past firewalls and security measures. As beneficial innovations continue regarding the uses of the cyberspace, the negative innovations also enable misuses of this same space. As a result, individuals must be aware of all data connected to their accounts, and consider potential misuses should that data be released when providing information online. Further, legal framework to address these breaches must be considered as following many breaches lawsuits arise in vast numbers against the company and calls for criminal consequences for the hackers. Breaches have become a common and consistent occurrence, and individuals must monitor accounts, and consistently check their own information and security settings to ensure they are not the victims of data breaches and other misuses of cyber data.

Corporate Uses of Individual Data

Another risk to the privacy and security of individual users is that posed by the intentional sale of data profiles on the part of online companies. Although the number of individuals utilizing social media platforms is becoming increasingly widespread, many users do not fully understand what they are agreeing to when using these platforms, specifically how their data is collected and sold by each platform. Moreover, users generally remain unaware as to the responsibilities that these actors have in regard to the protection of their individual data. Facebook and Google are two of the most popular websites in use today. One is the most popular social media platform and the other remains the most commonly used search engine, while increasingly expanding to provide numerous other services.[135] The amount of individual data that each collects on its users is enormous, and as such raises several concerns regarding user privacy and the protection of individual data.[136] It should be noted that although both platforms have privacy policies outlining how they collect and use individual data, these are often vague and by no means extensive in their descriptions of the specific ways in which each user's individual data is used.[137] For instance, both platforms describe several sources of automatically logged individual data as including search queries, cookies, local storage of user's individual data, the device that the user is accessing the platform from as well as their location.[138] These privacy policies themselves are often problematic in several ways. First, the complex terminology employed in such policies is often beyond the level of comprehension of the average user. The second issue is the sheer length of the policies themselves. It is estimated that it would take an internet user an average of two hundred and fifty hours per year to read the privacy policies of the websites that they visit in their entirety.[139]

There are two types of information that these platforms collect. As mentioned previously, these online services collect data through user profiles, made up of information that users typically provide during the initial sign up process. Facebook terms this form of data 'information you provide', and similarly Google refers to this as 'information you give us.' However, Facebook's privacy policy also states, 'we also collect information about how you use our services' which is comparable with Google's reference to 'information we get from your use of our services.'[140] Both platforms take both types of information that they collect and centralize it to create a more complete profile of their users.[141] A 2014 update in Facebook's privacy policy introduced further data collection measures through the use of cookies and social plugins like Facebook's 'Like Button'.[142] However, the majority of data collected by Facebook is still voluntarily provided by the user during the sign up process and through the creation of and updates to their profile.[143] Although Facebook gathers a significant amount of individual data on its users, Google exceeds Facebook both in the sheer amount of data that it gathers due to the extensive use of its search engine and apps as well as its greater tracking abilities.[144] Although like Facebook, Google also gathers data from the personal information provided by its users, Google's primary source of individual data collection is 'search query data.' This information is composed of the content that a user searches for when using a Google platform.[145] Moreover, when Googled introduced Google+ in June of 2011 it brought about a significant change in the way search results were increasingly personalized with less priority given to relevancy. Two factors that influence a user's search results include the country that they are in, as well as if they are logged into a Google account which then allows for Google to determine more favourable results based upon individual search histories.[146]

Although the use of such platforms is often free, profit is earned by the platform through advertising. Individual data is of increasing economic value and social media platforms are built upon this idea.[147] The collection and sale of user data is an increasingly important driver of profit for social media platforms and online retailers.[148] As a result, social media sites have an incentive to encourage their users to enter as much information about themselves as possible so that this data can be used to provide more targeted advertisements and increase revenue for both the platform itself and advertisers.[149] To highlight, advertisements make up 98 percent of Facebook's revenue.[150] Most social media platforms such as YouTube, Facebook, Twitter and Google all state that by creating an account and agreeing to their terms and conditions, a user agrees to allow them to share and sell their data for several purposes, the most common being marketing. For instance, Google's terms and services for Android smartphone users allow them to track nearly all of the user's internet activity. Facebook and Google take user data and contextualize it in a way that will be relevant to marketing and advertising.[151] Due to their extensive database of individual data, they have the ability to reach a brand's target market in ways far beyond that of traditional forms of advertisement. These platforms can identify trends in a user's preferences, desires, and needs and in turn place advertisements that the user is far more likely to engage with.[152]

Facebook successfully delivers what they term to be "social ads" to their users. Facebook targets certain ads towards particular demographics based on age and gender, user preferences, engagement with content on the platform, as well as interests of their Facebook friends.[153] Arguably, the business models of these social media platforms themselves are aimed at privacy violation.[154] Both Facebook and Google engage in behavioural advertising, which entails tracking its users' online behaviour and then using the data collected to show advertisements that are personally tailored to each individual. They also engage in contextual advertisement which refers to advertisements that are related to the content found on a given website. However, the line between behavioural advertising and contextual advertising has become increasingly thin as it has been found that when search engines such as Google display contextual advertisements the content shown is also influenced by past search queries tied to the user's IP address.[155]

Facebook and Google explain who they share user's individual data with using broad umbrella terms such as "partners," "customers," "subsidiaries and companies," "organizations," and "individuals outside Google."[156] Furthermore, the exact degree of access that third party companies have to user data collected by social media platforms is often greater than necessary. For instance, a study looking at 150 popular Facebook applications found that they enabled access to more user data than was needed for the purposes of advertising.[157] Moreover, Facebook and Google both do not adequately disclose the type and extent of the personal information that is provided to advertisers. In particular, although users are aware of the information that they willingly provide to these platforms, they are not aware of exactly what information is later collected as a result of their use of the platform.[158] Moreover, these platforms have no control over how these third parties use the data provided beyond their initial purposes. Despite regulations in place designed to protect individuals from this invasive profiling and the subsequent sale of these profiles, many online services have been shown to comply with the letter of the law, while circumventing its intent. For example, Google notably does not allow third parties to obscure features such as the 'opt out' buttons in an effort to gain more access than needed in regard to mobile applications found in Google's Android app store, yet places no constraints on what forms of data these applications may request as "information they need" to function.[159] Additionally, Google itself is known to use questionable tactics to obtain user consent, as it has been noted that the Gmail app will repeatedly request access to a user's microphone and camera until they agree.[160] Unfortunately, it is difficult for a user to identify if their privacy has been violated if they are not aware of the personal information that has been collected regarding them and how exactly this information is being used.[161] This collection of user data into profiles is enabled by both the weakness in legal restrictions on this practice, as well as consumer ignorance regarding their own privacy. While there are some legal constraints on profiling in place, such as the need for individual consent, companies operating online have increasingly utilized dishonest methods to obtain this consent, and without stricter legal restrictions on how this consent must be given, this trend is likely to continue. Furthermore, these existing protections are effectively useless if users simply blindly agree to a service's complicated and often inaccessible terms and conditions, again highlighting the need for informed consumers to play an active role in protecting their own privacy online.

Government Uses of Individual Data

Another area of risk posed to the individual regarding the use of their own data profiles comes from state actors, who often either directly circumvent their own laws protecting citizen privacy, or outright make legal exception for themselves. In Canada, use of the internet as a mainstream communications mechanism is becoming increasingly surveilled by law enforcement and intelligence agencies, posing a challenge to the privacy and non-discrimination rights that are core to the Canadian legal framework[162]. New legal powers to monitor users have been particularly targeted toward terrorist activities and suspects, where agencies now have the capabilities to track and analyze the use of Internet for communication, propaganda, research, planning, publicity, fundraising and creating a distributed sense of community. Policing of such activities has therefore become more preemptive as surveillance bodies now have the legal right and the surveillance capabilities necessary to criminalise a range of activities that could be deemed as 'supporting' terrorism.

Several laws govern the scope of Canadian activities in the domestic and international surveillance realm. The *National Defence Act* governs the Canadian Security Establishment (CSE) which holds a mandate limiting its activity to the following:

A. To acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
B. To provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada;
C. To provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.[163]

The CSE commissioner has expanded upon the limitations on parts a) and b) by stating that "…CSEC [CSE] may use and retain a private communication obtained this way but only if it is essential to either international affairs, defence or security, or to identify, isolate or prevent harm to Government of Canada computer systems or networks."[164] CSE is unanimously defended by the government, with ministers consistently claiming that the scope of its activities is compliant with the law.

The introduction of Bill-C51 in 2015 further expanded the powers of CSIS without enhancing related oversight. The bill facilitated information sharing practices within Canadian and Canada-US agencies and included the Security of Canada Information Sharing Act (SCISA), an act which permits sharing of government surveillance data across seventeen government institutions, most of which have little to do with terrorism. University of Toronto professor Ron Deibert has argued that "the Canadian checks and balances just aren't there. We have no parliamentary oversight of CSEC [CSE], no adequate independent entity to watch the watchers and act as a constraint on misbehaviour. It just doesn't exist now."[165]

In an email to the *Globe and Mail*, former CSE spokesperson Ryan Foreman said that while there are accidental intercepts of the content of the Canadian communications that they are mining, they attempt to make this data anonymous after they obtain it. "Metadata is used to isolate and identify foreign communications, as CSE is prohibited by law from directing its activities at Canadians," writes Foreman. While the collection of metadata was temporarily suspended in 2008, it has since been reinforced.

Metadata, or data about data, is a large debate within the study of Canadian privacy and surveillance law. It is known that a metadata program exists in Canada, much like our US counterparts, the details of the program have never been publicly disclosed and the questions about the privacy implications of metadata collection remain unanswered.[166] The argument that metadata collection is less invasive than other methods should be challenged. The process can include geolocation information, call duration, call participants and internet protocol addresses. Though it is assured that these methods are not invasive, studies have shown that after months of anonymized cell phone data, only four data points were needed to identify a specific person 95 percent of the time, while others have proved that sexual identity can be guessed based on Facebook metadata.[167] CSE acknowledged in 2008 that "bulk, unselected metadata presents too high a risk to share with second parties at this time, because of the requirement to ensure that the identities of Canadians or persons in Canada are minimized, but re-evaluation of this stance is ongoing."[168]

An example of the collection of this kind of data can be seen in the following example reworked from *A Primer on Metadata* created by the former Information and Privacy Commissioner of Ontario, Ann Cavoukian.[169] Someone makes a telephone call from a primary school to an individual in a corporate area. Immediately, the individual's location via cell phone towers can be traced to have left that area and then subsequently traced to the primary school. From there, the person's cell-phone was traced to a local walk-in clinic. One week later, the same person was located at a specialist's office, and then back to the same primary school. From the data gathered here, it is easy to deduce that the person has a child between the ages of four and thirteen and that the child is sick. While this does not seem like the most intrusive collection of information, the more sensitive this information is, the more damage it could potentially do.[170]

The risks posed by the collection of this sensitive information are connected to the vulnerability of the individual in question, and in many cases privilege comes strikingly into play. Its importance can be noted in the earlier mentioned Ashley Madison case, and can specifically be seen in regards to the LGBTQ2+ community. The invasion of your web search history can be particularly troubling if recent searches are similar to "how to come out to your family", "birth control morning after pill," "divorce lawyers in London, Ontario."[171] The more privileged an individual is, the less they need to worry about a hack to your private data.

In the post 9/11 world, there has been a stark shift from a post-crime to a pre-crime society. The previous post-crime society and the old penology of crime focused on finding the individual responsible for the crime and ensuring that appropriate punishment was meted out to the guilty party. No longer is our society satisfied with the simple punishment of a crime, but there is now a need to prevent crime from happening in the first place. This shift has two main trends: the first is "a more proactive, predictive, and pre-crime methods" and the second is the creation of more "surveillance technologies and more specifically, databases and profiling/data mining methods becoming more and more ubiquitous in policing practices."[172]

The creation of cloud networks has allowed for greater interconnectivity, at every level of access. In terms of government networks, the use of the cloud is incredibly efficient for sharing data, logistics, and software. While proponents of the cloud argue that this allows for a more democratic governmental network, namely that perhaps this will allow for greater transparency from citizen to government work, cloud networks quickly come under fire for issues of data sovereignty.[173] This is heightened by pre-crime society, where a significant part of policing has become the gathering and storage of intelligence that could potentially be useful later.[174]

Due to the increase of cloud networks at the governmental level, it is easy for different departments within the government to share information. This development has had many positive impacts on everything from healthcare provision to law enforcement. When children go missing and Amber Alerts are issued, the relaying of this data to members of the populace is faster than ever before, as seen in the recent tragic case of Riya Rajkumar. While some are quick to complain about being woken up in the middle of the night, these alerts are generally effective.[175] However, this sharing of private data over multiple levels of government also has less positive implications, such as the increased ease with which different departments are able to gather individual data without their knowledge or consent.[176] For example, areas of the Canadian government can access your Canadian Revenue Agency (CRA) account without a warrant and without notification.[177] This is all due to the crime prevention society in which we live, as the idea is that the government must do their best to maximize the security of all, even if that means infringing on the security of the few. However, we are learning that the few may not necessarily be just a few anymore when it comes to whom the government is collecting intelligence on.

The Canadian Security Intelligence Service (CSIS) was subjected to scrutiny in 2017 when a judge ruled that CSIS had been storing information that was legally collected under warrant “long after it had decided the information was not related to a security threat.”[178] The collection of metadata by CSIS is done in the Operational Data Analysis Centre (ODAC), which both collects and stores the metadata. More concerning is that they were not fulfilling their “duty of candor” which maintains that CSIS must be upfront with the Federal Court about the purpose of its information-seeking warrants.[179] On top of this, CSIS is not required to inform citizens when they are obtaining information from the Canada Revenue Agency. It is through the expansion of Bill C-51 that CSIS has obtained more information from other government agencies.

Recommendations

3.1 Development of Stricter Legal Frameworks for the Protection of Individual Data

Actors: Governments, Corporate
Type of Recommendation: Legal
Main Cyber Issues Involved: Privacy, Big Data, Personal Data, Data Collection, Surveillance, Ownership/Control of Resources, Storage and Communication of Data, Pace of Technological, Change, Hacking, Social Dependence
Main IR Issues Involved: Governance, Human Rights, Reach of International Law, Extra-territoriality, Cooperation, Crime, Legitimacy

Explanation We recommend that states pursue stricter protections for the rights of the individual regarding online privacy and their rights regarding the collection, transfer and control over their own individual data. This should be at both the national and international level, and could include:

- **A.** Establishing firm legal definitions for types of online services, such as social media platforms, and mobile applications to better clarify the rights of the individual for both corporations and individual users.
- **B.** Implementing basic legal rights to individual data privacy and control, such as the adoption of an erasure right like the GDPR 'right to be forgotten,' the legal requirement for more direct and transparent communication of data collection permissions.[180]
- **C.** The Establishment of legal restrictions on Opt-Out data processing consent models, instead implementing and Opt-In system and prohibiting making access to services contingent on the provision of consent.
- **D.** The Updating of Pre-Cyber legal principles to address cyber technologies, with an emphasis, for example, on the sale of individual data, the clandestine tracking of individuals, and the recording information through speakers and software that are supposedly "off," without consent, as well as to set precedent for their application regarding cyber issues.

Challenges: Most social media platforms gain a significant portion of their revenue from advertising and data sales, and thus limitations to data collection would result in a loss of revenue. This will likely result in any legal restrictions regarding the collection and sale of data facing resistance from corporations that engage in the newly regulated practices. Similar regulations to those proposed can currently be found worldwide; the EU's GDPR is a prime example, which requires corporations inform their users within 72 hours of a breach of their personal information, [181] or they could face fines up to 2% of its global revenue.[182] However, this is not to say that this revenue completely disappear. Even under the new GDPR policies, social media corporations are still thriving in Europe, because people do consent to the sale of their personal data and opt to remain a part of this process. In one prominent example, Facebook started implementing the outlined GDPR globally in mid-2018;[183] however, this is definitely not a feature that many users are aware of. Facebook needs to increase this apparent transparency feature and other sites should follow suit.

Justification: By implementing national regulations regarding the rights of the individual and their data online, the protection of individuals from corporations or institutions can at best be controlled. By entrenching these protections at the national level, the rights of the individual can be officially protected by national laws. This will allow each national government to ensure the rights of its own citizens are protected, while building towards a national understanding of the important role played by these rights.

3.2 Common Standards, Legal Minimum Requirements and Best Practices for Corporate Actors

Actors: Governments, Private Enterprise, Banks, Consumers
Type of Recommendation: Legal, Normative

Main Cyber Issues Involved: Privacy, Big Data, Personal Data, Anonymity, Data Collection, Trust/Mistrust, Espionage, Hacking, Commodification of Information, Social Dependence Innovation, Security Threat, Storage and Communication of Data
Main IR Issues Involved: Leadership, Cooperation, Legitimacy, Human Rights, Governance, Crime, Securitization

Explanation: We recommend that universal standards for the protection of individual's data are created for companies that collect and store personal data. This could include:

A. Maintaining adequate firewalls or security measures evaluated as sustainable and reasonable by industry experts

B. Regulated timelines and methods of information release in the event of a breach, specifying what notice must be given to affected clients.

C. Comprehensive response protocols, for both automated breaches and for targeted hacks

D. The establishment of legal options for recourse when individuals feel a company has not adequately protected their data.

Challenges: Corporate backlash will present a significant challenge in creating minimum requirements. Additionally, acquiring the trust from consumers will be a difficult but necessary step in upholding standards. Finally, popular support for legal recourse will be required to begin to develop the necessary procedures.

Justification: The creation of standardized regulations will foster greater accountability in corporate actors and build better avenues for recourse for individual users when their rights are violated.

3.3 Educational Campaigns for Individual Users, Highlighting the Risks of Online Activities and How to Protect Individual Privacy

Actors: Consumers, Citizens, Governments, Non-State Actors, Civil Society
Type of Recommendation: Normative
Main Cyber Issues Involved: Privacy, Personal Data, Data Collection, Ownership/Control of Resources, Trust/Mistrust, Commodification of Information, Access, Hacking, Big Data
Main IR Issues Involved: Leadership, Cooperation, Human Rights, Development

Explanation: We recommend the creation of education campaigns for individual users online, to educate the general population on the specific risks posed to their privacy and rights online by criminals, states and corporations. The focus of these campaigns would be to highlight potential risks to individual security, and to inform the individual both of which actions they can take to better protect themselves, as well as what to expect from their governments regarding individual protections. In addition to the general public, these campaigns could target vulnerable groups specifically, such as children interacting with the internet for the first time, or elderly individuals with less experience and understanding of recent technological developments.[184]

Challenges: Some of the most vulnerable groups in the cyber realm are the older and younger populations, who are unaware of the potential risks nor the strategies to identify and protect their data from misuse. However, implementing educational campaigns may fail to reach these populations unless implemented in a large scale and uniform manner. Furthermore, these campaigns will require constant funding and regular review to ensure that their information and data is up to date and not misleading. This can best be approached by considering possible audiences for the campaign closely, and creating a consistent curriculum that can be updated as necessary.

Justification: While there currently are regulations and protections designed to help individuals assert their privacy rights, the unfortunate reality is that these protections are often either ignored or circumvented by corporations. By working to improve the cyber literacy of online users and educate them, these vulnerable users can be protected from misuses of their individual data. While increased cyber literacy is ideal for society as a whole when considering how to protect individual privacy and data rights, by first targeting those groups, those at the greatest risk can be helped.

[113] *Internet Usage Worldwide,* report no. Did-12322-1, Statista, 2018, Accessed March 4, 2019, 10-13.

[114] Jangirala Srinivas, Ashok Kumar Das, and Neeraj Kumar, "Government Regulations in Cyber Security: Framework, Standards and Recommendations," *Future Generation Computer Systems* 92 (2019): 179-180.

[115] Lillian Ablon, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, RAND Corporation (2016): 1-3.

[116] Giuseppe Colangelo and Mariateresa Maggiolino, “Data Accumulation and the Privacy–Antitrust Interface: Insights from the Facebook Case,” *International Data Privacy Law* 8, no. 3 (2018): 224-225.

[117] General Data Protection Regulation (GDPR). (2018). *General Data Protection Regulation (GDPR),* Article 4.

[118] Sasha Romanosky, Rahul Telang, and Alessandro Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?," *Journal of Policy Analysis and Management* 30, no. 2 (2011): 256-357.

[119] General Data Protection Regulation (GDPR). *General Data Protection Regulation (GDPR),* (2018): Article 4, Accessed at https://gdpr-info.eu/.

[120] General Data Protection Regulation (GDPR). *General Data Protection Regulation (GDPR),* (2018): Article 4, Accessed at https://gdpr-info.eu/.

[121] Reza Mahbod, Rob Irish and Mike Fredrickson, “A Guide to Cybersecurity,” *The Journal of Government Financial Management* 66, no. 3 (2017): 35. https://www-lib-uwo-ca.proxy1.lib.uwo.ca/cgi-bin/ezpauthn.cgi?

[122] Orla Lynskey, “At the Crossroads of Data Protection and Competition Law: Time to Take Stock,” *International Data Privacy Law* 8, no. 3 (2018): 179–180

[123] Orla Lynskey, “At the Crossroads of Data Protection and Competition Law: Time to Take Stock,” *International Data Privacy Law* 8, no. 3 (2018): 179–180

[124] Taylor Armerding, "The 18 biggest data breaches of the 21st century," *CSO Online*, (December 2018).

[125] Taylor Armerding, "The 18 biggest data breaches of the 21st century," *CSO Online*, (December 2018).

[126] Taylor Armerding, "The 18 biggest data breaches of the 21st century," *CSO Online*, (December 2018).

[127] Steve Mansfield-Devine, "The Ashley Madison Affair," *Network Security*, (September 2015): 9.

[128] Steve Mansfield-Devine, "The Ashley Madison Affair," *Network Security*, (September 2015): 9.

[129] Steve Mansfield-Devine, "The Ashley Madison Affair," *Network Security*, (September 2015): 13.

[130] Steve Mansfield-Devine, "The Ashley Madison Affair," *Network Security*, (September 2015): 13.

[131] James Bradshaw, "BMO, CIBC’s Simplii Face Fallout from Data Breaches," *The Globe and Mail*, May 29, 2018.

[132] James Bradshaw, "BMO, CIBC’s Simplii Face Fallout from Data Breaches," *The Globe and Mail*, May 29, 2018.

[133]Lillian Ablon, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, RAND Corporation (2016): 39.

[134] Lillian Ablon, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, RAND Corporation (2016): 41.

[135]Asunción Esteve, “The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA,” *International Data Privacy Law* 7, no. 1 (2017): 36-37.

[136] Asunción Esteve, “The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA,” *International Data Privacy Law* 7, no. 1 (2017): 36-37.

[137] Asunción Esteve, “The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA,” *International Data Privacy Law* 7, no. 1 (2017): 38.

[138] Asunción Esteve, “The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA,” *International Data Privacy Law* 7, no. 1 (2017): 39.

[139] Asunción Esteve, “The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA,” *International Data Privacy Law* 7, no. 1 (2017): 40.

[140] Asunción Esteve, “The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA,” *International Data Privacy Law* 7, no. 1 (2017): 39.

[141] Asunción Esteve, “The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA,” *International Data Privacy Law* 7, no. 1 (2017): 39.

[142] Asunción Esteve, “The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA,” *International Data Privacy Law* 7, no. 1 (2017): 38.

[143] Asunción Esteve, “The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA,” *International Data Privacy Law* 7, no. 1 (2017): 39.

[144] Christopher Mims, “Who Has More of Your Personal Data Than Facebook? Try Google; Google Gathers More Personal Data than Facebook Does, by Almost Every Measure--so Why Aren’t We Talking about It?,” *WSJ Pro. Cyber Security*, (2018): 1.

[145] Asunción Esteve, “The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA,” *International Data Privacy Law* 7, no. 1 (2017): 39.

[146] Mark A. Gregory, David Glance, *Security and the Networked Society*, (Cham: Springer International Publishing, 2013): 237.
[147] Asunción Esteve, "The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA," *International Data Privacy Law* 7, no. 1 (2017): 36.
[148] Kellyton dos Santos Brito et al., "How People Care about Their Personal Data Released on Social Media," *2013 Eleventh Annual Conference on Privacy, Security and Trust* (IEEE, 2013), 111.
[149] Kathrin Knautz and Baran S. Katsiaryna, "*Facets of Facebook: Use and Users*," (Berlin and Boston: De Gruyter, 2016), 152-153.
[150] Stephen L. Baglione et al., "Factors Affecting Facebook Advertisements: Empirical Study," *International Journal of Business, Marketing, and Decision Sciences (IJBMDS)* 11, no. 1 (2018): 124.
[151] Asunción Esteve, "The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA," *International Data Privacy Law* 7, no. 1 (2017): 36-7, 39-40.
[152] Stephen L. Baglione et al., "Factors Affecting Facebook Advertisements: Empirical Study," *International Journal of Business, Marketing, and Decision Sciences (IJBMDS)* 11, no. 1 (2018): 124.
[153] Newton Lee. *Facebook Nation: Total Information Awareness*, 2nded. New York, NY:
Springer Science + Business Media, 2013, 100.
[154] Christopher Mims, "Who Has More of Your Personal Data Than Facebook? Try Google; Google Gathers More Personal Data than Facebook Does, by Almost Every Measure--so Why Aren't We Talking about It?" *WSJ Pro. Cyber Security*, (2018): 1.
[155] Asunción Esteve, "The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA," *International Data Privacy Law* 7, no. 1 (2017): 40.
[156] Asunción Esteve, "The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA," *International Data Privacy Law* 7, no. 1 (2017): 43.
[157] Brito et al., "How People Care about Their Personal Data Released on Social Media," 111.
[158] Asunción Esteve, "The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA," *International Data Privacy Law* 7, no. 1 (2017): 43.
[159] Christopher Mims, "Who Has More of Your Personal Data Than Facebook? Try Google; Google Gathers More Personal Data than Facebook Does, by Almost Every Measure--so Why Aren't We Talking about It?" *WSJ Pro. Cyber Security*, (2018): 2.
[160] Christopher Mims, "Who Has More of Your Personal Data Than Facebook? Try Google; Google Gathers More Personal Data than Facebook Does, by Almost Every Measure--so Why Aren't We Talking about It?" *WSJ Pro. Cyber Security*, (2018): 2.
[161] Asunción Esteve, "The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA," *International Data Privacy Law* 7, no. 1 (2017): 43.
[162] "Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31," *Ontario.ca,* https://www.ontario.ca/laws/statute/90f31#BK0
[163] The National Defence Act, Rsc 1985, C N-5, s. 273.64 can be found in Michael Geist, "Why Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era," in *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, ed. by Michael Geist. Ottawa: University of Ottawa Press, 2015.
[164] Michael Geist, "Why Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era." In Law, Privacy and Surveillance in Canada in the Post-Snowden Era. *University of Ottawa Press* (2015): 225-256, http://www.jstor.org/stable/j.ctt15nmj3c.12.227.
[165] Mitch Potter and Michelle Shephard, "Canada's Electronic Watchers Enjoy Secrecy Second to None," *Toronto Star*, November 9, 2013.
[166] Michael Geist, "Why Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era." In Law, Privacy and Surveillance in Canada in the Post-Snowden Era. *University of Ottawa Press* (2015): 230. http://www.jstor.org/stable/j.ctt15nmj3c.12.227.
[167] Ron Deibert, "Spy Agencies Have Turned Our Digital Lives Inside Out. We Need to Watch Them," *Globe and Mail*, June 10, 2013.
[168] Bill Robinson, "Metadata and Second Parties," *Lux Ex Umbra: Monitoring Canadian Signals Intelligence (SIGNIT) Activities Past and Present*. December 2, 2013. https://luxexumbra.blogspot.com/2013/12/metadata-and-second-parties.html.
[169] Ann Cavoukian, Canadian Electronic Library (Online service), and Information and Privacy Commissioner/Ontario. *A Primer on Metadata: Separating Fact from Fiction.* Toronto, Ontario: Information and Privacy Commissioner/Ontario, 2013.
[170] Nathan Freed Wessler, "How Private Is Your Online Search History?" American Civil Liberties Union, April 26, 2015, accessed March 08, 2019, https://www.aclu.org/blog/national-security/privacy-and-surveillance/how-private-your-online-search-history.
[171]Nathan Freed Wessler, "How Private Is Your Online Search History?" American Civil Liberties Union, April 26, 2015, accessed March 08, 2019, https://www.aclu.org/blog/national-security/privacy-and-surveillance/how-private-your-online-search-history.
[172] Rosamunde van Brakel and Paul De Hert, "Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies." *Journal of Police Studies* (2011): 165.

[173] Kristina Irion, "Government Cloud Computing and the Policies of Data Sovereignty," *International Telecommunications Society* (2011): 9.

[174] Kristina Irion, "Government Cloud Computing and the Policies of Data Sovereignty," *International Telecommunications Society* (2011): 9.

[175] Shane Gibson, "Amber Alert for Missing Ontario Girl Leads to Influx of Calls to Winnipeg 911," *CBC News*, February 15, 2019.

[176] Kristina Irion, "Government Cloud Computing and the Policies of Data Sovereignty," *International Telecommunications Society* (2011): 12.

[177] John Paul Tasker, "What You Need to Know about the CSIS Metadata Ruling," *CBC News*. November 5, 2016.

[178] John Paul Tasker, "What You Need to Know about the CSIS Metadata Ruling," *CBC News*. November 5, 2016.

[179] John Paul Tasker, "What You Need to Know about the CSIS Metadata Ruling," *CBC News*. November 5, 2016.

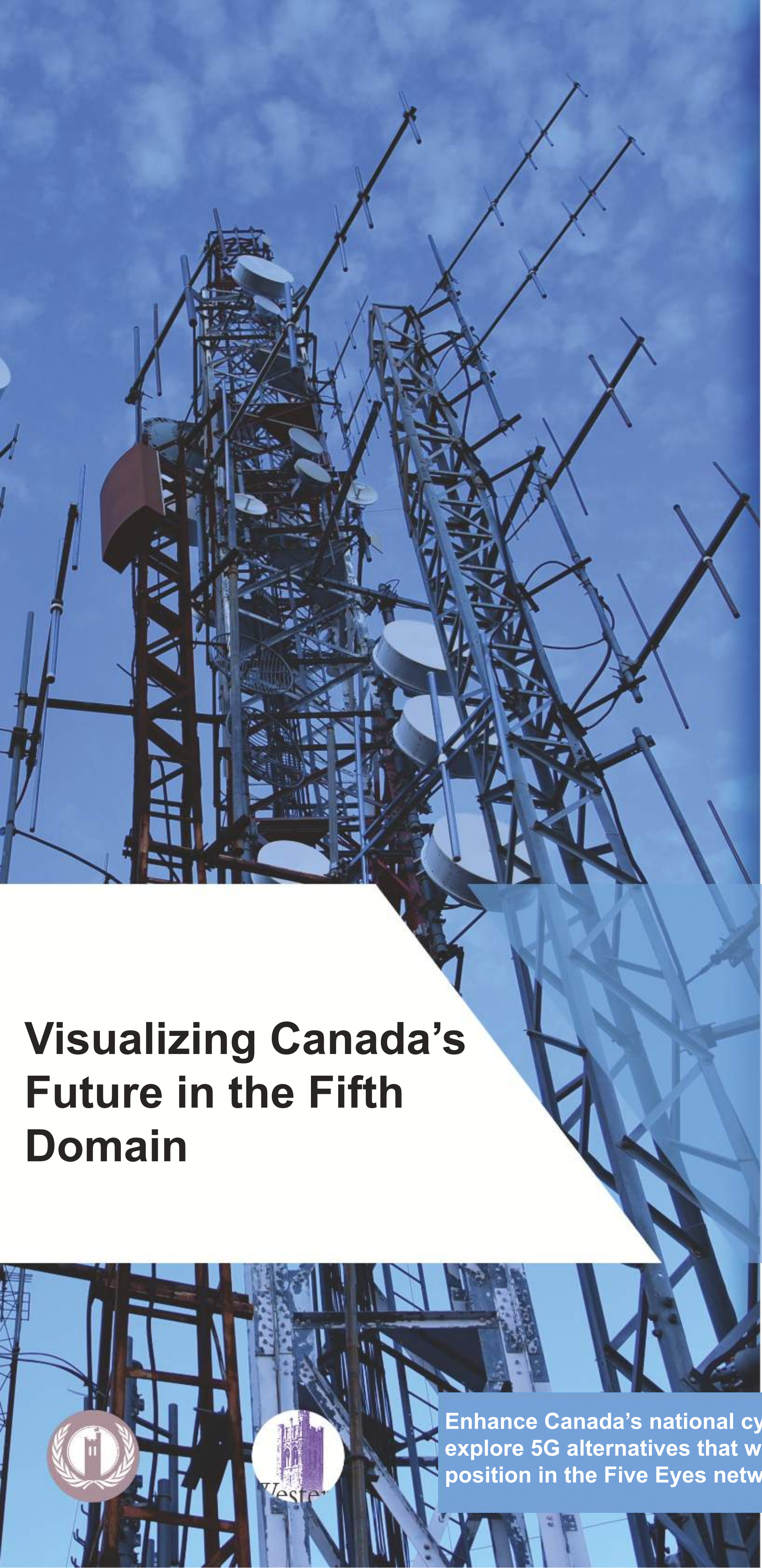
[180] General Data Protection Regulation (GDPR). *General Data Protection Regulation (GDPR)*, 2018, Article 17. Accessed at https://gdpr-info.eu/.

[181] "GDPR Key Changes," Key Changes with the General Data Protection Regulation – EU GDPR, Accessed March 20, 2019, https://eugdpr.org/the-regulation/.

[182] Susan Akbarpour, "How Does GDPR Impact Advertising And E-Commerce?" *Forbes,* May 08, 2018, Accessed March 20, 2019, https://www.forbes.com/sites/forbesagencycouncil/2018/05/08/how-does-gdpr-impact-advertising-and-e-commerce/#b46f58e32776.

[184] Brandon E. Gavett, Rui Zhao, Samantha E. John, Cara A. Bussell, Jennifer R. Roberts, and Chuan Yue. "Phishing Suspiciousness in Older and Younger Adults: The Role of Executive Functioning." *PloS One* 12, no. 2 (2017): 3.

5G



Visualizing Canada’s Future in the Fifth Domain

Enhance Canada’s national cybersecurity capabilities, and explore 5G alternatives that will help Canada maintain its position in the Five Eyes network and as a US ally.

5G Network

Infrastructure Development & Security Concerns

Background

Fifth Generation (5G) networking is a new wave of networking technology that is set to improve upon the Multiple-Input and Multiple-Output (MIMO) technology of 4G LTE networks that are currently widespread throughout most countries. Very recent advances in multimedia applications and cloud computing have necessitated advancements in networking technology, and more specifically, how different devices interact with a network. From 2016-2018 the global mobile network traffic grew from 2.6 exabytes of data to 15.8 exabytes of data (or about 15.8 billion gigabytes).[185] Addressing this huge year-on-year increase in mobile network access has underscored the need to further evolve cellular networks. New 5G technology seeks to ameliorate this exact issue by enabling 100 times faster internet speeds, 100 times the amount of users connected, decreased latency by a factor of 5, and 10 times more efficient power draw for devices operating on this network.[186] To put this into perspective, a 2 gigabyte movie downloaded on an older 3G network would take 26 hours, while the same video would take around 4 minutes to download on 4G LTE networks. On 5G networks, this same movie could be downloaded as fast as 3 seconds. This sort of speed, ease of access, and low latency would allow for new technologies like cloud computing, driverless cars, and eHealth services to run much more efficiently.[187] 5G technology greatly expands the internet of things and will enable consumer and commercial devices to be connected in a way that was not possible on a 4G network.

Infrastructure Development

In contrast to current wireless communication systems, 5G will significantly improve the energy consumption, cost, and resource-efficiency of a nation, which could further develop the system capacity with regards to affordability and energy consumption.[188] In general, the 5G network promises greater speed, which translates to faster communication and the potential of increased infrastructure development.[189] However, Canada and its allies face a challenge posed by China which presents a unique geopolitical dilemma. This dilemma places Canada between two global giants; China and the United States. China's Huawei has established contemporary research programs to develop alternatives to American suppliers, in an accelerated effort to develop its own 5G technology. 5G is intended to open up the potential of interconnected devices: self-driving cars, remote surgeries, and streaming virtual reality.

However, if hypothetically, relations between the two countries were to deteriorate, then Beijing could conceivably decide it wants access to any of that vital data spanning across Canada's 5G networks via Huawei. This would lead to a major concern of Chinese influence with its control over devices connected to the 5G network in Canada: interrupting critical infrastructure services.[190] If 5G is to play an instrumental role in infrastructure development and the Internet of Things, that development could be held hostage to the priorities of Chinese companies.[191] Though lucrative, noting this East versus West dichotomy, Canada should abstain from aligning their efforts with China, primarily due to the increased risk of alienation from the US and its other allies. This report will focus on two potential areas of risk in infrastructure development if Canada's 5G networks are developed under Huawei; water filtration and self-driving cars.

If China is granted access via Huawei, on the one hand there could be positive benefits for infrastructure development in Canada, on the other it could lead way to heightened risks with deadly consequences for Canadian water supplies. Insofar that Canada would be left vulnerable to the risk of compromised water filtration systems. Currently, many Canadian water filtration systems work on computers.[192] These computers are tasked with administering a specific amount of chlorine to destroy bacteria, fluoride for dental health, and other additives to keep the water potable.[193] If these chemicals are not administered appropriately, significant health risks may occur thereby impacting Canadian citizens. This includes water poisoning which could, in the worst cases, lead to death. This opens the possibility for China to essentially eradicate an entire population in targeted attack. In virtue of weaponizing water, an attack of this nature could be considered biological warfare and is thus a violation of international law under the 1975 Biological Weapons Convention. Allowing another state to possess this potential is a huge national security threat for the Canadian government.

Self-driving cars seem to be the natural direction in contemporary technological advancement and when they become the norm on the roads, a risk of traffic disruption could also present a security concern for Ottawa.[194] If international tension was to increase, the Chinese government could disrupt traffic patterns across all major cities.[195] There would be the possibility to pinpoint a location and interrupt the flow of data that makes autonomous vehicles drive safely in traffic. These self-driving cars could be made to crash into other vehicles or nearby buildings without the drivers control of consent, thus risking the life of the driver or a potentially damage of property.

Additionally, traffic lights could be manipulated to change abruptly, sparking further concerns about the potential for accidents. However, this does not necessarily suggest that all 5G infrastructure development is detrimental, as in the case of traffic and self-driving cars, the flow of traffic could improve with help of smart traffic management systems on a 5G network. Traffic signals would be able to change based on the current, real-time traffic patterns, which would be monitored by sensors and cameras.[196] This has already taken place in major cities through Internet of things (IoT) initiatives in order to increase traffic flow.[197] For example, in Kansas City, USA, sensors on street lights along a 3.54 kilometer rail line in March 2016 and Carnegie Mellon University's recent test of smart traffic lights in the city of Pittsburgh led to a 26.0 percent faster commute, and a 40.0 percent reduction in vehicle wait time, and a 21.0 percent decrease in vehicle emissions.[198] These practices could also have a profound impact for companies like Lyft and Uber.[199] Transport companies could save money on gas, and with an increased flow of traffic and a reduction in vehicle wait time, drivers could automatically increase their number of pickups. If vehicle-to-vehicle (V2V) communication technology can be deployed over a 5G network, potentially increasing in how closely cars could travel next to each other in a practice also known as platooning, which could lead to an increase in highway capacity and decreased commute times.[200] Using this technology would provide Canada with a greener alternative to traditional cars, with economic incentives for both states and private companies.

While the aforementioned risks are not unique to an alliance with China, they are amplified due to the constitutional limitation for Chinese companies such as Huawei.[201] If Canada is seeking to develop its own 5G network, the best course of action would be to focus on preserving its ally-ship with US and other countries seeking to develop 5G.

Balancing Geostrategy and Security Risks in 5G Development

Canada's approach to 5G technology development must take into account geopolitical considerations, and a balance of security, allies, and national interest. It is paramount that Canadian 5G technology development adopts a strategy which balances the risks of the technologies themselves, as well as the geopolitical implications associated with adopting them. 5G leadership will provide the foundation for technological innovations that will drive military capability and economic growth. Yet, it has far reaching implications because 5G network development represents both an economic and security contest. 5G competition is emerging as part of geopolitical competition for influence and power based on different options of national approaches to investment and innovation. The pursuit of 5G technology development in Canada requires that the government not focus solely on the technology itself, but what it signifies for geopolitics in the changing liberal world order.

There are currently four companies dominating the market for technologies needed for 5G networking: two European (Ericsson and Nokia) and two Chinese (Huawei and ZTE).[202] Canada's choice between these four companies in implementing its 5G network nationally will affect security and innovation in an increasingly competitive technological environment. It is important that the decision adopted by the Canadian government regarding 5G technologies maintains alliances and considers the positives of each company's technology while protecting against any security threats they may pose.

Chinese 5G companies Huawei and ZTE have acquired first-mover status in developing and proliferating 5G technology. This may result in geopolitical advantage by expanding its technological sphere of influence in Africa, Latin America, and the Middle East, where the Belt and Road Initiative has already provided strong incentives for governments to adopt the cheaper and more readily available Chinese technologies.[203] Expanding Chinese influence through 5G technology poses a security dilemma to the United States, which views China as a direct competitor and security threat. In America's assessment, China would theoretically be able to force its companies to install network backdoors which will allow it unfettered access to other countries' 5G networks, giving it enhanced espionage capabilities.[204] Limiting this expansion of influence will require similar effort by Western powers to promote 5G network creation by companies in the US and Europe. It is unlikely given the current technological infrastructure that Canada will be able to exert influence through expanding its own 5G technology, and rather, should align with allied efforts to counter Chinese influence in this new realm of geostrategic space.

Canada's Western allies have expressed growing concern with investing in Chinese 5G technology, in favour of a policy which excludes Chinese technologies, based on the grounds that Huawei and ZTE corporations pose threats due to the regulations required by the Chinese government. In August 2018, the Australian government formally banned Huawei and ZTE equipment for the country's 5G networks. In the EU, Jeremy Fleming, the director of the Government Communications Headquarters (GCHQ), singled out China as a significant threat for security of those countries who adopt Chinese 5G technology, advocating that security must be considered into new technologies, especially for protecting personal information.[205] European heads of state have been questioning the reliability of Chinese companies such as Huawei and

ZTE to build 5G networks, because backdoors could theoretically give China access to critical infrastructure that will soon be relying on 5G technology, such as water supply, road safety, and entire industries. World leaders have been calling for stricter security requirements for companies that will supply critical infrastructure backed by 5G, yet there has been no global consensus or even consensus among Western allies on this issue.[206]

However, the current approach by many Western states to prevent the spread of Chinese 5G technology is not tenable. It is not clear whether a coalition of non-Chinese infrastructure vendors could be assembled to provide the full spectrum of 5G infrastructure equipment in a cost-effective and timely manner.[207] Geostrategic challenges posed by Chinese 5G technology in Canada include deciding between the security threats that Huawei poses or damaging Chinese-Canadian relations by banning Huawei. China's ambassador to Canada, Lu Shaye, has warned of "repercussions" if Canada follows through with banning Huawei from participating in building Canada's 5G network.[208] Public Safety and Emergency Preparedness Minister Ralph Goodale is overseeing Canada's review of the security challenges and potential threats in Canada's future use 5G technology. Goodale must prioritize long and short term national interests while balancing the geostrategic elements of 5G network expansion.

5G networks promise internet speeds which can support futuristic technology that will revolutionize cyberspace. One of the leaders in developing 5G is the Chinese company, Huawei, which has been banned in New Zealand, Australia, Germany, and the United States.[209] The concern with Huawei is a result of the Chinese National Intelligence Law, which allows for the Chinese government to access information through private tech companies.[210] The United States has been the most outspoken about this law, and is a leading voice in publicizing the close links between the company and Chinese government.[211] Specifically, there are three articles of primary concern listed in the revised National Security Laws. Firstly, Article 7 clearly states that if the Chinese government claims the need to access data from a private entity, they can do so as they please, at any given time.[212] This article is a concern for Canadian privacy, and is also the primary reason why the other member-states of Five Eyes have banned Huawei outright. Secondly, Article 14 grants Chinese intelligence agencies authority when engaging in operations, granting them the ability to demand cooperation from businesses and organization.[213] Finally, Article 16 outlines that intelligence agencies are granted entrance to restricted areas, and may read or collect relevant files, items, or materials as they see fit.[214] This constitutional arrangement makes it possible for the Chinese government to access information as it pleases, which should be concerning to Canada when deciding whether to use Huawei for the 5G server. The statements of reassurance by Huawei chiefs are insubstantial as it is beyond their control whether the Chinese government will access the private information of Canadians.[215] The banning of Huawei in a majority of the 'Five Eyes' nations is a result of these articles, and in fear of the Chinese government utilizing Huawei to gather intel from the respected nations.[216]

Protectionism justified national security is ever-present and is branching into cyber security, but has the ability to strongly undermine liberal commitments to trade.[217] This extension into cyberspace is in response to the longstanding history, and fear of Chinese espionage. This is one of the major concerns that led the majority of the 'Five Eyes' deciding to ban Huawei outright in the country. The struggle created for Canada specifically is a direct impact of US influence.[218] However, the United Kingdom has reported that it has been monitoring Huawei's activity and indicated that it could only provide 'limited assurance' that national security risks from the company had been 'sufficiently mitigated.'[219] The United Kingdom is one of the remaining members of Five Eyes still to decide its final position on the adoption of Huawei's 5G technology. Since they have provided only limited assurances of being able to mitigate security concerns, it is vital to take precautions against possible tampering from the Chinese government. In reality, the individuals at higher risk of being victims of espionage are the ones involved in research, military, business competition, or the government.[220]

The United States' Department of Homeland Security has criticized Chinese companies for intellectual property theft, and with the increased strength of the new data processing technology it had led to 'industrial scale' espionage.[221] Nations including Australia, Canada, Germany, India, Taiwan and the UK have accused China of intrusion of public and private industries, highlighting that China has been identified as the most persistent cyber espionage actor internationally.[222] China allegedly prefers to leverage the benefit of cyber intrusions during peacetime as a means of data and information collection to gain commercial advantage.[223]

Scenarios and Recommendations

Canada is lagging behind major countries like China and the United States for 5G network implementation. United States wireless providers like AT&T and Verizon are expected to begin implementing 5G networks in select cities beginning at the end of 2019, making the United States the second country to begin rolling out 5G networks after China. Meanwhile, Canada's Big Three telecom companies have not yet offered information on their plans for a 5G rollout.[224] Bell Canada has been testing 5G technologies since 2015 in a partnership with Huawei. However, this partnership has caused some issues for the Canadian government vis-à-vis the US. The concern from US officials is that Huawei may use their technologies installed worldwide to provide information to the Chinese government thanks to an article in the Chinese Constitution that requires all Chinese companies to share data with the government.[225] This could essentially be a tool for the Chinese government to spy on Canadian corporate or government information, or even be able to have control over Canadian systems that would run on new 5G networks. However, Canadian cybersecurity experts have said that Huawei is not a threat given Canada's current safeguards, putting Canada in an awkward position.[226] US securitization of the issue is not unfounded as the US has historically been subject to Chinese industrial espionage through hacking, which has amounted to a $300 billion loss per year for US companies.[227] Senator Warner was unsure what the consequences would be if Canada did end up adopting Huawei's technologies, but he did say that there would have to be some degree of "untangling" of US and Canadian telecom networks which would greatly affect Canadians' access to internet as Canada relies heavily on US networks.[228] Furthermore, new technologies like driverless cars that would require integrated telecom networks in the future would not work as efficiently on separate 5G networks.

The Canadian government should look at 5G implementation in conjunction with Huawei in a cost-benefit analysis. Canada's relationship with China has been strained due to the Huawei CEO extradition case. However, despite US pressures, the Canadian government cannot simply back out of a 5G implementation deal with Huawei without some backlash. An agreement signed in 2012 by the Harper government called the Canada-China Agreement for the Promotion and Reciprocal Protection of

Investments could give China the legal right to sue the Government of Canada if it excludes Huawei for national security reasons.[229] This could potentially be very costly for the Canadian government and might explain why a decision to exclude Huawei is not an easy decision. Conversely, the Trump Administration has repeatedly threatened to remove Canada from the Five Eyes Alliance if it adopts Huawei's technologies, among other issues (like decoupling American and Canadian telecom infrastructure).[230] This would greatly harm Canada's special relationship with the US which could bleed over into other areas like trade and military cooperation in the worst cases.

Despite all this, recent developments in Britain have given Canada a bit more breathing room on the issues as it is likely that Britain will implement a 5G network using Huawei's technology. If Britain moves forward with these plans, it will set the precedent for Canada to do the same since Britain will most likely not be ousted from the Five Eyes Alliance given its importance. Each of these factors must be taken into account when making a decision. However, it is clear that Canada's past decisions have been short sighted and have now put the government in an awkward position to deal with this issue. Given the circumstances, there are three different realistic scenarios that depend on what the British government decides in the near future: Britain does not adopt Huawei's 5G technology and no precedent is set, Britain adopts Huawei's 5G technology but is subsequently removed from participation in the Five Eyes Alliance, and finally, Britain adopts Huawei's 5G technology and is able to remain in the Five Eyes intelligence network.

Scenario 1: Britain does not Adopt Huawei's 5G Technology

Although this does not currently look likely, if the British Parliament votes in favour of banning Huawei from its upcoming 5G network and opts to use Ericsson, Samsung, or Intel's solutions, then this would isolate Canada in the Five Eyes Alliance given that the other alliance partners would have banned Huawei's technology. In this scenario, we recommend that Canada ban Huawei's technology in favor of maintaining a stable relationship with its allies. Although banning Huawei from participating in Canada's 5G network may open Canada up to legal exposure from the Chinese government, and Huawei's technology is thought to be superior to those of the aforementioned companies, it would not be worth it for Canada to lose vital intelligence-sharing allies, and more critically, the trust of the US government as an ally. Further to this, there has been a bipartisan consensus in the US that if Canada adopts Huawei's 5G network, that network infrastructure between the two countries would have to be decoupled. This would have significant adverse effects on Canadian network infrastructure as a study conducted by the University of Toronto's Data Governance Department showed that around 75% of Canadian-to-Canadian communications online were routed through the United States, and a further 80% of Canadian-to-international online communication is routed through the United States.[231] Decoupling Canadian and American infrastructure at this juncture would significantly harm Canada's ability to communicate online across the country and internationally at significant cost to Canadian taxpayers.

4.1 Canada Should Ban Huawei Technology in Favour of Upholding Strong Relations with Five Eye Alliance.

Actors: Governments, Non state actors, Consumers, Citizens, Private enterprise, Civil society, Government of Canada, US, China, EU, OAS, etc
Type of Recommendation: Scenario-based
Main Cyber Issues Involved: Privacy, Surveillance/Data collection, Innovation, Commodification of Information, Pace of technological change, Social dependence (80%+ Cdns using internet actively), Security threat, Social division, Access, Ownership/control of resources, Trust/Mistrust, Governance, Espionage, Hacking, Protecting Individuals vs protecting internet, Big data, Personal data, Network infrastructure, Data storage
Main IR Issues Involved: Governance, Regionalism/Fragmentation, Sovereignty and State Power, Development, Human Rights, (Over) Securitization; electronic Pearl Harbor, Extra-territoriality, Reach of international law, Leadership, Cooperation

Explanation: Canada will be in a more restricted situation if Britain decides to ban Huawei as four of five Five Eye nations will have banned the tech company outright. As a result, Canada will have a challenging decision to make in terms of maintaining close allyship or adopting the 5G technology. Canada's situation will be restricted as the alliance is more important than gaining the tech from China.

Challenges: The challenges that become present with the decision to ban Huawei outright in Canada are significant in terms of the relationship between China and Canada. This ban will open Canada up to legal repercussions from China. (As mentioned, a deal signed by the Harper administration would put China in a legal position to sue Canada.) Another challenge Canada would face is that it would be longer until 5G would be able to come to Canada. Currently, Huawei is the leader in the development of the 5G network, and has the most advanced version to date.

Justification: It is not worth Canada risking partnership with the other members of the Five Eyes which would risk intelligence sharing between these nations as well as lose trust from the US. The US has reached bipartisan agreement that the two nations will have network infrastructure decoupled as a result of Canada adopting the Chinese technology. This decoupling would harm Canadian access to online communication internationally.

Scenario 2: Britain Adopts Huawei's 5G Technology and is Excluded from the Five Eyes Alliance

Scenario 2 is very similar to scenario 1; however, given Britain's history of ignoring US diplomatic pressure, it is likely that Britain will adopt Huawei's 5G technology. Both British and Canadian cybersecurity officials have made it clear that adopting Huawei's 5G technology would not pose a significant threat, but that measures would be put extra caution would be taken to ensure that there are no breaches in security. Despite this, if Britain adopts Huawei's 5G technology and is subsequently excluded from the Five Eyes network by the US, then Canada should not adopt Huawei's 5G technology. Allowing Britain to test

America’s seriousness about this issue first will give the Canadian government a strong indicator of the kinds of consequences that the US may impose if Huawei’s technology is adopted. If Britain is excluded from the Five Eyes network, Canada should not include Huawei in its 5G plans.

4.2 Canada Should not Adopt Huawei Technology

Actors: Governments, Non state actors, Consumers, Citizens, Private enterprise, Civil society, Government of Canada, US, China, EU, OAS,
Type of Recommendation: Scenario-based
Main Cyber Issues Involved: Privacy, Surveillance/Data collection, Commodification of Information, Social dependence (80%+ Canadians using the internet actively), Security threat, Social division, Access, Trust/Mistrust, Governance, Espionage, Hacking, Protecting Individuals vs protecting internet, Big data, Personal data, Storage and communication of data
Main IR Issues Involved: Governance, Regionalism/Fragmentation, Sovereignty and State Power, Development, Human Rights, Extra-territoriality, Reach of international law, Leadership, Cooperation

Explanation: While both British and Canadian tech specialists highlight that Huawei would not pose a significant threat, there need to be extra precautions taken by other nations to ensure increased security to mitigate potential breaches.

Challenges: This recommendation presents the challenge of waiting out the decision of Britain. Using them as a ‘tester’ will be beneficial, however, it would slow down the process of gaining 5G in Canada. If Britain were to adopt Huawei, and were excluded by the Five Eyes, Canada does not gain a flexible approach to the adoption. As there has been many statements highlighting the severing of relations by the US to Canada, it is not a guarantee that Canada would automatically remain a member of the Five Eyes.

Justification: If Britain is to adopt Huawei and is subsequently expelled from the Five Eyes alliance, it is not in Canada’s best interest to not adopt the tech as it would likely also be excluded. Canada should wait for Britain to test America’s patience to see the result of adopting Huawei tech, in order to properly assess the repercussions of adoption. In the case that Britain is excluded, Canada should not adopt Huawei technology.

Scenario 3: Britain Adopts Huawei’s 5G Technology and Remains in the Five Eyes Alliance

Given all the current parameters, this scenario is perhaps the most likely to occur of the three. The British Parliament is close to voting on including Huawei’s 5G technology despite US, Australia, and New Zealand’s concerns. Given that Britain is an integral part of the Five Eyes network, it would be unlikely that Britain would be excluded from the network by the US, although some political tensions may arise. While this scenario would certainly give the Canadian government room to maneuver, it must still be careful about including Huawei in its 5G network. While Canada may not be ousted from the Five Eyes network, there may still be network decoupling based on US security concerns which would be a major boon on Canadian connectivity. Because of this, we recommend that Canada communicate with the US to ensure that it can adopt Huawei's 5G technology without any reprisals given the precedent set by the British government. It is most important that Canada preserve its network connectivity with the US and its position in the Five Eyes network. Any decision that compromises these would be disastrous for the Canadian economy or security.

4.3 Canada has maneuverability in adopting Huawei, and should consult the US senate prior to adoption of tech to properly assess potential repercussions of the adoption.

Actors: Governments, Non state actors, Consumers, Citizens, Private enterprise, Civil society, Government of Canada, US, China, EU, OAS, etc
Type of Recommendation: Scenario-based
Main Cyber Issues Involved: Privacy, Surveillance/Data collection, Innovation, Commodification of Information, Security threat, Access, Ownership/control of resources, Trust/Mistrust, Governance, Espionage, Hacking, Protecting Individuals vs protecting internet, Big data, Personal data, Storage and communication of data
Main IR Issues Involved: Governance, Regionalism/Fragmentation, Sovereignty and State Power, Development, Human Rights, Extra-territoriality, Reach of international law, Leadership, Cooperation

Explanation: Given that Britain is a key member of the Five Eyes, it is unlikely that they would be ousted from the alliance. This would give Canada maneuverability in their decision to adopt Huawei. By adopting Huawei, Canada would gain access to a 5G network faster than using another provider as Huawei is currently the leader in developing the technology. The European developers, as well as AT&T in the US are close to developing the same technology but are not yet at the same point as Huawei. Therefore, Canada would be in a waiting position to adopt another provider's technology. The presence of Huawei in Canada would also facilitate the addition of 5G and would also support the relationship between Canada and China.

Challenges: Backlash for the adoption of Huawei from the US is highly likely, as numerous statements from US politicians highlighted the severing of ties as a result of untrustworthiness of Canada's decision. Political tension may develop as a result of the non-consensus on Huawei tech between the states. The decoupling of Canada and the US would result due to the concerns from the US on Huawei.

Justification: With the adoption of Huawei tech by Britain and it remaining a member of the alliance, Canada would gain the ability to consider the adoption of the tech as well. While there is a greater ability to decide on the adoption of the tech, it is recommended that Canada act in the interest of maintaining strong alliances as well as working to preserve network connectivity.

[185] Sherif Abdelwahab, et al., “Network Function Virtualization in 5G,” *IEEE Communications Magazine* (2016): 84.
[186] Sherif Abdelwahab, et al., “Network Function Virtualization in 5G,” *IEEE Communications Magazine* (2016): 84.
[187] Long Zhao, et al., *Massive MIMO in 5G Networks: Selected Applications*, (Washington: Springer, 2018), 1.
[188] Yin Zhang and Min Chen, *Cloud Based 5G Wireless Networks*, (Cham, Switzerland: Springer International Publishing, 2016), 5.
[189] Government of Canada, “What Is 5G?” Communications Research Centre Canada, July 20, 2017, Accessed at http://www.crc.gc.ca/eic/site/069.nsf/eng/00077.html.
[190] Aaron Hutchins, “What’s the Worst China Could Do with Access to Canada’s 5G Network?” Macleans, December 20, 2018, Accessed at https://www.macleans.ca/society/technology/whats-the-worst-china-could-do-with-access-to-canadas-5g-network/.
[191] Arthur Herman, “The War For the Worlds 5G Future,” *Forbes*, October 18, 2018, Accessed at https://www.forbes.com/sites/arthurherman/2018/10/17/the-war-for-the-worlds-5g-future/#33c374591fe5.
[192]Aaron Hutchins, “What’s the Worst China Could Do with Access to Canada’s 5G Network?” Macleans, December 20, 2018, Accessed at https://www.macleans.ca/society/technology/whats-the-worst-china-could-do-with-access-to-canadas-5g-network/.
[193] Aaron Hutchins, “What’s the Worst China Could Do with Access to Canada’s 5G Network?” Macleans, December 20, 2018, Accessed at https://www.macleans.ca/society/technology/whats-the-worst-china-could-do-with-access-to-canadas-5g-network/.
[194] Larry Downes, “5G: What is it Good For?” The Washington Post, June 5, 2018, Accessed at https://www.washingtonpost.com/news/innovations/wp/2018/06/05/5g-what-is-it-good-for/?utm_term=.b6e25ef181aa.
[195]Aaron Hutchins, “What’s the Worst China Could Do with Access to Canada’s 5G Network?” Macleans, December 20, 2018, Accessed at https://www.macleans.ca/society/technology/whats-the-worst-china-could-do-with-access-to-canadas-5g-network/.
[196] J. G. Andrews *et al*., "What Will 5G Be?," in *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, (2014): 1065, doi: 10.1109/JSAC.2014.2328098.
[197] J. G. Andrews *et al*., "What Will 5G Be?," in *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, (2014): 1065 , doi: 10.1109/JSAC.2014.2328098.
[198] Independent Fiber Networks, *4 Ways 5G Could Radically Change Transportation in Smart Cities*, March 8, 2019, http://ifnetwork.biz/resources/blog/5g-transportation-smart-cities.
[199] Independent Fiber Networks, *4 Ways 5G Could Radically Change Transportation in Smart Cities*, March 8, 2019, http://ifnetwork.biz/resources/blog/5g-transportation-smart-cities.
[200] Independent Fiber Networks, *4 Ways 5G Could Radically Change Transportation in Smart Cities*, March 8, 2019, http://ifnetwork.biz/resources/blog/5g-transportation-smart-cities.
[201] Robert Fife, “Ottawa Not Ruling out Blocking Huawei from 5G Supply Contracts,” *The Globe and Mail,* November 2, 2018, Accessed at https://www.theglobeandmail.com/politics/article-ottawa-not-ruling-out-blocking-huawei-from-5g-supply-contracts/.
[202] James A. Lewis, “How 5G Will Shape Innovation and Security,” *Center for Strategic & International Studies* (2018).
[203] Paul Triolo, Kevin Allison, and Clarise Brown, “Eurasia Group White Paper: The Geopolitics of 5G." *Eurasia Group*, (2008): 13.
[204] Samantha Hoffman,and Elsa Kania, “Huawei and the Ambiguity of China’s Intelligence and Counter-Espionage Laws,” *Australian Strategic Policy Institute* (2018).
[205] Paul Triolo, Kevin Allison, and Clarise Brown, “Eurasia Group White Paper: The Geopolitics of 5G." *Eurasia Group*, (2008): 16.
[206] Paul Triolo, Kevin Allison, and Clarise Brown, “Eurasia Group White Paper: The Geopolitics of 5G." *Eurasia Group*, (2008): 16.
[207] Paul Triolo, Kevin Allison, and Clarise Brown, “Eurasia Group White Paper: The Geopolitics of 5G." *Eurasia Group*, (2008): 13.
[208] Richard Fadden, “For the security of Canadians, Huawei should be banned from our 5G networks,” *The Globe and Mail*, January 30, 2019. Accessed at https://www.theglobeandmail.com/opinion/article-for-the-security-of-canadians-huawei-should-be-banned-from-our-5g/.
[209] "Huawei: Should We Be Worried about the Chinese Tech Giant?" *BBC News*, March 7, 2019. https://www.bbc.com/news/business-46465438.
[210] Virginia Greiman. 2018. Cyber espionage: The silent crime of cyberspace. *International Conference on Cyber Warfare and Security*: 245-251,XIII, https://www-lib-uwo-ca.proxy1.lib.uwo.ca/cgibin/ezpauthn.cgi?url=http://search.proquest.com.proxy1.lib.uwo.ca/docview/2018924246?accountid=15115 (accessed March 8, 2019).
[211]Dan Bousfield. "Revisiting Cyber-Diplomacy: Canada-China Relations Online." *Globalizations* 14, no. 6 (2017): 1054.
[212] Aaron Hutchins. "What’s the Worst China Could Do with Access to Canada’s 5G Network?" *Macleans*, December 19, 2018. Accessed at https://www.macleans.ca/society/technology/whats-the-worst-china-could-do-with-access-to-canadas-5g-network/.

[213] Aaron Hutchins. "What's the Worst China Could Do with Access to Canada's 5G Network?" *Macleans*, December 19, 2018. Accessed at https://www.macleans.ca/society/technology/whats-the-worst-china-could-do-with-access-to-canadas-5g-network/.

[214] Aaron Hutchins. "What's the Worst China Could Do with Access to Canada's 5G Network?" *Macleans*, December 19, 2018. Accessed at https://www.macleans.ca/society/technology/whats-the-worst-china-could-do-with-access-to-canadas-5g-network/.

[215] David Bond, "UK Cyber Intelligence Chief Urges West to Engage with China. *Financial Times*, October 24, 2018. https://www.ft.com/content/cef6706e-d771-11e8-a854-33d6f82e62f8

[216] "Huawei: Should We Be Worried about the Chinese Tech Giant?" *BBC News*, March 7, 2019. https://www.bbc.com/news/business-46465438.

[217] Dan Bousfield. "Revisiting Cyber-Diplomacy: Canada-China Relations Online." *Globalizations* 14, no. 6 (2017): 1054.

[218] Dan Bousfield. "Revisiting Cyber-Diplomacy: Canada-China Relations Online." *Globalizations* 14, no. 6 (2017): 1054.

[219] David Bond, "UK Cyber Intelligence Chief Urges West to Engage with China. *Financial Times*, October 24, 2018. https://www.ft.com/content/cef6706e-d771-11e8-a854-33d6f82e62f8

[220] Virginia Greiman. 2018. Cyber espionage: The silent crime of cyberspace. *International Conference on Cyber Warfare and Security*: 245-251,XIII. 246.

[221] David Bond. 2018. UK cyber intelligence chief urges west to engage with china. *FT.com* (Oct 24). 1.

[222] Emilio Iasiello, "China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities," *Journal of Strategic Security* 9, no. 2 (2016): 46.

[223] Emilio Iasiello, "China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities," *Journal of Strategic Security* 9, no. 2 (2016): 46.

[224] "U.S. Companies Announce 5G Launch Dates, but Canadian Telecoms Stay Mum," *CBC*, April 1 2018. Accessed at https://www.cbc.ca/news/business/5g-wireless-technology-launch-dates-1.4601594.

[225] Brennan MacDonald, and Vassy Kapelos, "Canada Could Threaten U.S. Security by Allowing Huawei into 5G Network, Says U.S. Senator," *CBC*, January 3, 2019. Accessed at https://www.cbc.ca/news/politics/powerandpolitics/canada-huawei-5g-tech-risk-us-1.4965297.

[226] Brennan MacDonald, and Vassy Kapelos, "Canada Could Threaten U.S. Security by Allowing Huawei into 5G Network, Says U.S. Senator," *CBC*, January 3, 2019. Accessed at https://www.cbc.ca/news/politics/powerandpolitics/canada-huawei-5g-tech-risk-us-1.4965297.

[227] William Banks, "Cyber Espionage, Surveillance, and International Law: Finding Common Ground," Address at the Texas A&M Law Review Symposium, October 17, 2014, 5.

[228] Brennan MacDonald, and Vassy Kapelos, "Canada Could Threaten U.S. Security by Allowing Huawei into 5G Network, Says U.S. Senator," *CBC*, January 3, 2019. Accessed at https://www.cbc.ca/news/politics/powerandpolitics/canada-huawei-5g-tech-risk-us-1.4965297.

[229] Janyce McGregor, "Banning Huawei from Canada's 5G Networks could be Costly for Taxpayers," *CBC*, February 17, 2019. Accessed at https://www.cbc.ca/news/politics/huawei-canada-china-fipa-1.5021033?fbclid=IwAR2K41T3cYWrRIR_C71ihiakxxDfNq58u-RhoSlpzIK1Ttule_y8tfoHUfo.

[230] Jim Bronskill, "U.K. Approval of Huawei's 5G Networks would give Canada Breathing Room, Expert Says," *Global News*, February 18, 2019. Accessed at https://globalnews.ca/news/4973087/huawei-5g-network-uk-canada/.

[231] Jonathan A. Obar, and Andrew Clement, "Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty," *Technology and Emerging Media* (2013): 5.

Information Warfare

THE DAILY
FAKE NEWS
ECONOMY OF THE EUROPEAN UNION
WORLD BANK'S STOCK AT ALL-TIME HIGH / US RATE RISE CHANCES RECEDE AS JOBS GROWTH SLOW
US RATE RISE CHANCES RECEDE AS JOBS GROWTH SLOWS
WORLD BANK'S STOCK AT ALL-TIME HIGH
THE WORLD IS MESSED UP

Visualizing Canada's Future in the Fifth Domain

Mitigate the ability of non-state actors to weaponize information and utilize information warfare tactics.

Information Warfare

Threats of Misinformation & Disinformation

Background

Robinson, Jones and Janicke in “Cyber warfare: Issues and Challenges” provide solid background on the various definitional issues with the terms “cyber warfare” and “information warfare.” They discuss four definitions of information warfare. Thomas Rhona defined the term as “the strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives.”[232] Martin Libicki broke down information warfare into seven sub-categories: command-and-control, intelligence-based, electronic, psychological, hacker, economic information, and cyber.[233] Dorothy Denning defined information warfare as “offensive and defensive operations against information resources of a win-lose nature.”[234] Kopp argued that the one of the main facets of information warfare was to “corrupt, deny degrade and exploit adversary information and information systems and processes while protecting the confidentiality, integrity and availability of one's own information.”[235]

Robinson et al. do not conclude on a preferred definition for information warfare. One conclusion can be drawn from their analysis that “information warfare” is viewed mostly through a state-centric lens in which states act within cyberspace to achieve strategic aims related to cyberspace. Their definition of cyber warfare as “the use of cyber attacks with a warfare-like intent” is similarly state-centric. The most comprehensive analysis of cyber warfare from a state-centric perspective is NATO’s Tallinn Manual on International Law Applicable to Cyber Warfare which “gives guidance on how existing laws of armed conflict apply to cyber war.”[236]

These definitions and the Tallinn Manual focus narrowly on both the state and on information and cyber warfare specifically as threats to ICTs. The selected cases on anti-intellectualism and the use of the internet by terrorist organizations consider a different understanding of information warfare which prioritizes information as the object of study. These cases look at information warfare from which a public diplomacy perspective, whereby non-state and state actors weaponize information in cyberspace to achieve strategic aims. For this purpose, information warfare is defined as “develop[ing] and us[ing] in practice various synthetic technologies in order to manage group and mass opinion in rival (opponent) countries.”[237] This passage in “Information Warfare and Deception” by William Hutchinson elaborates on this idea:

> “Information in the Information Age is about controlling the ‘infosphere’. It includes perceptions and information flows at the tactical, operational and strategic level in times of peace, tension, and war. As such, it means controlling sources and the dissemination of information that favours the dominant party. As such, that information may or may not represent physical reality. In other words, “information that favours the dominant party” might be a subset of ‘reality’ or, in fact, an ‘artificial reality.’[238]

This is not new to the conduct of warfare. Hutchinson tells the story of the conceptual development of information warfare through the advent of news media and reporting during wartime, beginning during the Vietnam War in the United States.[239] Since then, the US government has adapted to a changing mass media landscape and actively utilized public diplomacy techniques to control information within its population, deemed “information operations.”[240] As media and the ‘infosphere’ has increasingly moved online, so has information warfare. With the development of social media and a rapid expansion of the ‘infosphere’ in the 21st century, public diplomacy techniques have been adopted by non-state actor groups including terrorist organizations like ISIS and Al Qaeda, anti-vaxxers and climate change deniers who craft narratives to persuade people online.

Ignas Kalpokas in “Information Warfare On Social Media: A Brand Management Perspective” examines how actors can successfully create and spread information and narratives through social media. For example, through what the author calls “social cyber influence campaigns,” consumers contribute to “open source branding” whereby “consumers are the creators of the value that they themselves consume.”[241] This is effectively an explanation of virality online. When an actor creates a piece of information, the information builds an inertia formed by devoted consumers who read, internalize, endorse, and share the information with other consumers. An understanding of the networked spread of dis/misinformation online through information warfare tactics is a serious challenge for the international community, and has negative implications for issues ranging from public health, to national security, to safety from the potential impacts of climate change.

Anti-Intellectualism

In recent years, there has been a distinct rise in the number and influence of anti-intellectual groups within Canada, the United States, and globally which have been propagated through online mediums, specifically utilizing information warfare to spread their message. This includes the anti-vaccination movement and climate denial. Moreover, various populist governments have come to power on a message disparaging those who are highly educated, again using methods of mis/disinformation and engaging in information warfare.

The anti-vaccination movement has dominated the international press in recent years as the growing influence of this movement which began with a now disavowed article by British doctor Andrew Wakefield linking the vaccination for Measles, Mumps, and Rubella (MMR) with autism and spread by celebrity personalities like Jenny McCarthy and even Oprah Winfrey.[242] While the first wave of anti-vax sentiment spread after Wakefield’s findings in 1998, trust was slowly rebuilt until the Web 2.0 era, the era of user-generated online content, which has once again brought the anti-vaccine movement to prominence.[243] These groups have attempted to reframe themselves from anti-vaccine to pro safe vaccine while also skewing the results of scientific studies, framing vaccines are unnatural, and attacking critics as pharmaceutical industry “shills.”[244] Web 2.0 has brought together fringe elements who have always been against vaccination to have a more potent online presence, but they have also spread their influence through the use of these common tropes to reach those who are already predisposed to be distrustful of expert figures like doctors and scientists, and who are looking for an alternative source of knowledge.[245] The results have been catastrophic. With vaccination rates falling below the approximately 96-99%

necessary to maintain herd immunity, previously eradicated diseases are now re-emerging in society.[246] While Tafuri et al. emphasize the necessity for Health Care Workers (HCWs) to educate themselves to combat the anti-vaccination movement, it is clear that a far more comprehensive approach will likely be necessary to mitigate the widespread effects of the anti-vaccination movement.[247]

Climate denial groups are quite similar, although there is one important distinction to make between climate deniers and anti-vaccination groups. Like anti-vaccination groups, they craft the appearance of legitimacy online. The Global Warming Policy Forum (GWPF) for instance, which has almost 8,000 Facebook likes, begins its deception with its official sounding name and uses tactics like hyperlinking work done by themselves or other climate denial sites in lieu of external sourcing to appear legitimate.[248] While they also misrepresent scientific data through editorializing headlines, referencing discredited information, or simply lying about findings.[249] The difference though is that climate denial groups are supported by industry-funded or conservative think tanks who have a vested interest in climate denial – something which does not exist with the anti-vaccination movement.[250]

With the rising popularity and influence of these anti-intellectual movements, populist politicians, parties, and now elected governments are embracing this anti-intellectualism. Donald Trump stated on the campaign trail that "Autism has become an epidemic. You take this little beautiful baby and you pump… I mean it looks just like it's meant for a horse, not a child."[251] He further claimed that climate change is a hoax perpetrated by the Chinese.[252] While Viktor Orban has banned gender studies in Hungarian universities stating that only two genders exist despite the abundance of research to the contrary.[253] These beliefs are being mainstreamed because a distrust of public officials and experts leads to spillover effects, including the election of populist, anti-intellectual political figures.[254] Political Scientist Jonathan Kennedy denotes this relationship between populist politics and the anti-vaccination movement. With more anti-vaccine advocates come more people who subscribe to the politics of those who espouse populist rhetoric which is fundamentally reshaping our international system such as through growing protectionist trade policies and immigration restrictions, amongst others.[255]

Terrorism

The cyber sphere provides a nexus for terrorist organization to conduct information warfare aimed at recruiting and radicalizing individuals and populations. The internet is a transformative technology that terrorists are exploiting for the spread of propaganda, radicalizing new recruits, and procuring funding. Modern and sophisticated information control campaigns center on using online social networking to control narratives and recruit assets form the foundation of many operational terrorist networks. By exploring cases related to this phenomenon, we can better understand what elements need to be incorporated in order to create an effective cyber regime framework that addresses terrorism.

Terrorist organizations and insurgencies have long appreciated the importance of shaping the perceptions of contested populations. Groups like the Islamic State and Al Qaeda view information warfare as the central strategic mechanism through which politico-military activities should be framed.[256] These operations are often multi-dimensional, targeting both "friend and foe" through the same content and messages.[257] There are two main streams that IS used to control the flow of information and narratives. The first category is formal sources. This includes formally released communiqués, platforms such as billboards in areas that IS controls, online publications (such as Dabiq magazine) and videos.[258] The formal channel is aimed primary at domestic information control and population suppression. The M.O. of the IS in the domestic sphere is to deprive populations from reliable sources of information and instead amplify IS backed information sources the support the groups narratives and ideological positions. Many of the group's publications within this category read like news stories analyzing current events. Examples of this include pieces about the Assad regime's targeting of IS 'citizens' in Ar-Raqqa to the distribution of food and charity to citizens during Ramadan, to the commemoration of the destruction of the Syria-Iraq border.[259] The goal of this practice is to shape the perceptions of contested populations in order to solidify legitimacy in newly occupied regions and to provide a 'personalised' counter-narrative to Western media reporting as well as anti-IS rhetoric.

Furthermore, IS has used information warfare to give its audiences the perception of an accountable and transparent authority. It has established a short film series entitles 'On Patrol with the Office of Consumer Protection'. A featured a short interview with an Ar-Raqqa restaurant worker who stated that business was good under IS and that occupational health and hygiene inspections were working well. This is not uncommon, as many of IS' promotional material inside its territory proclaims improvements in the populations well-being. The message to the average citizen with this message is clear: under IS rule society will function effectively, government is accountable and is fulfilling God's will. Controlling the perception that life is better under IS is critical to the group's longevity and political interests. According to CIA reporting released in September 2014, IS had a fighting force of 20,000–31,500 stretched across approximately one-third of Syria and Iraq.[260]Without the support of local populations IS would have little hope of militarily holding the territory under its control, let alone implementing its highly bureaucratized governance apparatus. Since then, ISIS has largely been weakened even further, increasing their reliance on information control in order to keep the remaining populations under their control in check.

In their 'informal' communiqués, IS members use mobile phones and social-media forums like Twitter, Diaspora, Reddit, and Facebook to send text, photo and video messages.[261] These are targets more at international actors, namely at potential recruits. Combat videos, lifestyle Vlogs, and pictures have been used in draw in recruits from around the world. They aim to override narratives of IS being weak or a brutal lifestyle, instead portraying a life of adventure and personal fulfillment.[262] Informal IS mediums often serve as channeling mechanisms by finding and drawing in individuals interested in joining IS and redirecting them to official channels for recruitment. Key to this is messaging. IS must portray a narrative of victory and only victory in order to continue to attract recruits to its Middle Eastern branches. During 2016-2017, online stories about IS losing the fight had a profound impact on the group. Many recruits were unwilling to go to a place where IS was believed to be losing. Instead, branches of IS in Southeast Asia received most of the incoming recruit numbers, because they were still winning in this region. This highlights how critical it is to the IS position to control the online narrative of who's winning online.

Considering the transnational nature of information warfare and disinformation campaigns, our recommendations focus primarily on international frameworks. These frameworks incorporate state and private actors to re-establish trust in our public institutions and experts. Meaningful domestic policies can be implemented by the Canadian government. However, these policies should originate from international agreements and commitments with the Canadian government developing, adapting, and implementing these frameworks domestically.

Recommendations

Considering the transnational nature of information warfare and disinformation campaigns, our recommendations focus primarily on international frameworks. These frameworks incorporate state and private actors to re-establish trust in our public institutions and experts.

Meaningful domestic policies can be implemented by the Canadian government. However, these policies should originate from international agreements and commitments with the Canadian government developing, adapting, and implementing these frameworks domestically.

5.1 International Agreement and Framework for the Promotion of Cyber Literacy

Actors Involved: The United Nations, National Governments and their Respective Educational Bodies, Private Citizens
Type of Solution: Legal and Normative
Main Issues Involved: Online Radicalization, Internet Access, Social Division, Mis/Disinformation, Fake News
Main IR Issues: Governance, Sovereignty and State Power, Development, Election Interference, Reach of International Law, Cooperation

Explanation: One of the leading factors in the proliferation of fake news and the susceptibility of citizens to being influenced and manipulated by information warfare for malicious actors is the lack of education and cyber literacy. While education curricula cover the basics of math, English, science and other required subjects, it neglects to teach students how to identify sources of mis/disinformation and how to use the internet to better inform oneself instead of being exposed to and believing fake news sources. Consequently, we believe it would be advantageous to negotiate an international agreement which would primarily do three things to promote cyber literacy. First, it would create a United Nations cyber literacy body, potentially under the auspices of UNESCO, which would establish educational curricula standards for national governments to adopt to promote cyber literacy by studying of best practices and current challenges in promoting cyber literacy while also conducting primary research on improving cyber literacy. Second and most importantly, the international agreement would include an incentive structure with monetary inducements to encourage the adoption of cyber literacy standards for national governments to incorporate in their curricula with the ultimate aim being a mandate for a cyber literacy regulation “floor” which all states would have to adopt. Lastly, so that developing countries can participate in this initiative, this international agreement would create a funding mechanism to provide developing states with better internet access and the funds necessary to enforce a cyber literacy curriculum.

Challenges: There are three main challenges to this recommendation. First, acquiring funding for international initiatives is notoriously difficult as seen in the battle to establish a global climate fund over the past decade. The United States who has historically been one of the largest contributors to international institutions would like not contribute to this fund considering their current leadership and political climate, however, the EU would perhaps be a willing partner. Second, populist governments such as those in the United States and Hungary, as well as those who have utilized information warfare to promote their national interests like Russia and China might be hesitant or outright hostile to this proposal. Lastly, this recommendation does not address cyber literacy amongst older generations who are already out of school. There can be adult cyber literacy education classes, but they would likely not be mandatory like elementary and secondary schooling is in most countries.

Justification: We are recommending this action because it is one of the least invasive ways to combat information warfare and mis/disinformation. Unlike government censorship, promoting cyber literacy does not limit the freedom of the internet which we see as an important principle to uphold. Further, it empowers individuals to be more responsible citizens and it works to re-establish trust in experts and expert institutions which has eroded in the past few decades. Through these educational efforts, fake news sites can be pushed back to the fringes and the internet can be used as a tool to further citizens' information gathering and learning abilities while protecting democratic institutions from malevolent actors who seek to disrupt the system.

5.2 International Commitment to Address Disinformation

Actors Involved: United Nations, National Governments, Citizens, Consumers, Private enterprise
Type of Solution: Legal and Regulatory
Main Issues Involved: Mis/disinformation, Censorship, Freedom of Speech, Fake News
Main IR Issues: Governance, Human Rights, Reach of International Law

Explanation: The primary goal of this international agreement should be to provide a baseline commitment on which states can build national policy frameworks to address disinformation and limit the ability of non-state actors to intentionally mislead and harm people.

This international commitment could establish standard definitions for "disinformation," mutually-acceptable citizens' rights as they relate to disinformation, and commitments for states to take measures domestically to safeguard these rights. On this front, some work has already been accomplished according to the Council on Foreign Relations.[263] The UN Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) created a "cyber code of conduct" in 2015 which could be expanded upon.[264] This document noted a previous proposal for an "international code of conduct for information security" proposed by a few states including Russia and China in 2015.[265] An international agreement could set basic standards for how disinformation is understood in its relationship to citizen and consumer rights, and build ground for more ambitious international commitments in the future.

The Canadian government could adapt such an agreement nationally in a few ways. The Canadian government could commit to financially supporting civil society organizations and NGOs whose mandate it is to spread evidence-based information in cyberspace. These organizations could include those related to public health, science and anti-radicalization. This would require corporations like Facebook, YouTube, and Twitter to seriously curtail content which is fundamentally opposed to values articulated in the Charter. Transparency laws could be passed which require non-state actors to publicly disclose online who supports them financially. Lastly, the Canadian government could follow the example of the European Union's General Data Protection Regulation (GDPR) which sets standards for corporations which collect data from consumers, and defines rights for EU citizens in relation to their data online.[266] Canada could develop standards for corporations and rights for consumers related to disinformation spread in cyberspace.

Challenges: There are two major challenges to this proposal. The first is the political environment surrounding "freedom of speech" in Canada and the United States. Any attempt by the Canadian government to regulate 'speech' online could be politically costly. By approaching this from a civil society and Charter rights perspective, these political costs may be reduced. Secondly, any international agreement must satisfy states who typically demand strong clauses respecting national sovereignty. However, the proposal from China and Russia does provide some hope that an agreement on information could be possible. Also, establishing broader guidelines related to disinformation regulation, instead of legally-binding obligations, should reassure states that they have latitude to decide their own policy domestically. However, this raises another challenge: who defines "disinformation?" An international agreement on information warfare could permit authoritarian regimes to regulate any groups in cyberspace which threaten their legitimacy.

Justification: The primary goal of these initiatives is to protect citizens from non-state actors intending to use principles of information warfare to achieve harmful strategic aims. Related to anti-intellectualism, there is a serious need for governments to characterize anti-vaxxer organizations as security threats and address them accordingly. While criminalization may be too unpalatable for free speech absolutists, delegitimizing these groups and revealing their political aims through mandated transparency laws could be effective. Related to anti-terrorism, corporations like Twitter have taken measures to remove accounts linked to ISIS from their platforms. However, a concerted international effort to deplatform extremist/terrorist groups could be incredibly effective in eliminating their ability to practice information warfare and spread disinformation.

[232] Michael Robinson, Kevin Jones, and Helge Janicke, "Cyber warfare: Issues and Challenges," *Computers and Security* 49 (2015): 72. https://www.academia.edu/33071521/Cybersecurity_in_the_EU_Common_Security_and_Defence_Policy_CSDP_-_Challenges_and_risks_for_the_EU_STUDY_Science_and_Technology_Options_Assessment

[233] Michael Robinson, Kevin Jones, and Helge Janicke, "Cyber warfare: Issues and Challenges," *Computers and Security* 49 (2015): 72. https://www.academia.edu/33071521/Cybersecurity_in_the_EU_Common_Security_and_Defence_Policy_CSDP_-_Challenges_and_risks_for_the_EU_STUDY_Science_and_Technology_Options_Assessment

[234] Michael Robinson, Kevin Jones, and Helge Janicke, "Cyber warfare: Issues and Challenges," *Computers and Security* 49 (2015): 72. https://www.academia.edu/33071521/Cybersecurity_in_the_EU_Common_Security_and_Defence_Policy_CSDP_-_Challenges_and_risks_for_the_EU_STUDY_Science_and_Technology_Options_Assessment

[235] Michael Robinson, Kevin Jones, and Helge Janicke, "Cyber warfare: Issues and Challenges," *Computers and Security* 49 (2015): 72. https://www.academia.edu/33071521/Cybersecurity_in_the_EU_Common_Security_and_Defence_Policy_CSDP_-_Challenges_and_risks_for_the_EU_STUDY_Science_and_Technology_Options_Assessment

[236] Michael Robinson, Kevin Jones, and Helge Janicke, "Cyber warfare: Issues and Challenges," *Computers and Security* 49 (2015): 83-84. https://www.academia.edu/33071521/Cybersecurity_in_the_EU_Common_Security_and_Defence_Policy_CSDP_-_Challenges_and_risks_for_the_EU_STUDY_Science_and_Technology_Options_Assessment

[237] O. V. Syuntyurenko, "Network Technologies for Information Warfare and Manipulation of Public Opinion," *Scientific and Technical Information Processing* 42 (2015): 205. https://link.springer.com/article/10.3103/S014768821504005X

[238] William Hutchinson, "Information Warfare and Deception," *Informing Science* 9 (2006): 213-214. https://link.springer.com/article/10.3103/S014768821504005X

[239] William Hutchinson, "Information Warfare and Deception," *Informing Science* 9 (2006): 213-214. https://link.springer.com/article/10.3103/S014768821504005X

[240] William Hutchinson, "Information Warfare and Deception," *Informing Science* 9 (2006): 215-216. https://link.springer.com/article/10.3103/S014768821504005X

[241]Ignas Kalpokas, "Information Warfare On Social Media: A Brand Management Perspective," *Baltic Journal of Law and Politics* 10, no. 1 (2017): 49.

[242] Anna Kata, "Anti-Vaccine Activists, Web 2.0, and the Postmodern Paradigm – An Overview of Tactics and Tropes Used Online by the Anti-Vaccination Movement," *Vaccine* 30, no. 25 (2015): 3780, 3784. https://www-sciencedirect-com.proxy1.lib.uwo.ca/science/article/pii/S0264410X11019086

[243] Anushka Asthana, Sarah Boseley, and Sonia Sodha, "Today in Focus: Is the Anti-Vaccine Movement Putting Lives at Risk?" *The Guardian Podcasts,* January 2019. Accessed from https://www.theguardian.com/society/audio/2019/jan/07/anti-vaccine-movement-lives-risk-measles-mmr-andrew-wakefield

[244] Anna Kata, "Anti-Vaccine Activists, Web 2.0, and the Postmodern Paradigm – An Overview of Tactics and Tropes Used Online by the Anti-Vaccination Movement," *Vaccine* 30, no. 25 (2015): 3781-3783. https://www-sciencedirect-com.proxy1.lib.uwo.ca/science/article/pii/S0264410X11019086

[245] Anna Kata, "Anti-Vaccine Activists, Web 2.0, and the Postmodern Paradigm – An Overview of Tactics and Tropes Used Online by the Anti-Vaccination Movement," *Vaccine* 30, no. 25 (2015): 3781-3783. https://www-sciencedirect-com.proxy1.lib.uwo.ca/science/article/pii/S0264410X11019086

[246] Azhar Hussain et. al., "The Anti-vaccination movement: A regression in modern medicine," *Cureus* 10, no. 7 (2018): 1-2. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6122668/pdf/cureus-0010-00000002919.pdf

[247] S. Tafuri et. al., "Addressing the anti-vaccination movement and the role of HCWs," *Vaccine* 32, no. 28 (2014): 4861-4862.

[248] Emma Bloomfield and Denise Tillery, "The Circulation of Climate Change Denial Online: Rhetorical and Networking Strategies on Facebook," *Environmental Communication* 13, no. 1 (2019): 24-26, 27-28, https://doi-org.proxy1.lib.uwo.ca/10.1080/17524032.2018.1527378

[249]Emma Bloomfield and Denise Tillery, "The Circulation of Climate Change Denial Online: Rhetorical and Networking Strategies on Facebook," *Environmental Communication* 13, no. 1 (2019): 27-28, https://doi-org.proxy1.lib.uwo.ca/10.1080/17524032.2018.1527378.

[250] Riley Dunlap, "Climate Change Denial Books and Conservative Think Tanks: Exploring the Connection," *American Behavioral Scientist* 57, no. 6 (2013): 700-701. https://journals-scholarsportal-info.proxy1.lib.uwo.ca/details/00027642/v57i0006/699_ccdbacttetc.xml

[251] Anushka Asthana, Sarah Boseley, and Sonia Sodha, "Today in Focus: Is the Anti-Vaccine Movement Putting Lives at Risk?" *The Guardian Podcasts,* January 2019. Accessed from https://www.theguardian.com/society/audio/2019/jan/07/anti-vaccine-movement-lives-risk-measles-mmr-andrew-wakefield

[252] Matthew Motta, "The Dynamics and Political Implications of Anti-Intellectualism in the United States," *American Politics Research* 46, no. 3 (2018): 467. https://journals.scholarsportal.info/details/1532673x/v46i0003/465_tdapioaitus.xml

[253] Lauren Kent and Samantha Tapfumaneyi, "Hungary's PM Bands Gender Study at Colleges Saying 'People Are Born Either Male or Female'," *CNN*, October 2018. Accessed from https://www.cnn.com/2018/10/19/europe/hungary-bans-gender-study-at-colleges-trnd/index.html

[254] Matthew Motta. "Political Implications of Anti-Intellectualism in the United States," *American Politics Research* 46 No. 3 (2018): 472-474, 483.

[255] Jonathan Gatehouse, "Growing anti-vax movement has global ramifications," *CBC News*, February 25, 2019. Accessed at https://www.cbc.ca/news/national-today-newsletter-measles-1.5026003

[256] Haroro J Ingram, "Three Traits of the Islamic State's Information Warfare," *The RUSI Journal* 159, no. 6 (2014): 4. https://journals-scholarsportal-info.proxy1.lib.uwo.ca/pdf/03071847/v159i0006/4_ttotisiw.xml

[257] Edgar Jones, "The Reception of broadcast Terrorism: Recruitment and Radicalization," *International Review of Psychiatry* 29, no.4 (2017): 322. http://vr2pk9sx9w.search.serialssolutions.com/?ctx_ver=Z39.88-2004&ctx_enc=info%3Aofi%2Fenc%3AUTF-8&rfr_id=info%3Asid%2Fsummon.serialssolutions.com&rft_val_fmt=info%3Aofi%2Ffmt%3Akev%3Amtx%3Ajournal&rft.genre=article&rft.atitle=The+reception+of+broadcast+terrorism%3A+recruitment+and+radicalisation&rft.jtitle=INTERNATIONAL+REVIEW+OF+PSYCHIATRY&rft.au=Jones%2C+E&rft.date=2017&rft.pub=TAYLOR+%26+FRANCIS+LTD&rft.issn=0954-0261&rft.eissn=1369-1627&rft.v

[258] [258]Haroro J Ingram, "Three Traits of the Islamic State's Information Warfare," *The RUSI Journal*, 159, no. 6 (2014): 4. https://journals-scholarsportal-info.proxy1.lib.uwo.ca/pdf/03071847/v159i0006/4_ttotisiw.xml

[259] [259]Haroro J Ingram, "Three Traits of the Islamic State's Information Warfare," *The RUSI Journal*, 159, no. 6 (2014): 4. https://journals-scholarsportal-info.proxy1.lib.uwo.ca/pdf/03071847/v159i0006/4_ttotisiw.xml

[260] Jim Sciutto, Jamie Crawford and Chelsea Carter. "ISIS Can Muster Between 20000 and 31500 Fighters, CIA Says" *CNN,* September 2014. Accessed from https://www.cnn.com/2014/09/11/world/meast/isis-syria-iraq/index.html

[261] Haroro J Ingram, "Three Traits of the Islamic State's Information Warfare," *The RUSI Journal*, 159, no. 6 (2014): 4. https://journals-scholarsportal-info.proxy1.lib.uwo.ca/pdf/03071847/v159i0006/4_ttotisiw.xml

[262] Haroro J Ingram, "Three Traits of the Islamic State's Information Warfare," *The RUSI Journal*, 159, no. 6 (2014): 6. https://journals-scholarsportal-info.proxy1.lib.uwo.ca/pdf/03071847/v159i0006/4_ttotisiw.xml

[263] Elena Chernenko, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms," *Council on Foreign Relations*, February 2018. Accessed from https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

[264] United Nations General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," *United Nations General Assembly, Seventieth Session.* July 22, 2015. Accessed from http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[265] United Nations General Assembly. "Letter Dated 9th January 2015 From the permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary General" *United Nations General Assembly, Sixty-Ninth Session.* January 13, 2015. Accessed from http://undocs.org/A/69/723

[266] Staff, European Commission. *2018 Reform of EU Data Protection Rules.* European Commission, 2018. Accessed from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Election Interference

Visualizing Canada's Future in the Fifth Domain

Assist corporate, state, civil, and individual actors in taking a larger role within cyberspace in order to mitigate the threat of election interference, and implement regulations to better protect the election process.

Election Interference

Foreign Intervention in the Cyberspace

Background

When discussing election interference, it is important to note that it is impossible to determine the exact effect an event or story has on the public's perception of political actors and parties. Elections also vary greatly, which means different countries face different challenges when it comes to mitigating interference. For instance, when looking at countries like Ukraine, the United States, and Sweden, the issues faced surrounding election interference differ. We will be looking at the effects of and use of, misinformation and disinformation within these countries and attempt to make recommendations for the upcoming Canadian federal election.

Case Study: The United States of America

We are currently witnessing the decline in reputable journalism in the United States. This decline can be attributed to a myriad of factors including, but not limited to: general distrust of journalistic institutions, a lack of representation, and the repercussions of shrinking revenue.[267] In particular, traditional news sources (i.e. print, radio, and cable news) are seeing a decrease in the share of their countries' total advertising revenues.[268] Instead of these traditional sources being the dominant actors in the dissemination of information, the internet, including social media platforms like Facebook and Twitter and search engines like Google, now have a larger audience. This shift is particularly concerning because new media does not undergo the same level of scrutiny as traditional media and are not held accountable to the information they spread.

This has become an issue in the United States in particular because private actors have used the internet as a tool to distribute false information, making mis/disinformation a major cause for concern. After the American Presidential Election in 2016, a variety of studies sought to quantify and categorize the types of fake news stories which circulated during the race. These studies will be analyzed to determine their impact on the outcome of the 2016 federal election.

The Internet and the 2016 Election

According to Allcott and Gentzkow's study, 62 percent of adults received news on social media during the 2016 election.[269] In addition, popular fake news stories received more shares and interactions than mainstream media stories. Of the stories analyzed in their study of the 156 most shared fake stories on Facebook, 115 of them were pro-Trump or anti-Clinton with a total of 30 million shares whereas 41 of them were Pro-Clinton or anti-Trump with a total of 7.6 million shares. This study shows that voters rely on internet media as a replacement for legacy news sources. This has also resulted in is a greater exposure to fake news for Republican voters in particular.[270]

One particular issue is determining the impact a story might have on an election. Kathleen Hall argues that “linguistic priming, media agenda setting and framing, the susceptibilities of late deciders, the dispositions of those who view both candidates unfavorably, [and] the effects of imbalances in the amount of negative information available about alternative candidates,” were all ways the fake news stories could have affected voting outcomes.[271] She emphasizes how stories created during the election were mostly aimed at mobilizing and demobilizing the types of voters Trump needed to win.[272] This is also reflected by Allcott and Gentzkow’s study where the most prominent stories shared were Pro-Trump or Anti-Clinton. They correlate to a rise in the creation of these stories to a rise of support from white evangelicals and military households for Trump. This was in combination with stories used to suppress the support of black voters and supporters of Democratic Primary candidate Bernie which Hall argues was enough to get Donald Trump elected to office.[273]

Foreign Influences in 2016

Internet news sources seek out ad revenue through viewership and shares which has resulted in the creation of news stories that appeal to emotion and entertainment value. Unfortunately, fake news stories have become profitable and have dominated online news. This is evident by the fact that fake news stories generate more interaction online than news stories from traditional news outlets.[274] During the 2016 election some journalists were able to track an upsurge in fake stories originating from Veles, Macedonia. There was a group of computer science undergraduates and teenagers who launched multiple websites with English domains like USADailyPolitics.com, WorldPoliticus.com and DonaldTrumpNews.co. The stories distributed on these domains generated large, engaged audiences earning some students thousands of Euros daily in digital advertising revenue.[275] Vian Bakir and Andrew McStay also explain how experiments with left leaning content under-performed when compared to Pro-Trump content. This showed that fake stories generated for ad revenue purposes did disproportionately benefit the Trump campaign.[276]

Ukraine in Focus

Election interference conducted through information warfare tactics is best analyzed through the 2016 Ukrainian Presidential Election. Ordinarily, individuals receive most of their information from traditional media sources like cable, print, and radio. In some countries, like Russia, these sources are either owned by the state, controlled by the state, or heavily influenced by the state.[277] In extreme cases, this means that the state has a monopoly on information. Thus, information can often double as propaganda or be used to create specific narratives.[278] With the introduction of the internet and social media the state has lost this monopoly. But states like Russia have been proving this to be incorrect.

With regard to Ukraine, Russia has incorporated cyberspace into its strategic information warfare policy.[279] In addition to controlling a variety of traditional news sources, Russia has also made an effort to turn social media into a weapon.[280] When a state is unable to comprehend social media, private actors can use it to oppose popular narratives and promote dissent.[281] However, when a state is knowledgeable about social media, they attempt to promote pro-state narratives.

One such tactic is strategic posts to social media sites. For example, to control the narrative of the Crimean conflict, resources have been devoted to creating "official, semi-official, and unofficial sources of war-related information."[282] Other efforts include the illegal retrieval of information which is often released without authorization.[283] The results of such tactics mean that individuals must be critical of the information they come across.

Another strategy is the outright dissemination of fake news. An example of this occurred when the Russian media organization Channel One reported that a 3-year-old boy was crucified by Ukrainian soldiers, even though it never happened.[284] Alternatively, social media functions differently. Here, information is less vetted and is not held to a high degree of scrutiny. For example, a Twitter user posted a photo of a crying girl who was allegedly murdered, although it was actually a still from the film *The Brest Fortress*.[285] Traditional and social media are not mutually-exclusive as overlap tends to occur fairly frequently. For example, traditional media will sometimes cite a tweet or Facebook post that is spreading false information.[286]

Also in the Ukraine case, trolls or 'opinion agents' are used as a strategy.[287] These people actively make posts that either impersonate specific groups, actively spread fake information, or oppose what they deem to be harmful opinions.[288] This makes it extremely difficult to use social media as users are unaware of who is a truly opinionated person or a troll. The Russian government has been so successful with their use of trolls that a US commander described their tactics as "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[289]

Since it is difficult to track, we cannot confidently say whether any of these strategies had an effect on the outcome of the recent Ukrainian Presidential election. Instead, it is confirmed that there was an attempt to alter the actual outcome of the ballot counting process.[290] The attack was launched by a hacktivist group known as CyberBerkut.[291] On the 21st of May 2014, CyberBerkut hacked into Ukraine's Central Election Commission where they disabled core network nodes and components of the election system. [292, 293] The result was that a live count was broadcasted for an entire day prior to the end of the election. Additionally, malware was planted in the voting software which sought to alter the data that was collected.[294] A conclusive link to the Russian government was unable to be established.

Combatting Election Interference in Sweden

Due to the perceived threat of Russian election interference, within the past three years, the Swedish government has started to implement several active defensive measures to raise the country's preparedness to an election interference attempt. Before the September 2018 elections, Sweden began to provide additional resources towards enhancing its information and cyber security strategies across all levels of government. One of the collaborations that took place was between the Swedish Armed Forces and the Swedish National Defense Radio Establishment to strengthen the country's cyber defense capabilities.[295] Furthermore, the Swedish government updated its national security strategy document. The document placed high importance on protecting democracy and freedom of speech and elections from the threats of interference from foreign actors and/or states.[296] Along with this strategy, the Swedish government presented a specific "societal information and cyber security" strategy that encourages a "whole-of-society approach."[297] The new Swedish strategy involves multiple levels of responsibility including the roles of national, regional and local government actors and includes non-state actors like private corporations and stakeholders as well as citizens. While finally, in January of last year, they created an agency responsible for psychological defense that specifically focuses on countering disinformation and foreign influence.

For the September 2018 election, Sweden had assigned the Civil Contingencies Agency to be the lead agency and coordinator of the nation's efforts to counter disinformation and influence operations throughout the country. They conducted an analysis along with the Swedish Police Authority and the Election Authority to bring to light what type of vulnerabilities they may expect within their system. This analysis led to the Civil Contingencies Agency disseminating information and guidance to relevant actors. Around 7,000 civil servants at all different levels received training on influence operations and the risks tied with them. The goal was to increase their capability to identify vulnerabilities and counter any threats to the election process. One example of this was creating a type of "Facebook hotline" to provide government officials a forum to report fake Facebook pages. The Civil Contingencies Agency, the Swedish Police and the Election Authority have all worked together to create a high-level national forum to coordinate preemptive defense mechanisms and to strengthen Sweden's overall ability to fight against any interference that occurs related to elections.[298]

The Government of Sweden also works directly with the media to ensure the public's access to reliable and truthful information.[299] The government holds several meetings with traditional and social media representatives to go over possible procedures to combat disinformation and bolster cyber security. The Civil Contingencies Agency meets quarterly through its chaired Media Preparedness Council to go over this dialogue within a formal setting. The Civil Contingencies Agency and the Election Authority work together to offer training to all major Swedish media groups to increase their ability to recognize and flag falsified information relating to the election. Another government agency, the Swedish Media Council, works to empower young people as informed media users and has created a nationwide educational program to teach youth about Russian propaganda. Some Swedish media outlets have also followed suit and launched their own efforts like creating forums that counter disinformation and fact-check. Another focus of the Swedish Police is to educate politicians and political parties to raise their awareness and involvement to counter it. They also provided a handbook to 50,000 politicians at each level of government that works as a guidebook about how to spot disinformation campaigns, increase password protection, how external actors hack into computer systems and what kind of steps to take in order to better protect themselves.[300]

The government of Sweden has placed protecting the democratic system at the forefront of its national security goals and is taking the threat of election interference very seriously. Due to the perceived threat of Russian government election interference, Sweden is taking precautionary measures to raise awareness and capabilities to stop it from happening to them.

Cambridge Analytica Case Study

Cambridge Analytica is a political data analytics firm that specializes in collecting large amounts of consumer data. This is data that political organizations can utilize for targeted advertisements to internet users. In 2014, the firm harvested millions of Facebook users' data without authorization. Facebook estimates that around 87 million users were affected, including 622,000 Canadians.[301] In particular, Cambridge Analytica was involved with a pro-Brexit campaign organization, Leave.EU and later, in 2016, was involved in doing political work for the future U.S. president Donald Trump's general election campaign. On May 1st, 2018, the company closed down because of negative publicity relating to a Facebook investigation.[302]

Christopher Wylie had helped create AggregateIQ, a B.C. based consultancy firm that he says created Ripon, the program used by Cambridge Analytica to target Republican voters in the United States. AggregateIQ is under close scrutiny in Britain for its involvement in the 2016 Brexit referendum. Wylie alleges that the company wrongfully received campaign funds from the anti-EU side in the referendum, while a group of British lawyers released documents claiming that the company did participate in a plan to break election laws. Another company involved was the parent company of Cambridge Analytica, SCL Elections. SCL Elections CEO, Alexander Nix, was once in charge of Cambridge Analytica until he was later suspended. An undercover investigation done by Britain's Channel 4 leaked coverage of Nix and other Cambridge Analytica executives suggesting they could use bribes and other illegal tactics to help clients achieve their political ends. After Wylie left Cambridge Analytics, he created Eunoia Technologies, which is another data-analytics company. In 2016, the firm signed a $100,000 contract with the Canadian Liberal Research Bureau for a project that would help monitor social-media. Canada's Privacy Commissioner Daniel Therrien's office is now formally investigating Facebook over this incident.[303]

The data was obtained through a personality testing application on Facebook. The application was called, "thisisyourdigitallife," and some 270,000 people downloaded it and used it. The application's licensing agreement required users to provide their personal information. It not only allowed Cambridge Analytica to acquire their personal information but also that of their friends on Facebook. AggregateIQ used the data derived from the Facebook information to develop a program called Ripon, which was designed to manage fundraising and voter databases. It targeted specific voters based on psychological profiles created from the data and used questionnaires and surveys to collect more political data for the use of bolstering the Republican Party. Facebook allowed for research methods like this application to take place, but did not allow it to be sold to a third party. When Facebook learned that this data was sold and used for political ends in 2015, it discretely asked the parties involved to discard all the collected data and did not ask for confirmation that the data had been deleted. Cambridge Analytica did not delete the data.[304] The company worked on election campaigns in several major states for a Republican political action committee. Its main objective was "voter disengagement" and "to persuade Democrat voters to stay at home."[305]

This example illuminates the dire need to set higher standards and expectations for corporations and social media platforms like Facebook to better protect its users from data being manipulated and used to influence the election process and outcome. Similar instances of unidentified election interference could exist on social media platforms, putting Canadians at risk in the next election. Facebook is beginning to change policies to better protect its users' personal data, however, other organizations need to follow suit. Individuals should also be aware of the type of information they are allowing to be collected through user agreements of many applications and websites. Corporations within Canada need to bar applications from collecting personal details about users and using that data for commercial purposes relating to elections. Facebook said it will keep looking into the misuse of data of Cambridge Analytica and will be more aware if other companies are trying to do this as well. Jeff Chester, who works for the Center for Digital Democracy, a digital advocacy group in Washington, said faults in Facebook's privacy practices will not disappear despite the end of Cambridge Analytica. Chester said, "Cambridge Analytica's practices, although it crossed ethical boundaries, is really emblematic of how data-driven digital marketing occurs worldwide.

Rather than rejoicing that a bad actor has met its just reward, we should recognize that many more Cambridge Analytica-like companies are operating in the conjoined commercial and political marketplace."[306]

Recommendations

6.1 Establish NGOs and Civil Society Organizations Dedicated to Reviewing and Fact-Checking Public Information and Media

Actors Involved: Private Actors (Corporations, Academic Institutions, etc.), NGOs.
Type of Recommendation: Legal and Normative, Technological.
Main Issues Involved: Elections interference, Disinformation, Misinformation, Fake News
Main IR Issues: Governance, Sovereignty and State Power, Election Interference, Cooperation

Explanation: Of particular interest is StopFake.org, which is an initiative that Canadian citizens could take use in countering disinformation. Canada could create a platform that mirrors StopFake. Its mission was to analyze large volumes of information and publish only what they could definitively prove false. Their webpage uses a form through which readers can submit news stories for evaluation. Their commitment to upholding journalistic objectivity is the ideal scenario of Western media practice, and calls for a bottom-up approach. Civil society actors will be involved in the fact-checking process and presenting it to the public. Information will only be published on StopFake if it can be deemed irrefutably untruthful and misrepresentative.

Challenges: This recommendation could face backlash as a form of government or corporate censorship. With regards to the governmental approach, detractors will see this as the beginning of an institution in which truth is heavily controlled by the government. This necessitates a focus on private actors rather than governments, to mitigate this risk. Governments must first work on building trust before taking a major role in information evaluation and control. However, in using the private approach, challenges in regards to access may still arise. Although private actors are generally better situated to provide the tools and skills to gauge the credibility of information, encouraging individuals to make use of such information is difficult. This may be due to issues of access or mistrust.

Justification: This recommendation assumes that those who have the ability to act, should act. By subjecting information sources to the scrutiny of fact-checking organizations, sources of misinformation will become apparent. Sources known for frequently spreading misinformation will be exposed and those who are not known for it will gain credibility. By having organizations that run independently from government institutions, this recommendation avoids related issues of government corruption and trust.

6.2 Comprehensive Legislation that Requires Multiple Methods of Counting Ballots

Actors Involved: The Integrated Technological Crime Unit (ITCU) of the Royal Canadian Mounted Police (RCMP), Department of Justice Canada, Office of the Privacy Commissioner of Canada (OPC), Canadian Radio-television and Telecommunications Commission (CTRC), Shared Services Canada (SSC), Treasury Board Secretariat (TBS), Defence Research and Development Canada (DRDC), Innovation, Science and Economic Development Canada, Department of National Defence (DND), Canadian Centre for Cyber Security, Canadian Centre for Cyber Security, Communications Security Establishment (CSE), Canadian Anti-Fraud Centre (CAFC), Canadian Security Intelligence Service (CSIS), Innovation, Science and Economic Development Canada (ISED), BlackBerry Limited, Rogers Communications Inc., Bell Canada, and other relevant Non-Governmental Organizations and Private Actors.
Type of Recommendation: Legislative, Technological.
Main Issues Involved: Elections Interference, Information Security, and Regulation.
Main IR Issues Involved: Governance, State Power, Election Interference, and Sovereignty.

Explanation: As shown by the interference of the 2016 Ukraine Presidential election, electronic methods can be compromised by outside actors. For instance, the malware that ensured that the electronic counting system would display a preferred result regardless of the actual outcome came from an external source. Conducting a physical count in addition to the electronic count protected the integrity of the final results. Further, using a closed platform for the electronic ballot will ensure that key controls can only be accessed internally. Thus, multiple forms of ballot counting, in addition to more secure electronic ballot systems, will lower the chances of successful interference. The physical count, alongside the Russian news report, revealed that the results of the electronic ballot counting system were altered. Physical ballots, although they require manpower, are not as susceptible to alteration.

Challenges: Some problems arise with using a two-pronged approach. When using physical and electronic counting systems, the costs of facilitating increase exponentially. For instance, the costs of training physical ballot counters as well as the financial burden of maintaining the software and hardware of electronic ballots is discouraging. Likewise, the creation and maintenance of a network that is wholly dedicated to elections is costly due to the infrastructure that must be laid down. As a closed system, either heavy duty encryption or a wired connection must be built to ensure that there are no external access points, without sacrificing reliability. Finally, more methods of counting ballots increase the possibility of mistakes and present a challenge for timing.

Justification: Ensuring that multiple methods of counting can protect against any sort of interference. If the physical is compromised, then the electronic is maintained and vice-versa. This increases the overall security of elections as the possibility to interfere is reduced across all methods. Further, each method acts as a failsafe option in case one method is compromised.

6.3 International Agreement and Framework for Maintaining the Integrity of Sovereign Democratic Elections

Actors Involved: The United Nations, National Governments (and their respective domestic bodies), Private Actors, Non-Governmental Organizations
Type of Recommendation: Legal, Regulatory, Educational
Main Issues Involved: Disinformation, Misinformation, Fake News, Censorship, Free Speech, Control of Information, Government vs. Private Responsibilities
Main IR Issues Involved: Sovereignty, Governance, Human Rights, International Law, Norm Violation, State Power, Democracy, Elections Interference, Security

Explanation: A framework which is targeted at maintaining national sovereignty, with a focus on elections, can be effective at safeguarding the integrity of elections internationally. Through international commitments against interference, norms can be built which delineate the boundaries between acceptable and unacceptable uses of state influence.

Challenges: With regards to an international agreement framework, the main challenge will be in building consensus among the various states, considering the inherent desire to protect national sovereignty.

Justification: With the growing threat of cyber interference, there is a dire need to better protect the election process from foreign and domestic interference.

[267] Jones, David A. "Why Americans Don't Trust the Media." *Harvard College Press/Politics* 9 no. 2 (2004): 62; Thompson, Derek. "The Media's Post-Advertising Future is Also its Past." *The Atlantic*, December 31, 2018.

[268] Thompson, Derek. “The Media’s Post-Advertising Future is Also its Past.” *The Atlantic*, December 31, 2018.

[269] Hunt Allcott, and Matthew Gentzkow. “Social Media and Fake News in the 2016 Election.” *Journal of Economic Perspectives* 31 no. 2 (2017): 212.

[270] *It is worth noting that although republican voters were more susceptible to viewing fake news, the study also demonstrated that they were less susceptible to believing it likely since they experienced increased exposure. Education levels was also a contributing factor to the susceptibility.* Allcott (2017), 228.

[271] Kathleen Jamieson, Hall. *Cyberwar : How Russian Hackers and Trolls Helped Elect a President What We Don't, Can't, and Do Know*, Oxford University Press, Incorporated, 2018, 211.

[272] Kathleen Jamieson, Hall. *Cyberwar : How Russian Hackers and Trolls Helped Elect a President What We Don't, Can't, and Do Know*, Oxford University Press, Incorporated, 2018, 212.

[273] *Had the 2016- over-2012 increase in the Green Party vote gone instead to Clinton, the Democrats would have carried Michigan and Wisconsin to put in perspective how close the results were.* Hall (2018), 212.

[274] Mark Verstraete, Derek E. Bambauer, and Jane R. Bambauer. “Identifying and Counter Fake News.” *Andy Black Associates* (2017): 5.

[275] Mark Verstraete, Derek E. Bambauer, and Jane R. Bambauer. “Identifying and Counter Fake News.” *Andy Black Associates* (2017): 5.

[276] “*Other profit-oriented fake news genres also proliferate, including health and well-being sites (Silverman and Alexander 2016); and sites where US celebrities praise a small, US town for its helpful people and promising blockbusters filming nearby, apparently micro-targeting these town residents to gain advertising clicks.”* Verstraete (2017), 6.

[277] Ulises A. Mejias and Nikolai E. Vokuev, "Disinformation and the Media: The Case of Russia and Ukraine," *Media, Culture & Society* 39, no. 7 (2017): 1030.

[278] Ulises A. Mejias and Nikolai E. Vokuev, "Disinformation and the Media: The Case of Russia and Ukraine," *Media, Culture & Society* 39, no. 7 (2017): 1028.

[279] Margarita Jaitner, "Russian Information Warfare: Lessons from Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), 88.

[280] Margarita Jaitner, "Russian Information Warfare: Lessons from Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), 88.

[281] Ulises A. Mejias and Nikolai E. Vokuev, "Disinformation and the Media: The Case of Russia and Ukraine," *Media, Culture & Society* 39, no. 7 (2017): 1028.

[282] Margarita Jaitner, "Russian Information Warfare: Lessons from Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), 91.

[283] Margarita Jaitner, "Russian Information Warfare: Lessons from Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), 91.

[284] Ulises A. Mejias and Nikolai E. Vokuev, "Disinformation and the Media: The Case of Russia and Ukraine," *Media, Culture & Society* 39, no. 7 (2017): 1033.

[285] Ulises A. Mejias and Nikolai E. Vokuev, "Disinformation and the Media: The Case of Russia and Ukraine," *Media, Culture & Society* 39, no. 7 (2017): 1033.

[286] Ulises A. Mejias and Nikolai E. Vokuev, "Disinformation and the Media: The Case of Russia and Ukraine," *Media, Culture & Society* 39, no. 7 (2017): 1033.

[287] Margarita Jaitner, "Russian Information Warfare: Lessons from Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), 93.

[288] Margarita Jaitner, "Russian Information Warfare: Lessons from Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), 93.

[289] Ulises A. Mejias and Nikolai E. Vokuev, "Disinformation and the Media: The Case of Russia and Ukraine," *Media, Culture & Society* 39, no. 7 (2017): 1028.

[290] Michael N. Schmitt, ""Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chicago Journal of International Law* 19, no. 1 (2018): 36-37.

[291] Michael N. Schmitt, ""Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chicago Journal of International Law* 19, no. 1 (2018): 36-37.

[292] Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), 81.

[293] Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), 56.

[294] Lawrence Norden, Ian Vandewalker, and Robert J. Woolsey, "Securing Elections from Foreign Interference," Securing Elections from Foreign Interference, last modified 2017,

https://www.brennancenter.org/sites/default/files/publications/Foreign%20Interference_0629_1030_AM.pdf?fbclid=IwAR2bLLM7oBvKHGNoEFT3naJo40TNKhgKAnAKKTig982hrXHRndhwTf0sfNY.

[295] Brattberg, Erik, and Tim Maurer. *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*. Vol. 23. Carnegie Endowment for International Peace, 2018, 22.

[296] Sweden. 2017. *The National Security Strategy of Sweden.* [Stockholm]

[297] Brattberg, Erik, and Tim Maurer. *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*. Vol. 23. Carnegie Endowment for International Peace, 2018, 22.

[298] Brattberg, Erik, and Tim Maurer. *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*. Vol. 23. Carnegie Endowment for International Peace, 2018, 23.

[299] Karlsson, Michael, Christer Clerwall, and Lars Nord. "Do not stand corrected: Transparency and users' attitudes to inaccurate news and corrections in online journalism." *Journalism & Mass Communication Quarterly* 94, no. 1 (2017): 154.

[300] Brattberg, Erik, and Tim Maurer. *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*. Vol. 23. Carnegie Endowment for International Peace, 2018, 24.

[301] The Globe and Mail Editors. "Cambridge Analytica, AggregateIQ and the Facebook Scandal: A Guide to Who's Accused of What." *The Globe and Mail*. May 02, 2018.

[302] The Globe and Mail Editors. "Cambridge Analytica, AggregateIQ and the Facebook Scandal: A Guide to Who's Accused of What." *The Globe and Mail*. May 02, 2018.

[303] The Globe and Mail Editors. "Cambridge Analytica, AggregateIQ and the Facebook Scandal: A Guide to Who's Accused of What." *The Globe and Mail*. May 02, 2018.

[304] The Globe and Mail Editors. "Cambridge Analytica, AggregateIQ and the Facebook Scandal: A Guide to Who's Accused of What." *The Globe and Mail*. May 02, 2018.

[305] Cadwalladr, Carole. "The great British Brexit robbery: how our democracy was hijacked." *The Guardian*7 May 07, 2017.

[306] BC News Editors. "Cambridge Analytica Shutting Down, Blames Bad Press | CBC News." CBCnews. May 02, 2018.

Conclusion

Summary of Case Studies

As evidenced throughout this report, developments in cyber technology and their potential misuse poses a number of significant challenges to the interests of individuals, corporations, national governments, and the international community. While each section of this report offers recommendations geared towards mitigating or eliminating the challenges associated with a single area of concern regarding cyberspace, the only way to address the underlying challenges behind these concerns is the coordination of a number of diverse policy recommendations and actors. The issues outlined in this report highlight five underlying challenges associated within cyberspace, and one challenge which, while not inherently cyber, does have impacts on responses to specific cyber issues. These challenges consist of a lack of cyber-literacy, the absence of international standards, formal rights and protections for individuals online, ineffective incentives for corporations to act in the interest of the public good online, the lack of trust in public institutions, and the unequal access to cyber technologies worldwide. Each of these challenges must be addressed in order to establish an effective international cyber regime.

The first of these challenges addressed throughout the report is the general lack of cyber literacy on the part of governments, corporations and individual users. Increasing cyber literacy internationally is beneficial for a number of reasons, as it decreases risks related to privacy and security of individuals online and reduces the effectiveness of fake news. Various recommendations throughout this report are aimed at increasing cyber literacy among individual users, corporate employees, and the international community as a whole to particularly combat election interference in Ukraine and the United States and mis/disinformation which have propagated false ideas surrounding the efficacy of vaccines for instance.

The second of these challenges is the lack of international frameworks and regulations regarding cyber technologies and online practices. Due to the inherently transnational nature of the internet and cyber technologies, no single nation, body, or organization is capable of enforcing its standards or vision for cyber governance on the entirety of cyberspace. Only through cooperation and collaboration can effective policies addressing the concerns and implications of cyber technology be effective. By establishing international frameworks and standards, continuity of practices can be achieved transnationally. This would allow for data to be secure regardless of where it is located or who is collecting it, the creation of common development practices which utilizes new technology like cryptocurrencies, or to collectively stand against mis/disinformation. While domestic policies have been attempted to address issues arising in cyberspace, it has become clear that international commitments are necessary.

The third of these challenges is the lack of formal rights and protections for individual citizens and users when acting online. The concerns regarding the rights and privacy of the individual online are often connected to the treatment of personal data and information online, something especially relevant considering the extent to which individual data is commodified by private corporations. With corporations and governments taking a more active role in shaping the nature of access to the internet and interactions online, the need for protections of individual security and privacy has become increasingly evident. From ensuring that governments and corporations respect the rights of individual privacy, freedom of speech, and control over their own information, to ensuring users online are acting in an informed and responsible manner, improving the formal protection for these individual rights online will serve to decrease the risks posed to individuals by cyber technologies. One major example of these risks is that of the retention of individual data profiles by major social media services. By collecting information on the actions of an individual online, private corporations are capable of collecting and selling details regarding an individual's interests, travel history and personal information. By increasing the protections afforded to the individual user online, both nationally and internationally, much of the individual risk posed by cyber technologies can be resolved.

The fourth challenge is the unequal access to the internet worldwide, and the implications this inequality has on international development. While access to cyber technologies has been shown to improve state economies, services, and the rate of development within these states, large disparities in internet access exist across the world. With the potential for greater mobility of both information and capital in terms of international development and aid, the potential benefits posed by cyber technologies have become increasingly clear. As recent decades have seen an increase in cash transfers as a method of international development aid provision, the benefits of cyber technologies like cryptocurrencies offer potential improvements in the efficiency, scope, and transparency of development aid. Despite this, there are a number of challenges associated with the inequality connected to access to cyber technologies, such as the high initial cost of developing the necessary infrastructure for proper use of cyber technologies in developing nations. A number of specific recommendations made within this report are focused on decreasing the cost and impact of this infrastructure development and similar cyber technologies, so as to make the use of these technologies more accessible in the context of development aid.

The fifth and final of these challenges is the lack of incentives for corporations to pursue the public good on the internet. Almost all corporations are profit-seeking entities, due to the responsibility they hold to their shareholders; however, actions which promote the public good are not always those which produce the greatest profits. By creating regulation or incentives for corporations, they can be reoriented towards the public good, such as legislating greater security for private information, or institutionalizing hacking-based corporations to find vulnerabilities in software. This report addresses some of these situations and offers recommendations on possible courses of action to rectify these issues of incentive. One such example is increasing data sovereignty through domestic infrastructure development. In some states, corporations do not have a profit-based incentive to fully develop internet infrastructure, as the cost of expanding infrastructure, when compared to the potential revenues derived from expansion, are often seen as prohibitive. This is especially true in states with large, low-population densities and isolated areas. In response, public-private partnerships can be created, in order to provide the benefits of infrastructure to the population, without disrupting the corporations' responsibility to their shareholders.

There is one further challenge that underpins several of the recommendations, but is not inherently cyber-based: the lack of trust in public institutions. The recent trend of populism worldwide symbolizes another, more insidious trend. Individuals no longer trust that their governments are pursuing their best interests. Lack of trust in government may not be a new phenomenon, but it is the extent to which it has propagated throughout the globe, alongside new cyber-issues such as the spread of misinformation and disinformation, that catalyzes it into a serious concern. This challenge is seen as a factor that amplifies the negative effects of fake news, misinformation and disinformation, and as such, it is extremely difficult to challenge directly. Instead, these recommendations use civil society actors and NGOs to combat instances of fake news and mis/disinformation, or promote cyber literacy in order to increase the ability of individuals to combat these trends. These groups can respond to factually incorrect or partially false statements in media without the historic and current distrust tainting their retort, as might be the case with national governments. While these recommendations do provide certain value, there are trade-offs made in these decisions. Cyber innovation is definitively important to some economies, particularly those of developed nations with high levels of internet use. As such, innovation should have been more thoroughly addressed, to make it more amenable to those states with economies more heavily reliant on innovation-based tech production. Similarly, the focus on the individual over corporations can be perceived as another possible point of conflict in this cyber regime. While the EU has a GDPR which is similarly individual focused, China, Russia, USA, and other states do not appear to hold the same affinity toward protecting individual rights over those of corporate or state interests.

When considering the recommendations laid out throughout this report, it becomes clear that a wide variety of actors must be involved in the process of addressing the implications and risks of cyber technologies, including civil society, private corporations, individuals, national governments, and international organizations. Despite the benefits of addressing a multifaceted and transnational issue like cyber governance through collaboration both nationally and internationally, a number of the recommendations made throughout this report are focused toward the potential impact of a single actor or a small number of actors in its implementation. Many of these recommendations are straightforward, or uncontroversial in nature, and as such can likely be implemented quickly, facing only minor challenges to their adoption. For example, from the corporate perspective, recommendations such as introducing employee cyber literacy training, enhanced cybersecurity measures or best practices are a few examples of these types of recommendations. While many of the more promising recommendations involve collaboration at the international level, these short-term, easily implemented recommendations would likely help address the long-term challenges posed by cyber technologies, while laying the foundation for the more challenging recommendations.

While recommendations focused on short-term aims of single actors to mitigate the negative effects of cyber technologies and their misuses can work, they do little to address many of the underlying causes of these same concerns. As a result, many recommendations in this report are focused on more ambitious goals, primarily involving the collaboration of multiple actors whose interests and agendas may not initially be aligned. By working towards partnerships between state and non-state actors, or international agreements to address the transnational implications of cyberspace, these recommendations would ideally contribute to the underlying goal of this report to develop a truly international cyber regime. Finally, while some of the recommendations within this report, such as improving cyber literacy, may be easy to implement by a single actor, the success of these programs require continued commitments on the part of multiple actors and consistent adaptation in the face of ever changing cyber technologies.

From the 2018 case of Swedish electoral interference to the 2019 Facebook updates responding to GDPR, the impacts of cyberspace on the world today are readily apparent. As such, the recommendations use these developments as reference points, with which the current faults can be fixed or mitigated. In doing so, it provides both short and long-term ideas which can be materialized into positive change. This inclusion allows a balance between pragmatic immediate improvements and long-term goals which incremental developments can aim towards. Furthermore, it considers challenges to the enactment of each recommendation, while also reviewing some implications of its implementation. While this report does review a wide variety contexts, from development to corporations and personal data to information warfare, it repeatedly returns to a focus on the individual. The report continuously advocates positions which privilege individuals over other actors, especially businesses. While this could be considered a weakness of the report, in reflection of the countless lives negatively impacted by security breaches and government failures, this focus on the individual is the right approach to building a cyber regime.

Works Cited

“4 Ways 5G Could Radically Change Transportation in Smart Cities.” In *Independent Fiber Networks*, 2016. http://ifnetwork.biz/resources/blog/5g-transportation-smart-cities.

Abdelwahab, Sherif, Bechir Hamdaoui, Mohsen Guizani and Taieb Znati. “Network Function Virtualization in 5G.” *IEEE Communications Magazine* (2016): 85-91.doi:10.1109/MCOM.2016.7452271

Ablon, Lillian, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky. *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information.* RAND Corporation (2016). http://www.jstor.org/stable/10.7249/j.ctt1bz3vwh.

About the World Bank. March 13, 2019.http://www.worldbank.org/en/about.

Aiello, Rachel. “Feds unveil plan to tackle fake news, interference in 2019 election.” *CTV New*s, January 30, 2019. Accessed at https://www.ctvnews.ca/politics/feds-unveil-plan-to- tackle-fake-news-interference-in-2019-election-1.4274273.

Akbarpour, Susan. "How Does GDPR Impact Advertising And E-Commerce?" Forbes. May 08, 2018. Accessed March 20, 2019. https://www.forbes.com/sites/forbesagencycouncil/2018/05/08/how-does-gdpr-impact-advertising-and-e-commerce/#b46f58e32776.

Allcott, Hunt and Matthew Gentzkow. “Social Media and Fake News in the 2016 Election.” *Journal of Economic Perspectives* 31, no. 2 (2017): 211-236.

Almeida, Virgilio A., Danilo Doneda, and Jacqueline De Souza Abreu. “Cyberwarfare and Digital Governance.” *IEEE Internet Computing* 21, no. 2 (2017): 68-71. doi:10.1109/mic.2017.23.

Alvarez, Carlos. “ICT as a Part of the Chilean Strategy for Development: Present and Challenges.” In *The Network Society. From Knowledge to Policy*, edited by Manuel Castells and Gustavo Cardoso. Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2005.

Ammous, Saifedean. “Economics Beyond Financial Intermediation: Digital Currencies’ Possibilities for Growth, Poverty Alleviation and International Development.” *Journal of Private Enterprise* 30, no. 3 (2015): 19-50. http://link.galegroup.com/apps/doc/A426900749/AONE?u=lond95336&sid= AONE&xid=ed506d10.

Amoore, Louise. “Cloud Geographies. ”*Progress in Human Geography* 42, no. 1 (2016): 4-24.

Andrews, J.G. Stefano Buzzi, Wan Choi, Stephen V. Hanly, Angel Lozano, Anthony C. K. Soong, and Jianzhong Charlie Zhang. “What Will 5G Be?” *IEEE Journal on Selected Areas in Communications* 32, no. 6 (2014): 1065-1082. doi:10.1109/JSAC.2014.2328098.

Armerding, Taylor. "The 18 biggest data breaches of the 21st century," *CSO Online*, December 2018. Accessed at https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

Ashford, Chris. “Queer theory, Cyber-Ethnographies and Researching Online Sex Environments.” *Information & Communications Technology Law* 18, no. 3 (2009): 297-314. doi: 10.1080/13600830903424734

Asthana, Anushka, Sarah Boseley, and Sonia Sodha. “Today in Focus: Is the Anti-Vaccine Movement Putting Lives at Risk?” *The Guardian Podcasts,* January, 2019. Accessed at https://www.theguardian.com/society/audio/2019/jan/07/anti-vaccine-movement-lives-risk-measles-mmr-andrew-wakefield

Backman, Sarah. “Organising National Cybersecurity Centres.”*Information & Security* 32, no. 1 (2015):1-18.

Baglione, Stephen L., Katen Amin, Antron McCullough, and Louis Tucci. “Factors Affecting Facebook Advertisements: Empirical Study.” *International Journal of Business, Marketing, and Decision Sciences (IJBMDS)* 11, no. 1 (2018): 124-140.

Bakir, Vian and Andrew McStay. “Fake News and the Economy of Emotions.” *Digital Journalism* 6, no. 2 (2018): 154-175.

Banks, William. “Cyber Espionage, Surveillance, and International Law: Finding Common Ground.” *SSRN Electronic Journal* (October 2014): doi:10.2139/ssrn.2558155.

Barfield, Claude. “China Exposed on Steel Technology Cyber Theft: Why No Indictments?” *American Enterprise Institute* (March 2016):http://www.aei.org/ publication/china-exposed-on-steel technology-cyber-theft-why-no-indictments/.

Behrman, Jere. R., and Emmanuel Skoufias. “Mitigating Myths about Policy Effectiveness: Evaluation of Mexico’s Antipoverty and Human Resource Investment Program.” *The Annals of the American Academy of Political and Social Science* 606, no. 1 (2006): 244-275. https://www.jstor.org/stable/25097827.

Berg, Linda, and Henrik Oscarsson. “The Swedish General Election 2014.”*Electoral Studies* 38 (2014): 82-136.

Berghel, Hal. “Oh, What a Tangled Web: Russian Hacking, Fake News, and the 2016 US Presidential Election.” *Computer* 50, no. 9 (2017): 87-91.

Bjork-James, Sophie “Feminist Ethnography in Cyberspace: Imagining Families in the Cloud,” *Sex Roles* 73 (2015): 113-124. doi: 10.1007/s11199-015-0507-8

Bloomfield, Emma and Denise Tillery. “The Circulation of Climate Change Denial Online: Rhetorical and Networking Strategies on Facebook” *Environmental Communication* 13, no1 (2019): 23-34. https://doi-org.proxy1.lib.uwo.ca/10.1080/17524032 .2018.1527378.

Bond, David. “UK Cyber Intelligence Chief Urges West to Engage with China.” *Financial Times,* October 24, 2018, Accessed at https://www.ft.com/content/cef6706e-d771-11e8-a854-33d6f82e62f8

Bousfield, Dan. “Revisiting Cyber-Diplomacy: Canada-China Relations Online.” *Globalizations* 14, no. 6 (2017): 1045-1059. doi:10.1080/14747731.2017.1362176.

Brattberg, Erik, and Tim Maurer. *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*,vol. 23. Carnegie Endowment for International Peace, 2018.

Bronskill, Jim. “U.K. Approval of Huawei’s 5G Networks would give Canada Breathing Room, Expert Says.” *Global News*, February 18, 2019. Accessed at https://globalnews.ca/news/4973087/huawei-5g-network-uk-canada/.

Brown, Ian and Douwe Korff. “Terrorism and the Proportionality of Internet Surveillance.” *European Journal of Criminology* 6, no.2 (2009):119-134. doi:10.1177/ 1477370808100541.

Burns, Megan. “Information Warfare: What and How?” *Carnegie Mellon School of Computer Science*, 1999. https://www.cs.cmu.edu/~burnsm/InfoWarfare.html.

Cadwalladr, Carole. “The Great British Brexit Robbery: How Our Democracy was Hijacked.” *The Guardian*, May 07, 2017, https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy.

Cain, Patrick. “Feds Unveil Plan to Fight Foreign Interference in 2019 Federal Election.” *Global News*, January 30, 2019. Accessed athttps://globalnews.ca/news/4905368/foreign-election-interference-canada/.

“Cambridge Analytica, Aggregate IQ and the Facebook Scandal: A Guide to Who's Accused of What. ”*The Globe and Mail*, May 02, 2018. Accessed at https://www.theglobeandmail.com/world/article-what-is-cambridge-analytica-and-what-did-it-do-a-guide/.

“Cambridge Analytica Shutting Down, Blames Bad Press.” *CBC News*, May 02, 2018. Accessed at https://www.cbc.ca/news/technology/cambridge-analytica-shutting-down-1.4645324.

Can, Patrick. “Feds unveil plan to fight foreign interference in 2019 federal election.” *Global News*, January 30, 2019. Accessed at https://globalnews.ca/news/4905368/foreign -election-interference-canada/.

Canada. Global Affairs of Canada. Our Priorities in International Assistance. *Canada’s Feminist International Assistance Policy*, Ottawa, CA: Our Priorities in International Assistance, 2017. https://international.gc.ca/world-monde/assets/pdfs/iap2-eng.pdf.

Canada. Global Affairs Canada. *Priorities of Global Affairs Canada*. Ottawa, Ontario: Global Affairs Canada, 2018. https://www.international.gc.ca/gac-amc/priorities-priorites.aspx?lang=eng

Canada. Global Affairs Canada. *Departmental Plan 2018 – 19, Raison D’etre, Mandate and Role: Who we are and what we do.* Ottawa, Ontario: Global Affairs Canada, 2018. https://international.gc.ca/gac-amc/publications/plans/dp-pm/dp-pm_1819_mandate-mandat.aspx?lang=eng

"Canada's Internet Factbook." In Canadian Internet Registration Authority. January 11, 2019. https://cira.ca/factbook/canada's-internet-factbook-2018.

Cavoukian, Ann. *A Primer on Metadata: Separating Fact from Fiction*. Toronto, Ontario: Information and Privacy Commissioner, 2013.https://www.ipc.on.ca/wp-content/uploads/Resources/metadata.pdf

Center for Global Development. "Doing Cash Differently: How Cash Transfer Can Transform Humanitarian Aid." In *Overseas Development Institute*. September 2015. https://www.odi.org/sites/odi.org.uk /files/odi-assets/publications-opinion-files/9828.pdf.

Chowdhry, Geeta and Sheila Nair. *Power, Postcolonialism and International Relations: Reading Race, Gender and Class*. Routledge, 2013.

Clayton, Mark. "Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers. "*The Christian Science Monitor*, June 17, 2014. Accessed at https://www.csmonitor.com /World/Passcode/2014/ 0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers?fbclid=IwAR3dL9-FEan0K9FrxYRHpwN4t_9Cr1asLGKbfnBNbaja0yX3NIKPNpOIBMw.

Colangelo, Giuseppe and Mariateresa Maggiolino. "Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook Case." *International Data Privacy Law,* 8 no.3 (August 2018): 224–239. https://doi.org/10.1093/idpl/ipy018.

Committee on Homeland Security. *Economic Espionage: A Foreign Intelligence Threat to American Jobs and Homeland Security*. Washington: United States Government Printing Office, 2012. http://www.govinfo.gov/content/pkg/CHRG-112hhrg79843/pdf/CHRG112hhrg79843. pdf?fbclid=IwAR1-GFgUM-uIWOVK2banIsHZY1d3xbxYI998-PP3gJGvA94BGda1by07iKI.

Crilley, Kathy. "Information Warfare: New Battle Fields, Terrorists, Propaganda, and the Internet" *Aslib Proceedings* 53 No.7 (2001): 250-264. https://www.emeraldinsight.com/doi/pdfplus /10.1108/EUM0000000007059

Cyber War in Perspective: Russian Aggression Against Ukraine (2015): Tallinn: NATO CCD COE Publications, 2015.

Dahlgren, Peter. "The Internet, Public Spheres, and Political Communication: Dispersion and Deliberation." *Political Communication* 22, no. 2 (August 2006): 147-62. doi:10.1080/ 10584600590933160.

Davis, Susan. *Russian Meddling in Elections and Referenda in the Alliance*. NATO Parliamentary Assembly, 2018, https://www.nato-pa.int/download-file?filename=sites/default/files/2018-11/181%20STC%2018%20E%20fin%20-%20RUSSIAN%20MEDDLING%20-%20DAVIS%20REPORT.pdf.

De Filippi, Primavera and Internet Policy Review. "Foreign Clouds in the European Sky: How US Laws Affect the Privacy of Europeans." *Internet Policy Review* 2, no. 1 (2013).doi: 10.14763/2013.1.113.

Deibert, Ron. “Spy Agencies Have Turned Our Digital Lives Inside Out. We Need to Watch Them.” *Globe and Mail*, June 10, 2013. Accessed at https://www.theglobeandmail.com/ opinion/spy-agencies-have-turned-our-digital-lives-inside-out-we-need-to-watch-them/article12455029/.

Dermineur, Elise M. “Sweden's Election: A Vote Free from Meddling?.” *LSE European Politics and Policy* (EUROPP), September 18, 2018.Accessed at https://blogs.lse.ac.uk/europpblog/2018/09/12/ swedens-election-a-vote-free-from-meddling/.

“The Digital Arms Trade.” *The Economist*, March 30, 2013. Accessed at https://www.economist.com/ business/2013/03/30/the-digital-arms-trade.

Donnelly, Jack. *Realism and International Relations*. Cambridge: Cambridge University Press, 2000.

Doocy, Shannon, Hannah Tappis, and Emily Lyles. “Are Cash-Based Interventions a Feasible Approach for Expanding Humanitarian Assistance in Syria?” *Journal of International Humanitarian Action* 1, no.1 (2016): 10. https://link-springer-com.proxy1.lib.uwo.ca /content/pdf/10.1186%2Fs41018-016-0015-7.pdf.

Downes, Larry. “5G: What is it Good For?” *The Washington Post*, June 5, 2018. Accessed at https://www.washingtonpost.com/news/innovations/wp/2018/06/05/5g-what-is-it-good-for/?utm_term=.b6e25ef181aa.

Dunlap, Riley. “Climate Change Denial Books and Conservative Think Tanks: Exploring the Connection.” *American Behavioral Scientist* 57,no. 6 (June 2013): 699-731. https://journals-scholarsportal-info.proxy1.lib.uwo.ca/details/00027642/ v57i0006/699_ccdbacttetc.xml.

Egan, Erin. "Pardon the Interruption: It's About Your Privacy." Facebook Newsroom. May 24, 2018. Accessed March 20, 2019. https://newsroom.fb.com/news/2018/05/pardon-the-interruption/.

Eriksson, Johan, and Giampiero Giacomello. "The Information Revolution, Security, and International Relations: (IR) relevant Theory?" *International Political Science Review* 27, no. 3 (2006): 221-244. doi:10.1177/0192512106064462.

Eshet-Alkalai, Yoram. “Digital Literacy: A Conceptual Framework for Survival Skills in the Digital Era.”*Jl. of Educational Multimedia and Hypermedia*13, no. 1 (2004): 93-106. https://www.learntechlib .org/p/4793/.

Esteve, Asunción. “The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA.” *International Data Privacy Law* 7, no. 1 (2017): 36–47.

Fidler, David P. “Transforming Election Cybersecurity.” *Digital Repository @ Maurer Law*110, (2017): 337-342.https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=3547 &context=facpub.

Fife, Robert. “Ottawa Not Ruling out Blocking Huawei from 5G Supply Contracts,” *The Globe and Mail,* November 2, 2018. Accessed at https://www.theglobeandmail.com/politics/article-ottawa-not-ruling-out-blocking-huawei-from-5g-supply-contracts/.

Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31. *Ontario*, https://www.ontario.ca/laws/statute/90f31#BK0.

Gatehouse, Jonathan. “Growing Anti-Vax Movement has Global Ramifications.” *CBC News*, February 25, 2019. Accessed at https://www.cbc.ca/news/national-today-newsletter-measles-1.5026003.

Gavett, Brandon E., Rui Zhao, Samantha E. John, Cara A. Bussell, Jennifer R. Roberts, and Chuan Yue. "Phishing Suspiciousness in Older and Younger Adults: The Role of Executive Functioning." *PloS One* 12, no. 2 (2017) 1-16.

"GDPR Key Changes." Key Changes with the General Data Protection Regulation – EU GDPR. Accessed March 20, 2019. https://eugdpr.org/the-regulation/.

Geist, Michael. “Why Watching the Watchers Isn’t Enough: Canadian Surveillance Law in the Post-Snowden Era.” In Law, Privacy and Surveillance in Canada in the Post-Snowden Era. *University of Ottawa Press* (2015): 225-256. http://www.jstor.org/stable/j.ctt15nmj3c.12.227.

General Data Protection Regulation (GDPR). *General Data Protection Regulation (GDPR)*, 2018. Accessed athttps://gdpr-info.eu/.

Gibson, Shane. “Amber Alert for Missing Ontario Girl Leads to Influx of Calls to Winnipeg 911.”*CBC News*, February 15, 2019. Accessed at https://www.cbc.ca/news/canada/manitoba/winnipeg-911-amber-alert-1.5021997.

Gilchrist, Karen. “Australia's prime minister calls for global social media restrictions after Christchurch shootings” *CNBC, World Politics*, March 18, 2019,https://www.cnbc.com/2019/03/19/australias-pm-restrict-social-media-after-christchurch-mosque-attack.html.

Government of Canada. “What Is 5G?” *Communications Research Centre Canada*, July 20, 2017. Accessed at http://www.crc.gc.ca/eic/site/069.nsf/eng/00077.html.

Gregory, Mark A., and David Glance. *Security and the Networked Society*. Switzerland: Springer International Publishing, 2013.

Greiman, Virginia. “Cyber espionage: The silent crime of cyberspace.” *International Conference on Cyber Warfare and Security* (2018): 245-XIII.https://search.proquest.com/docview/2018924246?pq-origsite=summon

Gurney, Matt. “Canada’s plan to protect elections suffers some flaws.” *Global News Commentary*, February 1, 2019. Accessed at https://globalnews.ca/news/4913900/federal-election-foreign-interference/.

Guzzini, Stefano, and Anna Leander eds. *Constructivism and International Relations: Alexander Wendt and His Critics*. London and New York: Routledge, 2006.

Haigh, Maria, Thomas Haigh, and Nadine I. Kozak. “Stopping Fake News: The Work Practices of Peer-to-Peer Counter Propaganda.” *Journalism Studies*19, no. 14 (2018): 2062-2087.

Hart, Melanie. “Criminal Charges Mark New Phase in Bellwether U.S.-China Intellectual Property Dispute.” *Center for American Progress,* June 27, 2013. https://www.americanprogress.org /issues/security/news/2013/06/27/68339/criminal-charges-mark-new-phase-in-bellwether-u-s-china-intellectual-property-dispute/.

Haukkala, Hiski, Carina van de Wetering, and Johanna Vuorelma eds. *Trust in International Relations: Rationalist, Constructivist, and Psychological Approaches*. New York: Routledge, 2018.

Henley, Jon. “Russia Waging Information War Against Sweden, Study Finds.” *The Guardian*, January 11, 2017. Accessed at https://www.theguardian.com/world/2017/jan/11/russia-waging-information-war-in-sweden-study-finds.

Herman, Arthur. “The War for the Worlds 5G Future.” *Forbes*, October 18, 2018. Accessed at https://www.forbes.com/sites/arthurherman/2018/10/17/the-war-for-the-worlds-5g-future/#33c374591fe5.

Hoffman, Wyatt, and Ariel E. Levite. “Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?” *Washington: Carnegie Endowment for International Peace*, 2017. https://www-lib-uwo-ca.proxy1.lib.uwo.ca/cgi-bin/ezpauthn.cgi?url=http://search.proquest.com.proxy1.lib.uwo.ca /docview/1917694386?accountid=15115.

Hou, Rui. “Neoliberal Governance or Digitalized Autocracy? The Rising Market for Online Opinion Surveillance in China.” *Surveillance & Society* 15, no. 3/4 (2017): 418-424. doi:10.24908/ss.v15i3/4.6610.

“Huawei: Should We Be Worried about the Chinese Tech Giant?” *BBC News*, March 7, 2019. Accessed at https://www.bbc.com/news/business-46465438.

Hussain, Azhar, Syed Ali, Madiha Ahmed, and Sheharyar Hussain. “The Anti-Vaccination Movement: A Regression in Modern Medicine.” *Cureus* 10,no. 7 (July 2018): 1-8. https://www.ncbi.nlm.nih.gov /pmc/articles/PMC6122668/pdf/cureus-0010-00000002919.pdf.

Huston, Joe. “Give Directly: Cash Transfers, Basic Income, and Hurricane Relief.” *Talks at Google*, YouTube Video, 25:35, February 8, 2018. Accessed at https://www.youtube.com/watch?v =iyeIsVXjMzU.

Hutchins, Aaron. “What’s the Worst China Could Do with Access to Canada’s 5G Network?” *Macleans*, December 19, 2018. Accessed at https://www.macleans.ca/society/technology/ whats-the-worst-china-could-do-with-access-to-canadas-5g-network/.

Hutchinson, William. “Information Warfare and Deception” *Informing Science* 9 (2006): 213-223. https://www.hsdl.org/?view&did=443229.

Iasiello, Emilio. “China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities.” *Journal of Strategic Security* 9, no. 2 (2016): 45-69.

Ilgit, Asli and Binnur Ozkececi-Taner, “Identity and Decision Making: Toward a Collaborative Approach to State Action,” in *Psychology and Constructivism in International Relations: An Ideational Alliance*, edited by Vaughn P. Shannon and Paul A. Kowert. Ann Arbor: The University of Michigan Press, 2012.

Ingram, Haroro J. “Three Traits of the Islamic State’s Information Warfare.” *The RUSI Journal*159, no. 6 (2014): 4-11. https://journals-scholarsportal-info.proxy1.lib.uwo.ca/pdf/03071847/v159i0006/4_ttotisiw.xml.

International Monetary Fund. “IMF and the Sustainable Goals.” In *IMF Factsheets*, March 8, 2018. https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/16/46/Sustainable-Development-Goals.

Internet Usage Worldwide. Report no. Did-12322-1. Statista, 2018. Accessed March 04, 2019. https://www.statista.com/study/12322/global-internet-usage-statista-dossier/.

“INTERNET5: Shaping an Internet for Women’s Empowerment.” In *International Development Research Centre*, December 8, 2017.https://www.idrc.ca/en/research-in-action/internet5-shaping-internet-womens-empowerment.

Irion, Kristina. “Government Cloud Computing and the Policies of Data Sovereignty.” *International Telecommunications Society* (2011): 1-28.

Jaitner, Margarita. "Russian Information Warfare: Lessons from Ukraine." In *Cyber War in Perspective: Russian Aggression Against Ukraine*, edited by Kenneth Geers, 87-94. Tallinn: NATO CCD COE Publications, 2015.

Jamieson, Kathleen Hall. “Cyberwar: How Russian Hackers and Trolls Helped Elect a President What We Don't, Can't, and Do Know.*” Oxford University Press*, 2018http://ebookcentral.proquest.com/lib/west/detail. action?docID=5497194

Johnson, David R., and David Post. “Law and Borders: The Rise of Law in Cyberspace.” *Stanford Law Review* 48, no. 5 (1996): 1367. doi:10.2307/1229390.

Jones, David A. “Why Americans Don’t Trust the Media.” *Harvard College Press/Politics* 9, no.2 (2004): 60-75.

Jones, Edgar. “The Reception of broadcast Terrorism: Recruitment and Radicalization” *International Review of Psychiatry* 29,no.4 (August 2017): 320-326. doi:10.1080/09540261.2017.1343529.

Kahin, Brian. “Cyberinfrastructure and Innovation Policy.” *First Monday* 12, no. 6 (2007).

Kalpokas, Ignas. “Information Warfare On Social Media: A Brand Management Perspective” *Baltic Journal of Law and Politics* 10 no. 1,(2017):https://www.researchgate.net/publication/320761447 _Information_Warfare_on_Social_Media_A_Brand_Management_Perspective.

Karlsson, Michael, Christer Clerwall, and Lars Nord. “Do Not Stand Corrected: Transparency and Users' Attitudes to Inaccurate News and Corrections in Online Journalism.” *Journalism & Mass Communication Quarterly* 94, no. 1 (2017): 148-167.

Kata, Anna. “Anti-vaccine activists, Web 2.0, and the postmodern paradigm – An overview of tactics and tropes used online by the anti-vaccination movement” *Vaccine* 30,no. 25 (May 2015): 3778-3789. https://www-sciencedirect-com.proxy1.lib.uwo.ca/science/article/pii/S0264410X11019086.

Kelleher, Mike. “Sustainable Development Goals (SDGs) and the 2030 Agenda.” *World Bank Programs*, March 13, 2019. http://www.worldbank.org/en/programs/sdgs-2030-agenda.

Kent, Lauren and Samanthan Tapfumaneyi. “Hungary's PM Bands Gender Study at Colleges Saying ‘People Are Born Either Male or Female.'” *CNN*, October 2018. Accessed from https://www.cnn .com/2018/10/19/europe/hungary-bans-gender-study-at-colleges-trnd/index.html.

Khaldarova, Irina and Mervi Pantti. “Fake News: The narrative battle over the Ukrainian conflict.” *Journalism* Practice 10, no. 7 (2016): 891-901.

Kirkpatrick, David D. “Massacre Suspect Traveled the World but Lived on the Internet,” *New York Times*, March 15, 2019, https://nyti.ms/2FbCtGS.

Knautz, Kathrin, and Baran S. Katsiaryna. “Facets of Facebook: Use and Users.” *De Gruyter Berlin and Boston*, 2016.

Kragh, Martin, and Sebastian Åsberg. “Russia's Strategy for Influence Through Public Diplomacy and Active Measures: The Swedish case.” *Journal of Strategic Studies* 40, no. 6 (2017): 773-816.

Lansky, Jan. “Possible State Approaches to Cryptocurrencies.” *Journal of Systems Integration* 9, no. 1 (2018): 19-32. https://doaj.org/article/47ca1fef31254a5e8b1c9b62cad59c03.

Lee, Newton. *Facebook Nation: Total Information Awareness*, 2ndeed. New York, NY: Springer Science + Business Media, 2013.

Ludlow, Peter. *Crypto Anarchy, Cyberstates, and Pirate Utopias*. MIT Press, 2001.

Li, Gang, Wenji Niu, Li Guo, Lynn Batten, Yinlong Liu, and Guoyong Cai. “Editorial: Securing Cyberspace.” *Concurrency and Computation: Practice and Experience* 28 (2016): 1870-1871. DOI:10.1002/cpe .3753.

Macdonald, Brennan, and Vassy Kapelos. “Canada Could Threaten U.S. Security by Allowing Huawei into 5G Network, Says U.S. Senator.” *CBC News*, January 3, 2019. Accessed at https://www.cbc.ca /news/politics/powerandpolitics/canada-huawei-5g-tech-risk-us-1.4965297.

Mahbod, Reza, Rob Irish, and Mike Fredrickson. “A Guide to Cybersecurity.” *The Journal of Government Financial Management* 66, no. 3 (2017): 34-39. https://www-lib-uwo-ca.proxy1.lib.uwo.ca/cgi-bin/ezpauthn.cgi?

Maitra, Amit K. “Offensive Cyber-Weapons: Technical, Legal, and Strategic Aspects.” *Environment Systems and Decisions* 35, no. 1 (2014): 169-182. doi:10.1007/s10669-014-9520-7.

Mariscal, Judith. “Prospera Digital Phase II: Financial Inclusion for Low-Income Women in Mexico.” In *International Development Research Centre*, March 13, 2019. https://www.idrc.ca/en/project/prospera-digital-phase-ii-financial-inclusion-low-income-women-mexico.

May, Timothy. “The Crypto Anarchist Manifesto." *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*. 1992.

Mcgregor, Janyce. “Banning Huawei from Canada’s 5G Networks could be Costly for Taxpayers.” *CBC*, February 17, 2019. https://www.cbc.ca/news/politics/huawei-canada-china-fipa 1.5021033?fbclid=IwAR2K41T3cYWrRIR _C71ihiakxxDfNq58u-RhoSlpzlK1Ttule_y8tfoHUfo.

Mejias, Ulises A., and Nikolai E. Vokuev. “Disinformation and the Media: The Case of Russia and Ukraine.” *Media, Culture & Society* 39, no. 7 (2017): 1027-1042.

Miller, Dylan. “How 5G Could Start a Transportation Revolution in Smart Cities.” *IBISWorld*, April 6, 2018. https://www.ibisworld.com/industry-insider/analyst-insights/how-5g-could-start-a-transportation-revolution-in-smart-cities/.

Mims, Christopher. “Who Has More of Your Personal Data Than Facebook? Try Google; Google Gathers More Personal Data than Facebook Does, by Almost Every Measure--so Why Aren’t We Talking about It?” *WSJ Pro. Cyber Security*, 2018.

Mills, Charles W. "Racial Liberalism." *Black Rights/White Wrongs*, (2017): 28-48. doi:10.1093/acprof:oso/9780190245412.003.0003.

Molyneux, Maxine. “Mothers at the Service of the New Poverty Agenda: Progresa/Oportunidades, Mexico’s Conditional Transfer Programme.” *Social Policy & Administration* 40, no. 4 (2006): 425-449.http://resolver.scholarsportal.info/resolve/01445596/v40i0004/425_matsotapmctp.

Moravcsik, Andrew. “Taking Preferences Seriously: A Liberal Theory of International Relations.” *International Organization* 51, no. 4 (1997): 513–553.

Morgenthau, Hans J. *Politics Among Nations: The Struggle for Power and Peace*, 2nd ed. New York: Alfred A. Knopf, 1954.

Morris, Emma. “Children: Extremism and Online Radicalization.” *Journal of Children and Media* 10, no.4 (2016): 508-514. https://journals.scholarsportal.info/details /17482798/v10i0004/508_ceaor.xml.

Motta, Matthew. "The Dynamics and Political Implications of Anti-Intellectualism in the United States." *American Politics Research* 46,no. 3 (2018): 465-498.https://journals.scholarsportal.info/details /1532673x/v46i0003/465_tdapioaitus.xml.

Nguyen-Fredrick, Christine. "Feminist Rhetoric in Cyberspace: The Ethos of Feminist Usenet Newsgroups," *The Information Society* 15, no. 3 (1999): 187-197. doi:10.1080/019722499128493

Nieminen, Hannu. "Digital Divide and Beyond: What do we know of Information and Communications Technology's Long-Term Social Effects? Some Uncomfortable Questions." *European Journal of Communication* 31, no. 1 (2016): 19 -32.

Norden, Lawrence, Ian Vandewalker, and Robert J. Woolsey. "Securing Elections from Foreign Interference." *Securing Elections from Foreign Interference*, 2017. https://www.brennancenter.org/ sites/default/files/publications/Foreign%20Interference_0629_1030_AM.pdf?fbclid=IwAR2bLLM7oB vKHGNoEFT3naJo40TNKhgKAnAKKTig982hrXHRndhwTf0sfNY.

Nye, Joseph. S. Jr. *Power in the Global Information Age: From Realism to Globalization*. London: Routledge: Ch. 7.

Nye, Joseph S. Jr. "The Regime Complex for Managing Global Cyber Activities." In *Centre for Internet Governance Innovation*, May 2014, https://www.cigionline.org/sites/default/files/gcig_paper _no1.pdf.

Obar, Jonathan A., and Andrew Clement, "Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty." *Technology and Emerging Media*, 2013.

Orla, Lynskey. "At the Crossroads of Data Protection and Competition Law: Time to take Stock," *International Data Privacy Law* 8, no. 3 (2018): 179–180.

"Policy Brief: Privacy." In *Internet Society*. October 30, 2015. https://www.internetsociety.org/ policybriefs/privacy/.

Polyakova, Alina, and Spencer P. Boyer. "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition." *EUROPE* (2018).

Popper, Andrew F. "More than the Sum of All Parts: Taking on IP and IT Theft Through a Global Partnership." *Northwestern Journal of Technology and Intellectual Property* 12, no. 4 (2014): 254-290.

Potter, Mitch, Shephard, Michelle. "Canada's Electronic Watchers Enjoy Secrecy Second to None. "*Toronto Star*, November 9, 2013. Accessed at https://www.thestar.com/news/world/2013/11/09/canadas_ electronic_watchers_enjoy_secrecy_second_to_none.html.

Robinson, Bill. "Metadata and Second Parties." *Lux Ex Umbra: Monitoring Canadian Signals Intelligence (SIGNIT) Activities Past and Present,* December 2, 2013. https://luxexumbra.blogspot.com/ 2013/12/metadata-and-second-parties.html.

Robinson, Michael, Kevin Jones, and Helge Janicke. “Cyber warfare: Issues and Challenges.” *Computers and Security* 49 (August 2015): 70-94. https://www.researchgate.net/publication/276248097 _Cyber_warfare_Issues_and_challenges.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. “Do Data Breach Disclosure Laws Reduce Identity Theft?” *Journal of Policy Analysis and Management* 30, no. 2 (2011): 256-286.

Rosamunde van Brakel and Paul De Hert, “Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies.” *Journal of Police Studies* (2011): 163-192.

Rutenberg, Jim. “How ‘Fake News’ Changed The New York Times—and Didn’t.” *The Wilson Quarterly* 42, no. 1 (2018).

Santos Brito, Kellytondos. Vinicius Cardoso Garcia, Frederico Araujo Durao, and Silvio Romero de LemosMeira. “How People Care about Their Personal Data Released on Social Media.” *2013 Eleventh Annual Conference on Privacy, Security and Trust*(2013): 111–18.

Scheau, Mircea Constantin, and Pop Stefan Zaharie. “The Way of Cryptocurrency.” *Economy Informatics* 18, no. 1 (2018): 32-44. https://search.proquest.com/docview/2172009989/ fulltext/A6C9A3BE06904C6FPQ/1?.

Schmitt, Michael N. “‘Virtual’ Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law.” *Chicago Journal of International Law* 19, no. 1 (2018): 30-67.

Schwartz, Matthew J. “Weaponized Bugs: Time For Digital Arms Control.” *Information Week*, March 9, 2019. Accessed athttps://www.darkreading.com/attacks-and-breaches/weaponized-bugs-time-for-digital-arms-control/d/d-id/1106686.

Sciutto, Jim, Jamie Crawford and Chelsea Carter. “ISIS Can Muster Between 20000 and 31500 Fighters, CIA Says.” *CNN,* September 2014. Accessed athttps://www.cnn.com/2014 /09/11/world/meast/isis-syria-iraq/index.html.

Sevastopulo, Demetri, and David Bond. “US and UK Accuse China of Cyber Espionage Campaign.” *Financial Times,* 2018. Accessed at https://www.ft.com/content/f5f0b42c- 046c-11e9-99df-6183d3002ee1.

Shackelford, Scott J. “Business and Cyber Peace: We Need You!” *Business Horizons*59,no. 5 (2016): 539–548. doi:10.1016/j.bushor.2016.03.015.

Shackelford, Scott J. “Cyber Peace.” *Managing Cyber Attacks in International Law, Business, and Relations* 18, no.1 (2017): 1-47. doi:10.1017/cbo9781139021838.012.

Solnik, Claude. “Hackers for Hire.” *Long Island Business News*, October 4, 2018. Accessed at https://libn.com/2018/08/24/hackers-for-hire/.

Srinivas, Jangirala, Ashok Kumar Das, and Neeraj Kumar. “Government Regulations in Cyber Security: Framework, Standards and Recommendations.” *Future Generation Computer Systems* 92, (2019): 178-188.

Steans, Jill. *Gender and International Relations: Issues, Debates and Future Directions*. Polity Press, 2009.

Sudzina, Frantisek. “Distribution of Foreign Aid in Cryptocurrencies: Initial Considerations.” *International Advances in Economic Research* 24, no. 4 (2018): 387-388. http://link.galegroup.com .apps/doc/A563359711/AONE?u=lond95336&sid=AONE&xid=3405f7a3.

Sweden. *The National Security Strategy of Sweden,* 2017*.* Accessed at https://www.government.se/ 4aa5de/contentassets/0e04164d7eed462aa511ab03c890372e/national-security-strategy.pdf.

Syuntyurenko, O. V. “Network Technologies for Information Warfare and Manipulation of Public Opinion.” *Scientific and Technical Information Processing* 42,no. 4 (October 2015): 205-210. https://dl.acm.org/citation.cfm?id=2891214

Tafuri, S. Gallone, M. Cappelli, M. Martinelli, D. Prato, R. and Germinario, C. “Addressing the Anti-Vaccination Movement and the Role of HCWs.” *Vaccine* 32,no. 28 (August 2014): 4860-4865. https://www-sciencedirect-com.proxy1.lib.uwo.ca/science/article/pii/ S0264410X1301505

Tasker, John Paul. “What You Need to Know about the CSIS Metadata Ruling.” *CBC News*, November 05, 2016. Accessed at https://www.cbc.ca/news/politics/what-you-need-to-know-about-csis-metadata-1.3837104.

Thompson, Derek. “The Media’s Post-Advertising Future is Also its Past.” *The Atlantic*, December 31, 2018. Accessed at https://www.theatlantic.com/ideas/archive/2018/12/post-advertising-future-media/578917/.

Tickner, J. Ann. "You Just Don't Understand: Troubled Engagements Between Feminists and IR Theorists." *International Studies Quarterly* 41, no. 4 (1997): 611-632. doi:10.1111/1468-2478.00060.

Tunney, Catherine. “Ottawa setting up a new team to warn Canadians of potential election interference.” *CBC News*, January 30, 2019. Accessed at https://www.cbc.ca/ news/politics/election-interference-panel-1.4998409.

“U.S. Companies Announce 5G Launch Dates, but Canadian Telecoms Stay Mum.” *CBC*, April 1, 2018. Accessed at https://www.cbc.ca/news/business/5g-wireless-technology-launch-dates-1.4601594.

United Nations. “*Operational Guidelines for Cash-Based Interventions in Displacement Settings.”* UNHCR. https://www.unhcr.org/cash-based-interventions.html.

United Nations. *Sustainable Development Goals*, March 13, 2019. https://sustainabledevelopment .un.org/?menu=1300.

United States. Dept. of Homeland Security. Committee on Homeland Security. *Economic Espionage: A Foreign Intelligence Threat to American Jobs and Homeland Security*. Washington, DC: Committee on Homeland Security, 2012.http://www.govinfo.gov/content/pkg/CHRG-112hhrg79843/pdf/CHRG-112hhrg79843.pdf?fbclid=IwAR1-GFgUM-uIWOVK2banIsHZY1d3xbxYI998-PP3gJGvA94BGda1by07iKI.

Valeri, Lorenzo. "Affecting Trust: Terrorism, Internet, and Offensive Information Warfare" *Terrorism and Political Violence 12*,no.1 (2000): 15-26. https://www.tandfonline.com/doi/abs/10.1080 /09546550008427547

Van Brakel, Rosamunde and Paul De Hert, "Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies." *Journal of Police Studies* (2011): 163-192.

Verstraete, Mark, Derek E. Bambauer, and Jane R. Bambauer. "Identifying and Counter Fake News." *Andy Black Associates* (2017).

Waltz, Kenneth N. *Realism and International Politics*. New York: Routledge, 2008.

Wendt, Alexander. "Anarchy is What States Make of It: The Social Construction of Power Politics." *International Organization* 46, no. 2 (1992): 391-425. https://www.jstor.org/stable/2706858.

Wessler, Nathan Freed. "How Private Is Your Online Search History?" *American Civil Liberties Union,* April 26, 2015. https://www.aclu.org/blog/national-security/privacy-and-surveillance/how-private-your-online-search-history.

Xiaoming, Hao, and Chow Kay. "Factors Affecting Internet Development: An Asian Survey." *First Monday* 9, no. 2 (2004).

York, Jillian. "The Arab Digital Vanguard: How a Decade of Blogging Contributed to a Year of Revolution." *Georgetown Journal of International Affairs* 13, no. 1 (2012): 33-42.

Zhang, Yin, and Min Chen. "Cloud Based 5G Wireless Networks." *Cham, Switzerland: Springer International Publishing*, 2016.

Zhao, Long, et al. "Massive MIMO in 5G Networks: Selected Applications." *Washington: Springer*, 2018

Zilber, Neri. "Hackers for Hire: What Happens When the Best Cyberweapons are Controlled by the Private Sector?" *Foreign Policy* 230,(2018): 60-64. http://link.galegroup.com/apps/doc/A556838653/ AONE?u=lond95336&sid=AONE&xid=d8dc27d8.