The Cyber Operations Strategies of the United States and Canadian Governments:

A Comparative Analysis

Scott J. Shackelford

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

Acknowledgements

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This study was produced by an external consultant, contracted to produce studies for the Security and Technology Programme's Cyber Stability workstream, which is funded by the Governments of France, Germany, the Netherlands, Norway, and Switzerland, and by Microsoft. Gratitude is extended to Giacomo Biggio and Giacomo Persi Paoli for offering their thoughts on this research paper; special thanks to Alexandra Sergueeva for her thoughtful research support and for checking references during the drafting of this paper. Parts of this paper have been previously published as Shackelford & Bohm (2016) and Shackelford et al. (2019).

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

About the Author

SCOTT J. SHACKELFORD is Chair of the Cybersecurity Risk Management Program of Indiana University Bloomington, Executive Director of the Ostrom Workshop, and an Associate Professor of Business Law and Ethics at the Indiana University Kelley School of Business.

Photos: © www.https://www.shutterstock.com / p1 graphicINmotion / p2 Orhan Cam / p9 Jean-Claude Caprara / p14 Sharomka / p16 spainter_vfx

TABLE OF CONTENTS

On the Research Paper Series

The number of States possessing the capability to conduct international cyber operations against or through foreign information and communications technology (ICT) infrastructure is on the rise. These cyber operations can signal a mounting large-scale threat to the security of a State, could be understood as a violation of sovereignty, and may lead to an escalation.

To facilitate transparency, advance trust among States, and thus promote stability in international cyberspace, the UNIDIR Security and Technology Programme commissioned a series of research papers outlining national capabilities to conduct international cyber operations and the relevant national doctrines regulating the conduct of such operations. In the resulting papers, nine scholars and practitioners provide an overview of the capabilities and doctrines of 15 States across different regions: Australia, Brazil, Canada, China, France, Germany, India, the Islamic Republic of Iran, Israel, Japan, the Republic of Korea, the Russian Federation, Saudi Arabia, the United Kingdom of Great Britain and Northern Ireland, and the United States of America.

To read more about the research paper series, please refer to the “International Cyber Operations: National Doctrines and Capabilities” paper, available at www.unidir.org/cyberdoctrines.

Andraz Kastelic

Lead Cyber Stability Researcher,
Security and Technology Programme, UNIDIR

Introduction

The United States of America and Canada are interdependent across many dimensions, including the two States' reliance on shared critical infrastructure. As a result, regulatory efforts aimed at securing critical infrastructure in one State have an impact on the other, including in the cybersecurity context. This paper analyses the United States and Canadian cybersecurity strategies, including their treatment of so-called offensive cyber operations, along with relevant national doctrines pertaining to active defence and self-defence.

The concept of offensive cyber operation is interpreted broadly here to include relevant strategies and, where necessary, the policy statements, manuals, and legislation of each State to better inform conclusions. Particular attention is also paid to the role of international law and emerging cyber norms in guiding State practice relating to cyber operations in both the United States and Canada.

United States of America

In many ways, the United States (US) helped to pioneer the field of cybersecurity policy with its enactment of the Computer Fraud and Abuse Act (CFAA) in 1986. This was followed by establishment of the world's first Cyber Emergency Readiness Team (CERT) in response to the 1988 Morris Worm, which caused widespread havoc in the nascent Internet.[1] As US cybersecurity regulation and strategy have evolved over the following 35-year period, notable highlights include the founding of US Cyber Command (USCYBERCOM) in 2009. Still, an integrated approach to US cybersecurity law and policy has largely been lacking, with a veritable "alphabet soup" of agencies from the Department of Homeland Security (DHS) to the Federal Trade Commission (FTC) responsible for various aspects of the nation's cyber defences; the Department of Defense (DOD) alone reportedly operates more than 15,000 networks in 4,000 installations spread across 88 countries.[2]

The modern path of US cybersecurity policy was largely charted in 1998, when President Bill Clinton signed Presidential Decision Directive (PDD) 63.[3] This document marked the birthplace of the US emphasis on public–private partnerships to manage cyber threats to critical infrastructure, along with the sector-specific approach to curtailing those threats such as through the establishment of Information Sharing and Analysis Centers (ISACs).[4] Subsequent administrations have revised this policy: President George W. Bush rescinded it in favour of Homeland Security Policy Directive 7, and the Administration of President Barack Obama made its own revisions. However, throughout these administrations there was widespread agreement that these policies should be "enhanced", not replaced.[5] Now, more than 20 years later and through five successive US presidential administrations from different parties, these lodestars of cybersecurity policy such as the sector-specific, public-private approaches have remained a rare example of bipartisan agreement. However, what has changed more substantially over this timeframe is the offensive–defensive balance of the US national cybersecurity strategy.

US NATIONAL CYBERSECURITY STRATEGY

The US Government has been a leading cyber power for decades. Among other campaigns, it allegedly launched the Stuxnet attack in collaboration with Israel targeting the nuclear enrichment facilities of the Islamic Republic of Iran. The Stuxnet worm

[1] Shackelford (2018).
[2] Lord & Sharp (2011, 12).
[3] Clarke & Singer (2019, 89).
[4] Clarke & Singer (2019, 89).
[5] Clarke & Singer (2019, 89)

exploited vulnerabilities in the Siemens-manufactured centrifuges, particularly the programmable logic controllers (PLCs) in the Natanz plant.[6] Stuxnet marked a watershed moment in the history of cyber conflict for several reasons, including the use of cyberattacks to cause real-world damage; the number of so-called zero-day exploits (i.e. hitherto unknown vulnerabilities in software and operating systems) used in the exploit itself; and a much more activist stance in State-sponsored cybersecurity that showed other established and emerging cyberpowers around the world what was possible. This included the propensity for even sophisticated cyberattacks to cause collateral damage, as happened when Stuxnet jumped to other Siemens PLC systems around the world, infecting everything from traffic lights to nuclear power plants.[7] Still, the Bush Administration viewed the clandestine programme as a success and encouraged the incoming Obama Administration to continue it.[8]

The Obama Administration reacted to the widespread damage caused by Stuxnet in the wild with a new policy (in the form of PDD 20) to curtail the offensive authority of the DOD to launch cyberattacks without prior presidential approval.[9] Instead of leaning forward into active defence doctrine, the Obama Administration instead outlined a policy of cyber deterrence. This was built on the back of the Cybersecurity Framework of the National Institute for Standards and Technology (NIST CSF), which was argued to have a "deterrence-by-denial" benefit. This approach seeks to harden systems against cyber risks by increasing the costs to attackers of attempting to compromise protected networks – by deterring them from expending the necessary time and resources it contributes to overall cybersecurity. In particular, the Obama Administration contended that it would promote the adoption of the NIST CSF as a key means of improving US cyber defenses and, by extension, decreasing adversaries' perceptions of the benefits to be gained from engaging in malicious cyber activities against US computers and networks. Yet US cybersecurity strategy under the Obama Administration was criticized for not being more active in responding to an array of cyberthreats.

The DOD under the Administration of President Donald J. Trump has asserted that previous US cybersecurity strategies were ineffective at meeting the multifaceted cyberthreats facing the United States, particularly in managing cyber conflicts below the threshold of cyberwar. The Trump Administration was highly critical of the Obama Administration's approach to cybersecurity strategy, in particular the concern that adversaries were not being deterred from launching cyberattacks against US networks and interests. Yet, while in office, the Trump Administration's actions in many ways extended and reinforced Obama-era cyber capabilities, with the notable exception of pivoting away from deterrence-by-denial and towards "defend forward".[10] As such, the 2018 DOD Cyber Strategy argued that, along with defending critical infrastructure from significant threats, it is also vital to "[p]ersistently contest malicious cyber activity in day-to-day competition" short of armed conflict.[11] This amounted to a pivot away from a strategy of deterrence-by-denial and towards a renewed active defence doctrine. USCYBERCOM was empowered to achieve this goal without prior presidential approval, including the use of offensive cyberattacks such as the November 2018 takedown of a Russian bot farm.[12] Indeed, USCYBERCOM is now a mature combatant command with more than 130 operational teams. The Trump Administration policy shares characteristics with the more assertive Bush Administration cybersecurity strategy that preceded it.[13] The Trump policy was encapsulated in National Security Presidential Memorandum 13, which clarifies the legal authorities (such as the DOD General Counsel's framework for evaluating the legal sufficiency of proposed military cyber operations and the 2019 National Defense Authorization Act)[14] under which offensive cyberattacks may be launched. In short, it crystallized a "defend forward" approach to cyber operations designed to inhibit any foreign adversary from realizing strategic gains short of armed conflict. There is some evidence that this strategic shift paid some dividends. This may be seen by the United States ranking as the pre-eminent cyber power in the 2020 National Cyber Power Index of the Harvard Belfer Center, due in part to its capacity

[6] Zetter (2015).
[7] Zetter (2012).
[8] Zetter (2012).
[9] Borghard (2018).
[10] Ng (2018).
[11] US Department of Defense (2018, 4).
[12] US Cyber Command (2018); US Senate Committee on Armed Services (2019).
[13] The Bush Administration promoted three main priorities in its cybersecurity strategy stemming from the 2003 National Strategy to Secure Cyberspace: (1) safeguarding critical infrastructure; (2) addressing pervasive vulnerabilities; and (3) enabling the federal government to play a larger role in attributing cyberattacks back to foreign sources, along with aiding in watching and warning networks. Otherwise, it allowed the private sector to take the lead on most cyber incidents. US Government (2003, vii–x).
[14] US Code §394.

of more than 6,000 armed forces personnel tasked with conducting offensive cyber operations from Fort Meade, Maryland.[15]

Specifically, the 2018 DOD Cyber Strategy notes that the US military has to take regular action to protect the competitive advantage of its forces and defend US interests.[16] This includes the collection of intelligence through cyber-enabled means, along with the preparation of military cyber capabilities to be used during crises.[17] In particular, the DOD states in the strategy that it will "defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict".[18] Beyond this shift to defend forward in strategic thinking, the 2018 DOD strategy also continued the Obama Administration's emphasis on deterrence-by-denial by stating that: "We will strengthen the security and resilience of networks and systems that contribute to current and future US military advantages [such as by] collaborat[ing] with our interagency, industry, and international partners to advance our mutual interests".[19] The legal authority for the DOD to engage in this conduct was codified in the 2019 National Defense Authorization Act, which clarified that unacknowledged activities below the threshold of armed conflict are considered to be a legal form of so-called military activities. In response to this, USCYBERCOM has developed a so-called persistent engagement approach, which will allow the United States to engage with its adversaries while avoiding undue escalation.[20]

In short, the 2018 DOD Cyber Strategy may be read as a full-throated endorsement of active defence, saying that the DOD is empowered to employ "offensive cyber capabilities and innovative concepts that allow for the use of cyberspace operations across the full spectrum of conflict".[21] A significant focus of these efforts is the protection of vulnerable critical infrastructure, with the DOD stating that it "seeks to preempt, defeat, or deter malicious cyber activity" targeting these networks.[22] For example, the emphasis of the DOD strategy on defending forward may be read in part as a result of the success of the Russia Small Group, which was established by USCYBERCOM and the National Security Agency (NSA) to protect the 2018 congressional elections. The Russia Small Group demonstrated that persistent engagement and presence can contribute to success, which is why the DOD is now engaging in more information sharing with the private sector. The potential for international cooperation to advance these goals is discussed below.

Many of the core elements of the 2018 DOD Cyber Strategy are echoed in USCYBERCOM's 2018 Command Vision, entitled *Achieve and Maintain Cyberspace Superiority*.[23] Among other core elements, the Command Vision maintains that military superiority on land, at sea, in the air, and in space is critical to protecting US interests, and that the fifth domain of cyberspace is instrumental to security across these related fields. However, the USCYBERCOM vision underscores the uncertainty and associated risks of the United States falling behind its strategic adversaries in cybersecurity capabilities. In particular, the Command Vision singles out vulnerabilities in democratic institutions that may be exploited, and the extent to which hacktivists, criminals, and other non-State groups can work singly or collaboratively to target and exploit these weaknesses. Rather than reaction, the Command Vision underscores the defend forward approach of the DOD Cyber Strategy by maintaining that, given the evolution of cyber-attack capabilities, it is now vital that such attacks be stopped before they are allowed to penetrate US systems and critical infrastructure. To do so effectively, the USCYBERCOM Vision calls for the US military to limit the "freedom of action" of adversaries in cyberspace and to seize the initiative such as by helping to levy sanctions following successful or attempted cyberattacks. In all, the USCYBERCOM Vision argues that a reactive stance will not maintain US cyber superiority, and that instead the US cyber policy framework should reflect "Superiority through Persistence".[24]

[15] Voo et al. (2020, 8); US Cyber Command (n.d.).
[16] US Department of Defense (2018, 1).
[17] US Department of Defense (2018, 1).
[18] US Department of Defense (2018, 1).
[19] US Department of Defense (2018, 1).
[20] US Senate Committee on Armed Services (2019).
[21] US Department of Defense (2018, 1).
[22] US Department of Defense (2018, 2).
[23] US Cyber Command (2018).
[24] US Cyber Command (2018, 6).

These threads are tied together by recent remarks of General Paul Nakasone, the Commander of USCYBERCOM. In 2019, he argued that cyberspace is a different domain than traditional warfare because the United States is in constant contact with its adversaries.[25] Moreover, he argued that, since US security is actively challenged in cyberspace, it must be actively protected. Finally, Nakasone asserted that, since the advantage in cyberspace is fleeting, the initiative must be continually seized. Yet this is easier said than done given that barriers to entry are low in cyberspace and new tools are constantly being invented and repurposed. While with the nuclear advantage, weapons are stockpiled but not used, Nakasone argued that cyber weapons must be used to remain consequential—US adversaries have always been doing this, and it is always below the threshold of armed conflict. He also underscored how attacks have evolved from purely espionage, via disruption, to destructive attacks in cyberspace. There is now the option of launching attacks based on information warfare that influences political campaigns or steals intellectual property. Because of the interconnected nature of networks, partnerships are key to success. Persistent engagement means enabling other stakeholders (such as the Federal Bureau of Investigation, FBI) with information to act, highlighting the importance of inter-agency, international efforts to promote a global culture of cybersecurity referenced above. These remarks were reinforced by the DOD General Counsel, Paul Ney, in 2020. He argued that nearly every cyber tool has an Achilles heel which allows adversaries to take advantage of it. This includes not only military networks and equipment, but also the private sector which provides critical support to military operations. The benefit of cyber operations is that they have a low starting cost—they can be accomplished with a skilled operator, a computer, and a network connection. Because of this, decisions regarding cyberattacks must be made quickly, and the framework behind these decisions must be clearly outlined by the DOD lawyers.[26]

The approach of the Administration of President Joe Biden to active defence specifically and cybersecurity policy in general is still evolving at the time of writing. A flurry of executive actions has included new cybersecurity requirements for federal agencies and critical infrastructure providers on a range of issues including software supply chain security.[27] Together, these elements highlight a renewed focus on deterrence-by-denial through enhanced accountability and implementation of cybersecurity risk; on management best practices; and on deepening public–private partnerships especially with regards to threat intelligence.[28]

RELEVANT LEGISLATION

US law clarifies responsibilities for the leadership of offensive cyber operations. It specifies, for example, that the Secretary of Defense will take the lead on any clandestine military activity in cyberspace, which has been interpreted to be a traditional military activity falling under the 1947 National Security Act.[29] However, the Defense Secretary must update relevant Congressional Armed Services Committees on any and all military cyber activities in quarterly briefings. Additional duties may be entrusted to the Defense Secretary by the President, although the Congressional Armed Services Committees must be notified of any such changes within 15 days of approval. Relatedly, the Defense Secretary must compile an annual report on military cyberspace operations and submit it to the Armed Services Committees. In weighing whether to undertake actions that must be reported, US law requires that the DOD employ all instruments of national power in order to deter or respond in kind to any threat targeting US citizens and residents, democratic processes, critical infrastructure, or the armed forces. The US military is obligated to prioritize denial and deterrence ahead of retaliatory attacking when possible under this balancing act, but in all cases it should extract some cost from the attackers to dissuade similar future incidents.[30]

Yet it is not just the US Government that has engaged in offensive cyber operations; as in other States, there is an active debate underway in the United States about how much leeway to give to private actors in defending their own networks up to and including hacking back.[31] As such, the private sector has become an active player in the active defence debate,

[25] Nakasone (2019).
[26] Ney (2020).
[27] Bitko (2021).
[28] Bitko (2021).
[29] 10 US Code §394.
[30] 10 US Code §394.
[31] This analysis was first published in Shackelford et al. (2019).

even if it is not as public about it. Indeed, one survey at the Black Hat cybersecurity conference found that 36 per cent of respondents admitted to retaliatory hacking, with 13 per cent saying that they did so frequently.[32] The Computer Fraud and Abuse Act, as amended in 2008, criminalizes knowing "unauthorized access" to a computer, "unauthorized transmission" of things like malware (malicious software), damaging a protected computer or network, obtaining and trafficking private information, and affecting the use of a computer (such as by using a computer to form a botnet).[33] One interpretation of the CFAA is that it prohibits companies from accessing networks without authorization – even foreign ones due to the law's extraterritorial reach. Under this viewpoint, more passive measures that do involve the unauthorized access of networks are unlikely to violate the CFAA.[34] But there is also the global context that is worth keeping in mind as many States now have laws similar to the CFAA in force (including Canada, as discussed below). However, the US Department of Justice has yet to bring a single case against a US firm for hacking back in violation of the CFAA. In fact, there have been efforts to allow even greater latitude to the private sector to engage in active defence measures. Under the proposed Active Cyber Defense Certainty (ACDC) Act, for example, firms would be able to operate beyond their network perimeters, including the potential to conduct surveillance on entities "who are thought to have done hacking in the past or who, according to a tip or some other intelligence, are planning an attack".[35] This bill also clarifies "the type of tools and techniques that defenders can use that exceed the boundaries of their own computer network".[36] The bill, for example, would permit defendants the ability to claim "that their activities were just 'active cyber defense measures'" so long as they could prove a "persistent unauthorized intrusion" directed at their computers.[37] In summary, according to Tom Graves, a member of the US Congress, "This is an effort to give the private sector the tools they need to defend themselves".[38] However, as of the time of writing, the bill has not been passed out of committee.

Due to inaction in the US Congress, individual US states have been experimenting with a range of regulatory interventions designed to provide covered firms with greater certainty about the types of cybersecurity best practices, and active defence policies, that are permitted by law. These include laws designed to prohibit unauthorized access, similar to the CFAA, along with laws on data breach notification, anti-phishing laws, and laws designed to decrease the incidents of phishing, denial-of-service (DOS) and distributed DOS (DDOS) attacks, and extortion. The current status of these laws is summarized in Table 1.

[32] nCircle (2012).
[33] 18 US Code §1030; Granick (2009).
[34] Doyle (2010); Messmer (2012).
[35] Schmidle (2018).
[36] Wolff (2017b).
[37] Wolff (2017b).
[38] Schmidle (2018).

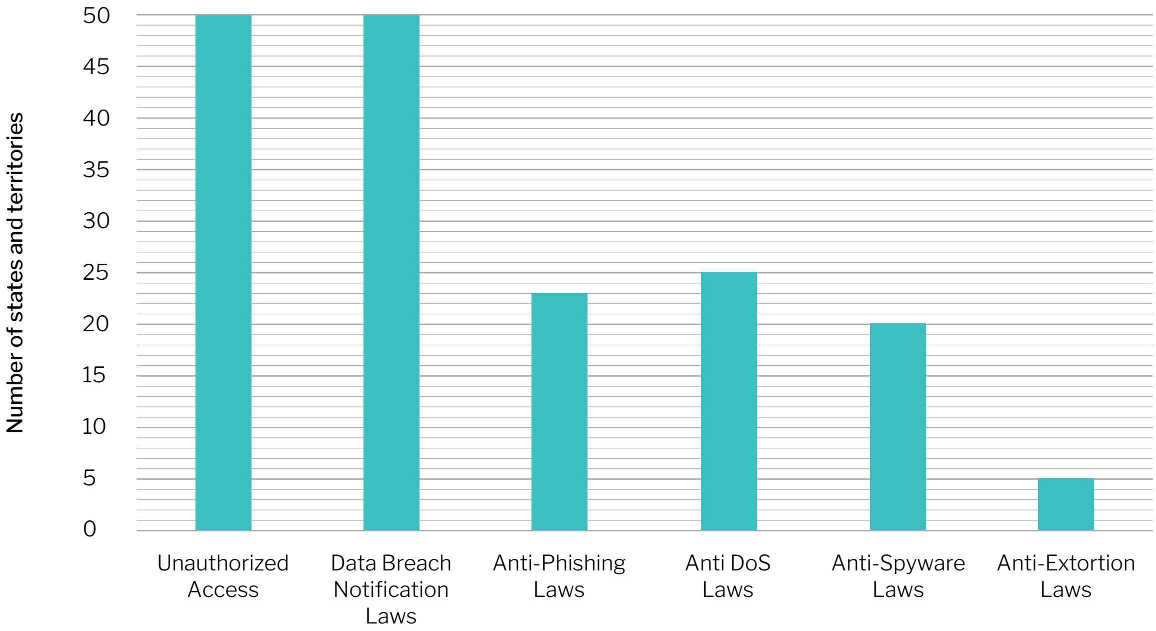
Table 1. Status of State-Level Cybercrime Laws related to Active Defence in the United States

Type of State Law	Coverage	Description
Hacking, Unauthorized Access, Computer Trespass, Viruses, Malware	All 50 states	All 50 states have enacted laws that generally prohibit actions that interfere with computers, systems, programs, or networks.
Data Breach Notification Laws	All 50 states	
Anti-Phishing Laws	23 states and 1 territory: Alabama, Arkansas, Arizona, California, Connecticut, Florida, Georgia, Illinois, Kentucky, Louisiana, Michigan, Minnesota, Montana, New Mexico, New York, Oklahoma, Oregon, Rhode Island, Tennessee, Texas, Utah, Virginia, Washington, and Guam	A total of 23 states and Guam have enacted laws targeting phishing schemes. Many other states have laws concerning deceptive practices or identity theft that may also apply to phishing crimes.
Anti-DOS/DDOS Laws	25 states: Alabama, Arizona, Arkansas, California, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Mississippi, Missouri, Nevada, New Hampshire, North Carolina, Ohio, Oklahoma, Pennsylvania, South Carolina, Tennessee, Virginia, Washington, West Virginia, and Wyoming	
Anti-Spyware Laws	20 states and 2 territories: Alaska, Arizona, Arkansas, California, Georgia, Hawaii, Illinois, Indiana, Iowa, Louisiana, Nevada, New Hampshire, New York, Pennsylvania, Rhode Island, Texas, Utah, Virginia, Washington, Wyoming, Guam, and Puerto Rico	There are 20 states and 2 territories with laws expressly prohibiting use of spyware. Other state laws against deceptive practices, identity theft, or computer crimes in general may be applicable to crimes involving spyware.
Anti-Ransomware Laws/Computer Extortion Laws	5 states: California, Michigan, Connecticut, Texas, and Wyoming	Currently 5 states have statutes that address ransomware, or computer extortion. Other state laws prohibiting malware and computer trespass may be used to prosecute these crimes as well.

Note: These data have been compiled from the National Conference of State Legislature (NCSL) Report on Computer Crime Statutes, http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx#Hacking (last updated 14 June 2018). It should also be noted that, in addition to these laws, 12 states maintain "data security laws", 8 of which include a requirement for firms to implement "reasonable" cybersecurity practices. At least 31 states also have data disposal laws that regulate when and how data is destroyed, including the use of "reasonable measures" to ensure that these data are "unreadable or undecipherable". Kosseff (2017, 49).

As is evident from these data, states have been making progress in regulating cybersecurity even as the US Congress has been more hesitant. This may be seen by the spread of data breach notification laws, which now cover all US states, territories, and Washington, DC.[39] Similarly, unauthorized access (e.g., active defence), anti-phishing, and anti-spyware laws seem to be reaching a tipping point, with nearly half of US states adopting versions of these prohibitions. However, perhaps surprisingly, only a handful of states have laws tackling the ransomware epidemic sweeping the United States.[40] The balance of these laws is illustrated in Figure 1.

Figure 1: Prevalence of select state-level cybersecurity laws in the United States



As for the substance of these statutes, there are various types of state anti-hacking laws that target specific conduct and computer crimes. However, these laws vary tremendously in form and substance. California's regime is among the most holistic. For example, California's Comprehensive Computer Data Access and Fraud Act protects individuals, business, and government agencies from unauthorized access, interference, and damage to computer data and systems, which has influenced other states to implement similar anti-hacking laws.[41] Indeed, such state-level experimentation is having an impact on how other jurisdictions, including States such as Canada, view the issue of active cyber defence, including offensive cyber operations.

[39] Larson (2017).
[40] Ng (2017).
[41] Levine & Haggarty (2016); California Penal Code §502.

Canada

As with the United States, Canada is no stranger to cyberattacks. To take one recent example, the Canadian healthcare sector – including researchers investigating potential COVID-19 vaccines – was "overwhelmed" by a series of cyberattacks targeting hospitals in June 2020.[42] In total, more than 40 million cyberattacks were reported by one Canadian cybersecurity survey in 2014.[43] In response to the myriad of cyberthreats facing Canada's public and private sectors, the Canadian Government has taken a series of mitigating steps, including new investments and the 2018 National Cyber Security Strategy. This strategy has some echoes of the US approach (outlined above), albeit with several notable differences. It has also worked with the US Government to create a number of national and bilateral initiatives to enhance North American cybersecurity, such as the 2012 Canada–US Cybersecurity Action Plan (discussed below).[44] Such actions are in response to the fact that the United States and Canada are interdependent along a number of dimensions, including the two States' reliance on shared critical infrastructure. For example, in 2012, electricity exports from Canada totalled nearly 60 million megawatt-hours, or roughly 1–2 per cent of total US consumption, although certain regions such as the US north-east and Midwest are particularly dependent upon Canadian power.[45] Moreover, Canada's cyber capacity is increasingly recognized as seen by its ranking as the eighth most comprehensive cyber power in the 2020 National Cyber Power Index.[46] However, Canada is ranked eleventh in terms of offensive cyber capabilities.[47]

CANADIAN NATIONAL CYBERSECURITY STRATEGY

On average, each Canadian citizen spends more time online than any other nationality.[48] Much like the United States, the Canadian Government has taken a variety of different approaches to protecting its citizens while they are socializing, shopping, and learning online such as by clarifying cybersecurity frameworks and standards to manage evolving cyber risks. This includes tasking a relatively large number of agencies to manage various aspects of enhancing Canadian cybersecurity. However, a key focal point of Canada's cybersecurity policymaking resides in its Department of Public Safety and Emergency Preparedness (known as Public Safety Canada,

[42] Burke (2020); Nowak (2020).
[43] White (2014).
[44] Public Safety Canada and US Department of Homeland Security (2012).
[45] US House of Representatives Committee on Energy & Commerce (2014).
[46] Voo et al. (2020, 2).
[47] Voo et al. (2020, 36).
[48] Government of Canada (2018).

PSC).[49] PSC has been referred to as the Canadian version of the US Department of Homeland Security; both are responsible for ensuring the cybersecurity of critical infrastructure.[50]

In 2005 the Canadian Government created the Canadian Cyber Incident Response Center (CCIRC) within PSC.[51] The CCIRC was created to help monitor the cybersecurity of both public and private sector networks and critical infrastructure. In this role, the CCIRC is also responsible for leading the Government's response to and recovery from cyberattacks. The CCIRC does this by advising government agencies and private companies on how to prepare for and mitigate cyberthreats, by providing technical expertise such as forensic cyber analysis, and by helping to share and increase collaboration among experts in support of critical Canadian cyber infrastructure. The CCIRC is Canada's version of the CERT that the United States reorganized under the jurisdiction of the DHS in 2003.[52] Both the CCIRC and the US CERT provide the civilian government and private sector with the tools and information they need to be able to stop, respond to, and mitigate cyber risks.[53]

Over the past decade, PSC has published many reports related to cybersecurity and protecting critical infrastructure. These detail what the Canadian Government and private sector must do to improve the cybersecurity of critical infrastructure and how these ideas should be implemented. In 2010, PSC published a National Strategy for Critical Infrastructure and in 2021 an updated Action Plan for Critical Infrastructure for 2021-23.[54] The National Strategy outlines 10 areas of critical infrastructure that are vulnerable to cyberattack (as opposed to the 17 sectors in the United States) and addresses how risks related to these areas of critical infrastructure should be mitigated.[55] It rationalizes that the ultimate responsibility for securing critical infrastructure rests in the hands of the local owners and operators. Based on this notion, the strategy describes a framework for how the Canadian Government plans to share important information and address challenges faced by the local operators and owners of diverse critical infrastructure assets.

In 2010, the PSC also published a report entitled *Canada's Cyber Security Strategy*, which describes the three main objectives of Canadian national cybersecurity strategy: securing government systems, working with the private sector to ensure that non-government systems are secure, and helping the Canadian public browse the Internet safely.[56] In the same year the Government also published an Action Plan for Canada's Cyber Security for 2010–2015 in order to help flesh out the cybersecurity strategy report.[57] Specifically, the Action Plan details what actions need to be taken by different stakeholders to achieve certain cybersecurity goals.[58] The Action Plan for Critical Infrastructure was updated to reflect vital infrastructure protection for the years 2014–2017. This updated Action Plan focuses on how cybersecurity has become increasingly important for critical infrastructure.[59] Many objectives in the updated Action Plan are similar to the NIST Cybersecurity Framework, which is a key way that the Obama and Trump administrations tried to promote cybersecurity due diligence in US critical infrastructure.

In 2018, Canada announced plans to spend a record amount of money on cybersecurity ($431.5 million Canadian dollars over 10 years) to achieve three main objectives: (1) securing government systems, (2) partnering to secure vital cyber systems, and (3) helping Canadians to be secure online. In particular, this funding is being used to support the Canadian Centre for Cyber Security, which aides collaboration between different levels of government and international partners; the creation of the National Cybercrime Coordination Unit; and the fostering of Canadian innovation and cyber talent.[60] The focus on protecting vulnerable critical infrastructure enshrined in the 2018 Canadian National Cyber Security Strategy is similar to the US approach described above, as is the emphasis on public–private partnerships to promote deterrence

[49] Public Safety Canada (2012).
[50] US Department of Homeland Security (2012).
[51] Ballew (2012).
[52] 44 US Code §3546.
[53] Public Safety Canada (2015).
[54] Government of Canada (2010c); Public Safety Canada (2014); Public Safety Canada (2021).
[55] Government of Canada (2010c).
[56] Government of Canada (2010b).
[57] Government of Canada (2010a).
[58] Government of Canada (2010a).
[59] Government of Canada (2014).
[60] Government of Canada (2018).

and due diligence, along with new provisions for both defence and offensive cyber operations in Canada's Communications Security Establishment.[61]

Yet, in comparison with the United States, Canada puts more emphasis on combating cybercrime than on taking action to prevent intrusion by State-sponsored adversaries. In so doing, the Canadian strategy has been more emblematic of the Obama Administration's approach to safeguarding national cybersecurity through deterrence-by-denial, rather than the "defend forward" mantra of the 2018 DOD Cyber Strategy, although there is some evidence that this is starting to change.[62] The Canadian strategy, for example, refers to cyberspace as a "global commons", which is terminology that the US Government also used until the 2018 DOD Cyber Strategy, which does not even reference "commons" once. The distinction is important as it helps define both the end goal – which had been defined by the US International Strategy for Cyberspace as an "open, interoperable, secure and reliable cyberspace" – and the means for attaining it.[63]

RELATED CANADIAN CYBERSECURITY POLICIES AND LEGISLATION

The 2018 Canadian National Cyber Security Strategy was the result of a cyber review undertaken in 2016. The review indicated that Canadians were concerned about their privacy online, and thus wanted to see protections put in place to protect their personally identifiable information.[64] At the same time, one respondent argued: "Privacy and security are not a zero-sum game and we can have both. There is no security without privacy. And liberty requires both security and privacy."[65] Additionally, better cyber hygiene was clearly warranted – from senior citizens to children. This finding extended to the lack of cybersecurity professionals in the Canadian Government and industry, mirroring the cybersecurity workforce shortage in the United States and indeed worldwide. Finally, external partners were shown to want a reliable point of contact for cybersecurity matters; organizations want consistent messaging, standards, and laws for cybersecurity; and stakeholders want to see more international collaboration, information sharing, and safeguards for rights and freedoms.[66] Running throughout the Canadian cyber review, however, was the need to safeguard small and medium-sized businesses against cyberthreats since they often lack the resources to do so effectively.

In 2020, Canada established baseline cybersecurity controls for small and medium-sized organizations, which it has defined as organizations with fewer than 500 employees.[67] These recommendations are meant to combat cybercrime; they are not mandatory, but rather are advice given to organizations to minimize their inherent risk of exposure to cyberattacks. The standards call on organizations to assess the threat level according to the confidentiality, integrity, and availability of data. Organizations are advised to develop an incident response plan, to automatically install patches and updates, to enable security software, to securely configure devices, to use strong user-authentication methods, to back up and encrypt data, and to invest in employee awareness training. In many ways, the list mirrors similar guidance given by the US Federal Trade Commission.[68]

Like the US Computer Fraud and Abuse Act described above, Canadian law also makes certain private sector active defence measures (including hacking back) illegal. Unlike the United States, there is no domestic push underway in Canada to amend these rules to provide greater leeway to the private sector in engaging in active defence measures. Nor does there appear to be a significant political movement pushing for Canada to follow the US defend forward approach. However, it remains unclear how much the US Government is relying on Canada and other Five Eyes members as part of its new cybersecurity stance, although the 2019 National Defense Authorization Act does permit USCYBERCOM to operate outside DOD networks in defence of strategic allies, including Canada, when invited to do so.[69] Table 2 summarizes these Canadian laws and policies, juxtaposed with the US approach.

[61] Government of Canada Public Consultation (2018, 16): "The #1 cyber challenge for Canada is that there are an increasing number of incidents that are causing harm to the economy and society, ranging from breaches, crimes, disruption of essential services, and destruction of corporate and country assets."

[62] Parsons & Gold (2020).

[63] US Government (2011, 3).

[64] Government of Canada (2018).

[65] Government of Canada (2018, 16).

[66] Government of Canada (2018, 16): "Canadian law enforcement should centralize their cybercrime resources ... A single window centre will make it easier for businesses to know who to call when their systems have been compromised, and will help law enforcement investigate and respond to cybercrime across jurisdictions."

[67] Canadian Centre for Cyber Security (2020).

[68] US Federal Trade Commission (2015).

[69] Pomerleau (2019).

Table 2. Canadian and US laws pertaining to active defence by non-State actors

Country	Title of law	Year of law	Relevant Language
Canada	- Criminal Code of Canada §342.1 - Criminal Code of Canada §430(1.1	- 1985 - 1985	- "Everyone is guilty of an indictable offence … who, fraudulently and without colour of right, … obtains, directly or indirectly, any computer service" - "Everyone commits mischief who wilfully a. Destroys or alters computer data; b. Renders computer data meaningless, useless or ineffective; c. Obstructs, interrupts or interferes with the lawful use of computer data; or d. Obstructs, interrupts or interferes with any person in the lawful use of computer data or denies access to computer data to a person who is entitled to access to it"
United States	- USA Patriot Act - Computer Fraud and Abuse Act	- 18 US Code §1030 (2001) - 18 US Code §1030 (1984, last updated 2008)	- This amended US law on computer fraud to pertain to "a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States" - The CFAA regulates those who "intentionally accesses a computer without authorization or exceeds authorized access" (§1030(a)(2)) - The US Department of Justice has noted that "[t]he term 'without authorization' is not defined by the CFAA" - The term "exceeds authorized access" is defined to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter" (§1030(e)(6))

Table 2. Canadian and US laws pertaining to active defence by non-State actors (continued)

Law	Year	Relevant Language
Canada		
Criminal Code of Canada §342.1	1985	• "Everyone is guilty of an indictable offence … who, fraudulently and without colour of right, … obtains, directly or indirectly, any computer service"
Criminal Code of Canada §430(1.1)	1985	• "Everyone commits mischief who wilfully (a) Destroys or alters computer data; (b) Renders computer data meaningless, useless or ineffective; (c) Obstructs, interrupts or interferes with the lawful use of computer data; or (d) Obstructs, interrupts or interferes with any person in the lawful use of computer data or denies access to computer data to a person who is entitled to access to it."
United States		
USA Patriot Act (18 US Code §1030)	2001	• This act amended US law on computer fraud to pertain to "a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States"
Computer Fraud and Abuse Act (8 US Code §1030)	1984 (last updated 2008)	• The CFAA regulates those who "intentionally accesses a computer without authorization or exceeds authorized access" (§1030(a)(2)) • The US Department of Justice has noted that "[t]he term 'without authorization' is not defined by the CFAA" • The term "exceeds authorized access" is defined to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter" (§1030(e)(6))

Opportunities for multilateral engagement

Building on the 2012 Cybersecurity Action Plan agreed by Public Safety Canada and the US Department of Homeland Security, in 2015 PSC and the DHS began coordinating a joint effort to further the resilience of shared critical infrastructure systems.[70] Among other things, the 2015 Action Plan calls for deeper integration of US-Canadian national cybersecurity activities and more collaboration with the private sector. It also recognizes that, as the Internet has no borders, it is the responsibility of all States to respond to cyberattacks to make sure that it is a safe space for all their citizens.

Despite this agreement, there was a growing divergence in cybersecurity law and policy between the United States and Canada during the Trump Administration. The defend forward approach of the US DOD has been partly followed, but not mirrored, by Canadian policymakers.[71] Similarly, while Canada signed the Paris Call for Trust and Security in Cyberspace, which calls for the banning of private sector active defence measures, the United States is the only member of the Five Eyes that has not signed on. The Paris Call is a multi-stakeholder statement of principles designed to help guide the international community towards greater cyber stability, and perhaps one day cyber peace (also known as digital peace). In particular, the agreement calls for action to safeguard civilian infrastructure and Internet access, and for the international community to "[t]ake steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors" – that is, to prevent aggressive active defence.[72] Since it was launched in November 2018, the Paris Call has been signed by 706 companies, 391 organizations and members of civil society, and 79 States (with the notable exception of the United States).[73] Moreover, Canada has called for additional clarity on how international law "puts guardrails on states' behaviour" in cyberspace, including with regards to due diligence.[74]

As of the time of writing, Canada has not published its views on how international law applies to cyber operations, as part of the ongoing United Nations processes. However, the Biden Administration has stated how international law applies to cyber operations both above and below the armed attack threshold.[75] Among other things, the US statement underscores the respect for the sovereign equality of States, along

[70] Public Safety Canada and US Department of Homeland Security (2015).
[71] Pomerleau (2019).
[72] Paris Call for Trust and Security in Cyberspace (2018).
[73] Sanger (2018b).
[74] Government of Canada (2019a); Government of Canada (2019b).
[75] United Nations General Assembly (2021).

with human rights protections, which it suggests places limits on sovereign activities in cyberspace. These scenarios could include the norm of non-intervention in the internal affairs of other States, such as never targeting electoral systems or public health infrastructure.[76]

What role can active defence play in a global culture of cybersecurity? Critics abound. According to Patrick Lin, a professor of philosophy at California Polytechnic State University, "It is much too premature to allow for hacking back, even if the practice isn't immoral ... At minimum, there needs to be a clear process to authorize or post-hoc review cyber counterattacks to ensure they're justified, including penalties for irresponsible attacks. That oversight infrastructure hasn't even been sketched out."[77]

Further, proposed US legislation such as the ACDC Act threatens to deepen this growing divide. As argued by Nicholas Schmidle in the *New Yorker*, "Should hacking back become legal, it may well help individual victims of cybercrime, but it is unlikely to make the Internet a safer place."[78] This view is shared by Chris Cook of the US Department of Justice, who said, "the crucial question policymakers should be asking is whether we are comfortable allowing foreign actors/private entities to do on our own networks what we are proposing to authorize on theirs".[79] Such a destabilizing development would curtail efforts aimed at establishing international cybersecurity norms, as James Lewis of the Center for Strategic and International Studies among others has argued, potentially leading to "an abandonment of US efforts to establish international norms against this type of activity".[80]

The emerging international norm against aggressive active defence does not mean that proactive cybersecurity – especially on the passive side of the active defence spectrum – is not essential to building resilience and due diligence across vulnerable critical infrastructure sectors. In fact, such a "lean in" approach to cybersecurity is essential to help guard against the more reactive mindset that has long bedevilled the field of cybersecurity risk management. Indeed, more firms seem to be embracing this proactive viewpoint, as seen in the Cybersecurity Tech Accord, across the Group of Seven (G7), and in all 50 US states – even as there is continued strong resistance to this change in mindset from the technology community.[81] As the political winds shift, and more firms suffer from cyberattacks that governments have so far failed to stop, passive active defence may well become more mainstream in more States. However, it remains an open question whether some combination of public and private sector offensive measures will meaningfully contribute to deterrence and a global culture of cybersecurity. Commentators including Richard Clarke and Robert Knake think not, arguing for the promotion of cyber resilience.[82] Others favour a "cyber moonshot" or Manhattan Project level of investment to harden systems.[83] Clearly, both deterrence-by-denial and active defence have their place, but growing divides between close allies threaten to add new fissures to an already increasingly fractured cyberspace.

[76] United Nations General Assembly (2021).
[77] Wolff (2017a).
[78] Schmidle (2018).
[79] Cook (2017).
[80] Cook (2017).
[81] Shackelford et al. (2019).
[82] Clarke & Knake (2019).
[83] Sanger (2018a).

Conclusion

In a special report on North America for the Council on Foreign Relations (CFR), a task force stated of the interconnection between the North American economies that "Cyber failures in one country could have ripple effects on neighbors and cross-border production", and it "recommends that the United States, Canada, and Mexico set baseline standards for cyber protection".[84] The NIST Cybersecurity Framework is certainly one candidate for such an undertaking, but it is not alone. There are other cybersecurity frameworks worth pursuing, such as those drawn from the Critical Security Controls and the US DHS Continuous Diagnostics and Mitigation Program to promote cyber hygiene.[85]

Moreover, the CFR report recommended several of the measures discussed in this paper, including deeper integration of national CERTs as well as robust international public–private information sharing. Indeed, these conclusions build on the US–Canadian Cybersecurity Action Plan, which, among other things, deepens cooperation between US and Canadian cyber emergency response teams and calls for more robust private-sector information sharing and better "public awareness" of the multifaceted cyberthreat.[86] Over time, such efforts may morph into a combined North American CERT and information sharing and analysis organization.

A more assertive "defend forward" cybersecurity strategy was not on the list of recommendations of the CFT task force, but for the time being it seems ingrained in US strategic thinking and, as a result, to some extent those of its allies including Canada. Still, by leveraging the resources available in the United States and Canada, both States may be able to more effectively meet the evolving cyberthreat than has been the case to date. In the process, they may help secure North American critical infrastructure and positively contribute to some measure of a global cyber peace.

[84] Petraeus & Zoellick (2015, 80).
[85] Petraeus & Zoellick (2015, 80).
[86] Public Safety Canada and US Department of Homeland Security (2015, 2–4).

References

Ballew, Steven. 2012. 'U.S. Can Learn from Canadian Cybersecurity Shortcomings.' *Daily Signal*, 5 November 2012. As of 19 October 2021: http://dailysignal.com/2012/11/05/u-s-can-learn-from-canadian-cybersecurity-shortcomings.

Bitko, Gordon. 2021. 'The Emerging Biden Administration Cyber Strategy.' *Forbes*, 9 June 2021. As of 19 October 2021: https://www.forbes.com/sites/gordonbitko/2021/06/09/the-emerging-biden-administration-cyber-strategy/?sh=6c07fb7c61e0.

Borghard, Erica. 2018. 'What Do the Trump Administration's Changes to PDD-20 Mean for U.S. Offensive Cyber Operations?' Council on Foreign Relations, 10 September 2018. As of 19 October 2021: https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations.

Burke, David. 2020. 'Hospitals "Overwhelmed" by Cyberattacks Fueled by Booming Black Market.' CBC, 2 June 2020. As of 19 October 2021: https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422.

Canadian Centre for Cyber Security. 2020. *Baseline Cyber Security Controls for Small and Medium Organizations:* As of 19 October 2021: https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations.

Cherry, Steven. 2010. 'How Stuxnet is Rewriting the Cyberterrorism Playbook.' *IEEE Spectrum*, 13 October 2010. As of 19 October 2021: https://automationation.wordpress.com/2010/11/08/how-stuxnet-is-rewriting-the-cyberterrorism-playbook.

Clarke, R. & R. Knake. 2019. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*, New York: Penguin.

Cook, Chris. 2017. 'Hacking Back in Black: Legal and Policy Concerns with the Updated Active Cyber Defense Certainty Act.' *Just Security*, 20 November 2017. As of 19 October 2021: https://www.justsecurity.org/47141/hacking-black-legal-policy-concerns-updated-active-cyber-defense-certainty-act.

Doyle, Charles. 2014. 'Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws.' Congressional Research Service. As of 19 October 2021: https://sgp.fas.org/crs/misc/97-1025.pdf.

Government of Canada. 2010a. *Action Plan 2010–2015 for Canada's Cyber Security Strategy.* As of 19 October 2021: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf.

— — —. 2010b. Please see https://unidir.org/sites/default/files/2021-06/Cyber%20Briefing%20Series%20-%20Paper%202%20-%20Final.pdf for guidance. *Cyber Security Strategy.* As of 19 October 2021: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.

— — —. 2010c. *National Strategy for Critical Infrastructure.* As of 19 October 2021: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.

— — —. 2018. *National Cyber Security Strategy.* As of 19 October 2021: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.

— — —. 2019a. ‘Statements by Canada During the Informal Consultative Meeting of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security’. 5–6 December 2019. As of 19 October 2021: https://www.un.org/disarmament/wp-content/uploads/2020/01/statements-canada-informal-consultative-meeting-gge-5-6-december.pdf.

— — —. 2019b. ‘Canada’s Implementation of the 2015 GGE Norms’. As of 19 October 2021: https://www.un.org/disarmament/wp-content/uploads/2019/11/canada-implementation-2015-gge-norms-nov-16-en.pdf.

Granick, Jennifer. 2009. ‘Amendments to Computer Crime Law Are a Dark Cloud with a Ray of Light.’ Electronic Frontiers Foundation, 15 June 2009. As of 19 October 2021: http://www.eff.org/deeplinks/2009/06/amendments-computer.

Kosseff, Jeff. 2017. *Cybersecurity Law*, New York: Wiley.

Larson, Selena. 2017. ‘Senators Introduce Data Breach Disclosure Bill.’ CNN, 1 December 2017. As of 19 October 2021: http://money.cnn.com/2017/12/01/technology/bill-data-breach-laws/index.html.

Levine, J. & H. Haggarty. 2016. ‘California Online Privacy Laws: The Battle for Personal Data.’ *Competition*.

Lord, K. & T. Sharp, eds. 2011. *America’s Cyber Future: Security and Prosperity in the Information Age*, Washington, DC: CNAS.

Messmer, Ellen. 2012. ‘Hitting Back at Cyberattackers: Experts Discuss Pros and Cons.’ Networkworld, 1 November 2012. As of 19 October 2021: https://www.networkworld.com/article/2161144/hitting-back-at-cyberattackers--experts-discuss-pros-and-cons.html.

Nakasone, Paul. 2019. ‘An Interview with Paul M. Nakasone.’ *Joint Forces Quarterly* 92(1): 4–9.

nCircle. 2012. ‘Black Hat Survey: 36% of Information Security Professionals Have Engaged in Retaliatory Hacking.’ *Business Wire*, 26 July 2012. As of 19 October 2021: https://www.businesswire.com/news/home/20120726006045/en/Black-Hat-Survey-36-Information-Security-Professionals.

Paul, Ney. 2020. ‘DOD General Counsel Remarks at U.S. Cyber Command Legal Conference.’ *U.S. Cyber Command Legal Conference*.

Ng, Alfred. 2017. ‘The Global Ransomware Epidemic is Just Getting Started.’ CNET, 28 June 2017. As of 19 October 2021: https://www.cnet.com/news/petya-goldeneye-wannacry-ransomware-global-epidemic-just-started.

— — —. 2018. ‘Trump Did Not “Inherit a Cyber Crisis,” Obama’s Cybersecurity Czar Says.’ CNET, 2 August 2018. As of 19 October 2021: https://www.cnet.com/news/trump-did-not-inherit-a-cyber-crisis-obamas-cybersecurity-czar-says.

Nowak, Peter. 2020. ‘Canada a Target for Cyberattacks on COVID-19 Research.’ *Globe & Mail*, 18 June 2020. As of 19 October 2021: https://www.theglobeandmail.com/featured-reports/article-canada-a-target-for-cyberattacks-on-covid-19-research.

Paris Call for Trust and Security in Cyberspace, 12 November 2018. As of 19 October 2021: https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf.

Parsons, C. & J. Gold. 2020. ‘A Deep Dive into Canada’s Overhaul of its Foreign Intelligence and Cybersecurity Laws.’ *Just Security*, 2 June 2020. As of 19 October 2021: https://www.justsecurity.org/70519/a-deep-dive-into-canadas-overhaul-of-its-foreign-intelligence-and-cybersecurity-laws.

Petraeus, David H. & Robert B. Zoellick (chairs). 2015. *North America:* Time for a New Focus, Independent Task Force Rep. No. 71. Council on Foreign Relations.

Pomerleau, Mark. 2019. ‘Here’s How Cyber Command is Using “Defend Forward”.’ *Fifth Domain*, 12 November 2019. As of 19 October 2021: https://www.fifthdomain.com/smr/cybercon/2019/11/12/heres-how-cyber-command-is-using-defend-forward.

Public Safety Canada. 2012. ‘Cyber Security: A Shared Responsibility’. As of 19 October 2021: http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/index-eng.aspx.

— — —. 2014. ‘Critical Infrastructure’. As of 19 October 2021: http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-eng.aspx.

— — —. 2015. ‘Cyber Security Incident Response Teams’. As of 19 October 2021: http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-prtnrs-eng.aspx.

— — —. 2021. 2021-2023 Action Plan for Critical Infrastructure. As of 19 October 2021: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/2021-ctn-pln-crtcl-nfrstrctr-en.pdf.

Public Safety Canada and US Department of Homeland Security. 2012. Cybersecurity Action Plan. As of 19 October 2021: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/cybrscrt-ctn-plan-eng.pdf.

— — —. 2015. Cybersecurity Action Plan. As of 19 October 2021: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-en.aspx.

Sanger, David. 2018a. *The Perfect Weapon*, New York: Crown.

— — —. 2018b. ‘U.S. Declines to Sign Declaration Discouraging Use of Cyberattacks.’ *New York Times*, 12 November 2018. As of 19 October 2021: https://www.nytimes.com/2018/11/12/us/politics/us-cyberattacks-declaration.html.

Schmidle, Nicholas. 2018. ‘The Digital Vigilantes Who Hack Back’. *New Yorker*, 7 May 2018. As of 19 October 2021: https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back.

Shackelford, Scott & Z. Bohm. 2016. ‘Securing North American Critical Infrastructure: A Comparative Case Study in Cybersecurity Regulation.’ *Canada–U.S. Law Journal* 40: 61–70.

Shackelford, S. 2018. ‘30 Years Ago, the World’s First Cyberattack Set the Stage for Modern Cybersecurity Challenges.’ *Conversation*, 1 November 2018. As of 19 October 2021: https://theconversation.com/30-years-ago-the-worlds-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges-105449.

Shackelford, S., D. Charoen, T. Waite & N. Zhang. 2019. ‘Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking.’ *University of Pennsylvania Journal of International Law*, 41: 377–427.

United Nations General Assembly. 2021. Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly Resolution 73/266 (2021). UN Document: A/76/136, 13 July 2021.

US Cyber Command. n.d. “Our History”. As of 19 October 2021: https://www.cybercom.mil/About/History.

— — —. 2018. *Achieve and Maintain Cyberspace Superiority:* Command Vision for US Cyber Command. As of 19 October 2021: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

US Department of Homeland Security. 2012. 'Safeguard and Secure Cyberspace'. As of 19 October 2021: http://www.dhs.gov/safeguard-and-secure-cyberspace.

US Department of Defense. 2018. *Cyber Strategy: Summary*. As of 19 October 2021: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

US Federal Trade Commission. 2015. *Start with Security: A Guide for Business*. As of 19 October 2021: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

US Government. 2003. *The National Strategy to Secure Cyberspace*. White House, February 2003. As of 19 October 2021: https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.

— — —. 2011. *International Strategy for Cyberspace*. As of 19 October 2021: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

US House of Representatives Committee on Energy & Commerce. 2014. 'North American Energy Infrastructure Act Will Bolster U.S.–Canada Electricity Relationship.' 7 May 2014. As of 19 October 2021: https://republicans-energycommerce.house.gov/news/press-release/north-american-energy-infrastructure-act-will-bolster-us-canada.

US Senate Committee on Armed Services. 2019. "Review Testimony on United States Special Operations Command and United States Cyber Command in Review on the Defense Authorization Request for Fiscal Year 2020 and the Future Years Defense Program". Hearing, 14 February 2019. As of 19 October 2021: https://www.armed-services.senate.gov/imo/media/doc/19-13_02-14-19.pdf.

Voo, J., I. Hemani, S. Jones, W. DeSombre, D. Cassidy & A. Schwarzenbach. 2020. *National Cyber Power Index 2020*. Harvard Kennedy School, Belfer Center for Science and International Affairs, September 2020. As of 19 October 2021: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.

White, Samantha. 2014. 'Global Cyber-Attacks Up 48% in 2014.' *CGMA Magazine*, 8 October 2014. As of 19 October 2021: http://www.cgma.org/Magazine/News/Pages/201411089.aspx.

Wolff, Josephine. 2017a. 'When Companies Get Hacked, Should They Be Allowed to Hack Back?' *The Atlantic*, 14 July 2017. As of 19 October 2021: https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679.

— — —. 2017b. 'Attack of the Hack Back.' *Slate*, 17 October 2017. As of 19 October 2021: http://www.slate.com/articles/technology/future_tense/2017/10/hacking_back_the_worst_idea_in_cybersecurity_rises_again.html.

Zetter, Kim. 2012. 'Report: Obama Ordered Stuxnet to Continue After Bug Caused It to Spread Wildly.' *Wired*. As of 19 October 2021: https://www.wired.com/2012/06/obama-ordered-stuxnet-continued.

— — —. 2015. *Countdown to Zero Day: Stuxnet and the Launch of het World's First Digital Weapon*. New York: Broadway Books.

The Cyber Operations Strategies of the United States and Canadian Governments:

A Comparative Analysis

This paper analyses the United States and Canadian cybersecurity strategies, including their treatment of so-called offensive cyber operations, along with relevant national doctrines pertaining to active defence and self-defence. The concept of offensive cyber operation is interpreted broadly here to include relevant strategies and, where necessary, the policy statements, manuals, and legislation of each State to better inform conclusions. Particular attention is also paid to the role of international law and emerging cyber norms in guiding State practice relating to cyber operations in both the United States and Canada.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH