Coalition Strategic Cyber Campaigns: Functional Engagement as Cyber Doctrine for Middle Power Statecraft

Joseph Szeman
Christian Leuprecht

INTRODUCTION

The volatile geopolitical environment, a resurgence of interstate conflict, erosion of multilateral institutions, and diplomatic, information, military, and economic competition put the rules-based international order at risk. The cyber domain is a microcosm of geopolitical rivalry among adversarial state actors, competing political systems and visions of the international political order. Both state and non-state actors have extended instability and competition into cyberspace by exploiting global dependence on information and communication technologies (ICT), consistently and at scale, to advance their national interests and degrade those of their rivals, short of the threshold of armed conflict.[1] Between 2005 and 2022, China, Iran, North Korea, and Russia sponsored nearly 77 percent of suspected operations.[2] The same malicious actors orchestrated over 80 percent of adversarial cyber campaigns recorded between 2000 and 2020.[3] As geopolitical rivalries escalate and societies become ever-more reliant on ICTs, the exploitation of cyberspace for strategic gain is sure to increase.

The expanding use of cyber operations amid broadening geopolitical instability has particular implications for traditional middle powers, notably Canada, Australia, Norway, and the Netherlands, among others. They occupy privileged positions at the core of the global political economy but have limited ability to shape the geopolitical environment and few resources to protect and project their national interests. Many of the world's most influential middle powers are also longstanding U.S. allies, have high levels of digital connectivity, strong knowledge-based economies, leading research institutions, and membership in coveted multilateral groupings and security alliances. Compounded by their hard-power resource constraints, for adversaries, middle powers represent low-risk, high-reward targets for exploitation in cyberspace. Middle powers thus have

Joseph Szeman is a political studies and history graduate of Queen's University at Kingston, where he has conducted research on strategic culture, deterrence, and coercion in cyberspace.

strong incentives but limited capacity to prevent the cyber-enabled degradation of their sovereignty, stability, and economic competitiveness.

How should middle powers respond to adverse changes in their environment resulting from a weakened rules-based international order and unrestricted cyber activity targeting its interests and instruments of national power? Albert Hirschman's classic book *Exit, Voice, and Loyalty* posits a framework for agency to act on consequential change: an actor can *exit*, use *voice*, or demonstrate *loyalty*.[4] By choosing to *exit*, an actor accepts the undesirable change in its environment and alters its behavior to adapt to the new situation.[5] For example, a middle power could respond to cyber activity that undermines its interests by abandoning its status and role as a middle power, which would downgrade its international standing and influence. Choosing *loyalty* means the actor accepts the undesirable change in their environment but does not alter their behavior.[6] In this case, a middle power accepts the changes to its environment and the resulting threats to its interests by not altering its response, instead choosing to maintain the status quo of its current efforts in cyberspace. This article contends that a *loyalty* response, which characterizes current multilateral efforts to develop explicitly accepted cyber norms, has not (and will not) provide middle powers with an effective solution to the increasing threats they face from malicious state-sponsored cyber activity. Lastly, Choosing *voice* means taking deliberate action to revert the environment to its original condition.[7] For example, a middle power could attempt to reverse changes to its environment, asserting itself in and through cyberspace by devising strategies to uphold the international order, advance its interests, and protect its sovereignty.

There are few lessons to be drawn from existing scholarship, which examines the cyberspace doctrine

Christian Leuprecht is Class of 1965 Distinguished Professor in Leadership, Department of Political Science and Economics, Royal Military College, Editor-in-Chief of the *Canadian Military Journal*, Director of the Institute of Intergovernmental Relations in the School of Policy Studies at Queen's University, senior fellow at the Macdonald Laurier Institute, and Adjunct Research Professor in the Australian Graduate School of Policing and Security, Charles Sturt University.

and operations of only a handful of great powers and authoritarian states. Comparatively, there is a dearth of research on the roles, incentives, activities, and ambitions of other states in cyberspace–particularly traditional middle powers, which differ from great powers in intent, capability, and opportunity. Moreover, existing approaches to leveraging operations in cyberspace as a tool of statecraft have not been developed with the characteristics, incentives, and resources of middle powers in mind, which makes them ill-suited to being readily adopted and operationalized by those countries.

Absent a cyber doctrine tailored to their unique geopolitical realities, middle powers are likely accumulating a strategic cyberspace-deficit relative to potential adversaries that have more readily grasped the opportunity space offered by the strategic use of cyber operations. This article aims to fill this gap: how should middle powers respond to deleterious changes in their geopolitical (and cyberspace) environments? By means of coalition cyber strategy campaigns: proactively shaping the boundaries of adversarial cyber activity as a *voice* strategy to participate more actively and effectively in efforts to develop cyber norms. This strategy, tentatively termed "functional engagement," draws on and modifies research on cyber persistence theory and the cyberspace strategy of persistent engagement in response to the resource constraints and strategic interests of middle powers.

First, this article describes the broad constitutive characteristics of middle powers. The first section contextualizes the unique foreign policy interests of middle powers and identifies what types of middle powers would benefit most from a strategy of functional engagement. To illustrate the challenges facing middle powers that seek to pursue a loyalty-based approach, the second section broadly outlines the failures of multilateral efforts to establish explicitly accepted cyber norms. The third section describes the contours of

cyber persistence theory and argues that, as a complement to ongoing multilateral efforts, the boundaries of tacitly acceptable state behavior in cyberspace, and potentially even in the wider geopolitical environment, can be cumulatively shaped by employing cyber operations in response to unacceptable behavior (the voice approach). The fourth section illustrates the point: it draws on traditional middle powers that are vulnerable to exploitation in cyberspace yet have limited resources to respond in order to formulate the concept of functional engagement as an approach tailored to middle powers. This section posits functional engagement as an alternative strategy, using Canada as a critical case study, given its geopolitical identity as a middle power, the threats emanating from cyberspace, and the relatively limited resources at its disposal.

THE CHARACTERISTICS OF MIDDLE POWERS

Analysts had initially bifurcated the international community into small and great state powers, but it soon became apparent that some small states were more powerful than others. Relative strength was to be recognized in the form of a "scheme of gradation," which, in the 1930s, gave rise to the concept of "middle powers."[8] The concept gained momentum thanks to the concerted diplomatic efforts of Canada and Australia to justify and solidify their international influence and core roles in the post-1945 global order.[9] In 1947, Canadian diplomat and historian George Glazebrook asserted that the formation of the United Nations would enable "middle powers" to be "capable of exerting a degree of strength and influence not found in the small powers."[10] A growing number of states have since either self-identified or been described by others as middle powers, including: Argentina, Australia, Canada, Brazil, Denmark, Japan, Malaysia, the Netherlands, Norway, Nigeria, Spain, Sweden, South Korea, and Turkey.[11] Although the question of what constitutes the attributes of a middle power is controversial, international relations scholars generally identify at least three useful theoretical perspectives: hierarchical, functional, and behavioral.[12]

First, the hierarchical approach categorizes states by measuring objective capability, asserted position, and recognized status.[13] It typically ranks states according to economic, military, or social metrics.[14] Their capabilities, international standing, or status rank these states in the "middle" of the international system: greater than those of small states but lesser than great powers. To explain the unique foreign policy behavior of middle powers, functional and behavioral approaches take the middle power concept further, beyond the status of a mere tool for ranking real capability.

The functional perspective argues that middle powers may on occasion exert influence in international affairs in specific instances based on their relative capabilities, interests, and degree of involvement.[15] By contrast, great powers are always capable of exercising international influence, while lesser states (than middle powers) are unable to exert real influence.[16] At the core of the functional concept is the idea that a state with relatively limited military

and economic capacity may nonetheless be successful in accruing "degrees of influence and authority among great powers and its neighbors that even reach into global forums."[17] This view holds that middle powers commit to maintaining the status quo, security, and order in the international system through leadership on specific global problems and foreign policy niches of their choosing.[18]

Lastly, the behavioral approach is the dominant contemporary paradigm for characterizing foreign policy behavior by middle powers. Sometimes also referred to as the middle power internationalist approach, the behavioral approach contends that a country is a middle power if it exhibits a certain type of foreign policy behavior—namely, advocating for compromise and seeking multilateral solutions to international problems.[19] Within this understanding, middle powers rely on international law to ensure predictability in global interactions, and on international organizations to provide forums through which they can establish and enforce acceptable conduct. To this end, middle powers focus their foreign policy efforts on global normative arrangements promoted through international organizations.[20] Accordingly, the behavioral approach reflects a "particular style of diplomacy, or a strategy backed by a commitment to liberal values and the absence of unilateralism which is a defining trait of a great power."[21]

The behavioral approach parses into "traditional" and "emerging" middle powers.[22] Traditional middle powers are "wealthy, stable, egalitarian, social democratic and not regionally influential," exhibit "a weak and ambivalent regional orientation," and offer appeasing concessions to pressures for global reform": Australia, Canada, Norway, and the Netherlands are examples of traditional middle powers.[23] In contrast, emerging middle powers are semi-peripheral to the core of the global political economy, "materially inegalitarian and recently democratised states that demonstrate much regional influence and self-association" and that seek to reform the global order. Examples of emerging middle powers include Argentina, South Africa, Malaysia, and Turkey.[24] Both traditional and emerging middle powers benefit from the status quo of the current liberal international order.[25] However, lacking in capacity to alter the global balance of power or affect deep change in the international system, both types of middle powers are vulnerable to global instability that threatens to upend the status quo. Traditional middle powers, therefore, seek to legitimize and stabilize the international order since they already occupy privileged positions at the core of the global political economy. In essence, their interests are best asserted by defending and upholding the status quo of this order. Whereas emerging middle powers may benefit from their regional economic dominance within the international order, they do not occupy privileged positions within the global political economy and thus have an incentive to transform the international order.

Although the constitutive features of middle powers are up for debate, common to all three approaches is an understanding that middle powers have limited economic or military capabilities and are capable of exerting only narrow influence in the international system

(the hierarchical perspective). To address these challenges and participate in foreign affairs, middle powers focus their resources on specific, relevant issues (the functional perspective), or towards enhancing their influence through explicit bargaining processes, conflict management, and multilateralism (the behavioral perspective). The distinction between traditional and emerging middle powers is a function of divergent interests and incentives. As legitimizers and stabilizers of their privileged role within the current global order, traditional middle powers in particular stand to face the most significant disruption from contemporary threats to the established rules-based international order—including from cyberspace. Owing to their roles within in the international system, they have a particular incentive to address cyber threats.

THE LOYALTY APPROACH AND THE ISSUE OF MULTILATERAL EFFORTS TO DEVELOP "CYBER NORMS"

In principle, the deteriorating stability of cyberspace makes the diffusion of transnational norms to regulate the behavior of state actors in cyberspace appealing to great and middle powers alike. Over the years, these efforts have taken a multilateral shape, touching numerous organizations, including the United Nations, G7, G20, and the Council of Europe.[26] Within more exclusive multilateral security alliances, additional attempts have also sought to codify an understanding of norms in cyberspace and the applicability of international law to cyber operations through NATO's "Tallinn Manual."[27]

Multilateral efforts to establish cyber norms have been floundering for good reason. First, liberal and illiberal states differ fundamentally in their respective visions of the future of cyberspace and the rules-based international order.[28] Illiberal regimes are working to shape the digital ecosystem in line with authoritarian values, advancing the state-centric concept of "cyber sovereignty" to prioritize the role of regime security and preservation over individual liberty. Russia and China, backed by other member states of the Shanghai Cooperation Organisation, have championed the concept of "information security" instead of "cyber security." Information security aims to control information flows that could jeopardize internal stability and seeks to prevent the dissemination of information that is incompatible with countries' internal political, economic, and social stability, as well as their spiritual and cultural environment.[29] States that adhere to the concept of information security fundamentally perceive the content of information itself as a threat, from which follows deeper state surveillance and control over online content to preserve regime stability. The fundamental divide between, on the one hand, the United States and its Western allies and, on the other, Russia, China, and other illiberal states, indicates that great power competition and divergent conceptions of cyberspace, particularly regarding the free flow of information, the applicability of international humanitarian law, and the doctrine of state responsibility, permeate multilateral negotiations.[30] Consensus on a normative framework for state behavior in cyberspace is thus constrained by broader competitive interactions between great powers

and perceived threats that the liberal order and the interconnectedness of cyberspace pose to illiberal regimes.[31]

At the same time, multilateral efforts have grown increasingly divorced from the operational realities of conducting cyber operations.[32] Indian diplomat Arun Sukumar argues that multilateral efforts are doomed to fail since states are rapidly scaling up their offensive cyber capabilities and are "buying time" to test the possible effects of new offensive cyber capabilities.[33] Illiberal states are concerned that any further endorsement of international law will undermine asymmetric advantages they derive from operating in cyberspace.[34] Even during the most productive years of UN-led efforts to develop cyber norms, the pace, scale, sophistication, and severity of cyber operations of all types conducted by Russia and China have continued unabated. In 2015, as UN diplomats and scholars hailed their recent international consensus on the applicability of international law to cyberspace, Russian cyber actors disrupted parts of the Ukrainian power grid and sabotaged the computer networks of French TV channel TV5 Monde.[35] In 2017—the same year that the Group of Governmental Experts process collapsed over a lack of consensus on the applicability of international humanitarian law to cyberspace—the release and global proliferation of the NotPetya malware, which incurred estimated losses in the tens of billions, was attributed to Russian state actors.[36] Despite efforts to curb economic espionage and intellectual property theft, an extensive US investigation concluded in 2018 that China has buoyed its economic growth with persistent campaigns of widespread, cyber-enabled technology transfer and intellectual property theft causing estimated losses to the US economy ranging from US$225 billion to US$600 billion annually.[37] By July 2021, the US and an "unprecedented" number of allies and partners, including the Five Eyes, the European Union, NATO, and Japan jointly condemned widespread cyber espionage campaigns conducted on behalf of the Chinese government.[38] Yet, the boundaries, scope, and scale of malicious state cyber activity have been expanding apace.

After two decades, norms for state behavior in cyberspace remain "contested, voluntary, unenforceable, vague and weakly internalized."[39] Some scholars are highly pessimistic, asserting that great power dynamics and fundamental disagreements between liberal and illiberal states over the preferred shape of the international order have so permeated multilateral processes that agreement among cyber powers is unlikely. Traditional middle powers lack the real capabilities necessary to deter or coerce malicious state actors effectively. Yet, they are especially vulnerable to weak normative frameworks for state behavior in cyberspace. Regardless, traditional middle powers have continued to approach the geopolitics of cyberspace through the attractive and familiar behavioralist tradition of middle power internationalism, in futile attempts to rally like-minded peers and illiberal states alike into agreeing to binding international frameworks. We characterize this approach as the loyalty response, since middle powers are maintaining their reliance on multilateral institutions and great powers to address issues of geopolitical rivalry, competition, and instability in cyberspace. This approach has proven ineffective, and multilateral efforts alone have proven

insufficient to meet the urgent challenge of setting clear, reasonable, and enforceable international rules for cyberspace. As the development of an explicit normative framework drags on, the empirical record of the past two decades shows that states are increasingly using cyber capabilities as tools of statecraft to achieve strategic advantage in the international environment. Curiously, these activities have largely remained below the threshold of armed conflict, which may indicate that cyberspace norms are actually being shaped tacitly through operations, rather than in the boardrooms of multilateral organizations.[40]

A VOICE APPROACH: CYBER PERSISTENCE AND SHAPING CYBER NORMS THROUGH TACIT BARGAINING

The extensive record of cyberspace competition occurring without escalation to armed conflict signals the emergence of a "new competitive space" wherein explicit agreement over the substantive character of acceptable behavior remains immature.[41] In essence, state actors appear to acknowledge tacitly that most competitive interactions in cyberspace are "bounded by a strategic objective to advance national interests while avoiding war," and thus are most easily and effectively employed as tools to achieve strategic advantage below the threshold of armed conflict and just short of war.[42] The empirical record of the last decade and scholarship on cyber escalation appear to confirm this assertion.[43]

To characterize the nature of strategic competition between states in cyberspace, scholars have, in recent years, coined the term "cyber persistence," which aims to capture how states employ cyber operations as tools of statecraft to change the relative balance of power and achieve strategic advantage in the international environment.[44] The dynamics of cyber persistence are derived from a fundamental feature of networked computing: interconnectedness, which produces a "structural imperative" for constant contact among all adversaries in the global system.[45] Interconnectedness increases the scale at which a state's "core economic, political, social, and military capability and capacity could be undermined" by cyber actors without regard for the constraints of geography and without the degree of control over the global commons on which the projection of conventional force is premised.[46] Cyberspace is both initiative-persistent or offense-dominant insofar as it favors the attacker over the defender at "very low entry costs for core access," as it offers asymmetric opportunities for attackers to generate cyber operations at scale against larger rivals that are orders of magnitude greater than would otherwise be possible outside of cyberspace.[47] Together, interconnectedness, initiative persistence, and asymmetry facilitate constant contact among all states, thereby producing a strategic environment that is structurally characterized by persistent (as opposed to episodic) competitive interactions below the threshold of armed conflict.[48] The scale of these activities in conjunction with the technical complexity of cyber operations has exceeded the ability of states to understand, manage, and reach consensus on cyber norms to regulate acceptable state behavior in cyberspace.

Proponents of cyber persistence contend that the consistent employment of cyber operations below the threshold of armed conflict by both liberal and illiberal states demonstrates a process of normalization or agreed competition, whereby tacitly accepted cyber norms have gradually evolved through competitive interaction between states in cyberspace.[49] Through this process (which cyber persistence scholars call a "tacit bargaining" approach), cumulative and robust operational engagement with adversarial actors has the effect of developing mutual understanding of the boundaries of acceptable/unacceptable state behavior in cyberspace. Ergo, to shape behavior proactively, states must seize the initiative by actively operating and engaging with adversaries in cyberspace in order to tacitly reach informal understandings about the boundaries of accepted behavior.[50] As part of the tacit bargaining process, cyber persistence scholar Michael Fischerkeller suggests that states should coalesce around "focal points," which he defines as "mutual understandings of acceptable/unacceptable behavior in agreed competition."[51] These focal points, if well-established and continually reinforced, may provide some needed stability in cyberspace by enabling states to use them to predict how other states may interpret or respond to a cyber operation.[52] For traditional middle powers, these focal points might include malicious, state-sponsored cyber activities that undermine the rules-based international order or that seek to degrade public confidence in democratic institutions, subvert or sabotage critical infrastructure systems, or reduce the effectiveness of international and multilateral organizations.

Nevertheless, is the substantive nature of the "agreed competition" between states in cyberspace beneficial to the interests of traditional middle powers? The "maturity" of these cyber norms remains nascent and "differing perspectives, ambiguity or uncertainty" over the character of acceptable cyber operations short of armed conflict is likely to continue to cause uncertainty and present a risk for inadvertent escalation.[53] Essentially this means that the absence of explicitly accepted cyber norms and the current immaturity of tacitly accepted norms leaves room for malicious state actors to legitimize the use of significantly disruptive cyber operations short of armed conflict.[54]

In fact, tacit bargaining processes in cyberspace that are antithetical to liberal interest and values may already be occurring. For much of the previous decade, the United States' restraint in responding to the continuous aggression in cyberspace from illiberal state actors such as Russia, China, and Iran has had a destabilizing effect by failing to disincentivize aggressors from operating with impunity. The result has been the gradual shaping and tacit acceptance of norms toward illiberal conceptualizations of cyberspace and the international order.[55] By failing to shape the development of cyber norms in their operational infancy, liberal states risk losing the initiative necessary to manage the emergence of norms that facilitate "massive theft of intellectual property, expanding control of internet content, attacks on data confidentiality and availability, violations of privacy, and interference in democratic debates and processes."[56]

SHAPING THE CYBERSPACE ENVIRONMENT THROUGH PERSISTENT ENGAGEMENT

In 2018 the U.S. Cyber Command (USCYBERCOM) reportedly undertook a series of cyber operations to respond to Russian disinformation efforts targeting US elections and institutions by publicly exposing individuals involved in disinformation efforts and disrupting the functions of the Internet Research Agency—the troll farm at the heart of Russian disinformation operations.[57] These activities formed part of the opening salvo of USCYBERCOM's novel cyberspace strategic doctrine of "persistent engagement"— the most important development in US cyber doctrine in the 21st century. These persistent engagement attempts sought to address a perceived strategic deficit in cyberspace on the part of the United States relative to its adversaries by operating as close as possible to the origin of adversarial cyber activity, and persistently contesting adversarial actors to generate continuous tactical, operational, and strategic advantage.[58] To do so, USCYBERCOM expects to operate "seamlessly, globally and continuously" in cyberspace, using continuous engagement with adversaries to seize and maintain strategic and tactical initiative.[59] Since 2018, under the banner of persistent engagement and to challenge adversarial activities wherever they operate, USCYBERCOM has deployed at least 27 Cyber National Mission Force teams (called "hunt forward" operations by USCYBERCOM) to 15 separate countries as part of its efforts to track and disrupt specific nation-state actors in foreign cyberspace.[60] Reportedly, USCYBERCOM efforts to defend the 2020 US elections may have involved eleven hunt forward operations across nine different countries.[61] More recently, in February 2022, prior to the Russian invasion of Ukraine, hunt forward operations that partnered with Ukrainian network operators were credited with mitigating malware capable of disrupting Ukrainian railway networks, enabling millions of Ukrainians to escape to safety and ensuring the flow of Western assistance remained undisturbed.[62]

Persistent engagement aims to generate "continuous tactical, operational, and strategic advantage in cyberspace," with the ultimate objective of cumulatively shaping the boundaries of acceptable adversarial behavior in cyberspace, through the aforementioned approach of tacit bargaining. [63] Therefore, cyber activities driven by persistent engagement are meant to function as a never-ending series of signals that will push adversaries toward a preferred set of cyberspace norms by continuously undermining their ability to succeed.[64] In 2018, USCYBERCOM operationalized a strategy of persistent engagement in its *Command Vision for U.S. Cyber Command: Achieve and Maintain Cyberspace Superiority.*[65] Through this strategy, USCYBERCOM aims to "secure US national interests in cyberspace and disrupt the cyber campaigns of US adversaries" by "defend[ing] forward as close as possible to the origin of adversary activity, and persistently contest[ing] malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage."[66] The ultimate objective of the strategy is to "influence the calculations of [US] adversaries, deter aggression, and clarify the

distinction between acceptable and unacceptable behavior in cyberspace."[67] In essence, the strategic doctrine of persistent engagement necessitates a more active US posture in cyberspace, with the overall strategic objective of inhibiting an adversary's attempts to intensify cyber operations against the US and its allies.

Proponents of persistent engagement contend that previous US approaches to cyberspace were overly reliant on multilateral initiatives to establish cyber norms explicitly, which in turn resulted in a restrained and reactive operational strategy in cyberspace.[68] By contrast, the very raison d'être of the persistent engagement strategy is as an operational complement to sole reliance on multilateral efforts to develop cyber norms, which is believed to have ceded the advantage in cyberspace to adversaries with an incentive to be more aggressive in their use of cyber operations.

Through persistent engagement, the US aims to "gain strategic advantage" in cyberspace by preserving a favorable distribution of power. This objective is ambitious, and global in scope, with an end state the US defines as acceptable or unacceptable behavior in cyberspace, but it is also somewhat ambiguous.[69] Critics of persistent engagement are also concerned about the lack of defined objectives and clarity regarding the strategy's actual implementation, proposing that in its current form, persistent engagement appears to proscribe an endless deployment of cyber resources in pursuit of vague strategic objectives.[70] Other critics argue that the persistent deployment of US cyber capabilities against rivals is destabilizing and risks unintended consequences through inadvertent escalation, thereby exacerbating instability in cyberspace and accelerating an already hyper-competitive and unstable environment.[71] However, concerns about escalation in and through cyberspace have generally been overstated. Recent research suggests that cyber operations are only narrowly escalatory, and only within the context of broader geopolitical crises.[72]

FUNCTIONAL ENGAGEMENT FOR TRADITIONAL MIDDLE POWERS

Traditional middle powers face significant threats in cyberspace and are vulnerable to adversarial cyber operations that undermine their national and global interests. Middle powers have largely responded to this growing threat by taking a passive approach: hardening their cyber defense capabilities and participating in multilateral initiatives to develop and diffuse transnational cyber norms. Middle powers may expect that the combination of these efforts will reduce the threats they face from malicious state actors in cyberspace. Since multilateral cyber diplomacy efforts have largely stalled, and given that the threats middle powers face in cyberspace are increasing exponentially, an alternative (or complementary) approach is necessary.

Cyber persistence theory and the concepts of tacit bargaining and normative shaping in cyberspace hold significant strategic utility for middle powers. The problem: cyber persistence theory has been formulated to guide the US approach to countering adversarial behavior in

cyberspace. The only known operationalization of cyber persistence theory—persistent engagement—specifically aims to alter the global balance of cyber power in the United States' favor by continually contesting its adversaries around the clock.[73] These objectives are unattainable for middle powers, not only due to inadequate resources, but also because they are misaligned with the foreign policy ambitions and characteristics of middle powers. In contrast, foreign policy interests more characteristic of middle powers might include maintaining the status quo, ensuring security and order in the international system, upholding the integrity of international organizations and democratic institutions, and protecting economic security and prosperity.

This article posits the cyber-strategic concept of functional engagement as a variation on persistent engagement uniquely tailored for operationalization by traditional middle powers. Functional engagement seeks to harness the strategic utility of cyber persistence theory and persistent engagement by adapting it to align more closely with traditional middle powers that strive to influence international affairs selectively as a function of their relative capabilities, interests, and degree of involvement.[74] The key difference between functional engagement and persistent engagement is the scope and scale of their respective objectives. Functional engagement proscribes a narrower application of tacit bargaining and normative shaping in cyberspace that reflects the limited cyber capabilities and foreign policy ambitions of traditional middle powers. To this end, functional engagement is premised on establishing and reinforcing a limited set of focal points that are communicated unambiguously to set boundaries for acceptable and unacceptable behavior in cyberspace. Middle powers can then harness their limited cyber capabilities more effectively against adversarial cyber actors that transgress these specific focal points.

An initial set of focal points for unacceptable behavior could include malicious activities that subvert or degrade the integrity of electoral processes or critical infrastructure systems, actions that undermine economic security or competitiveness, and behavior that undermines the effective functioning of international institutions. Instead of continuously and globally employing cyber capabilities to change the overall balance of power in the international system, functional engagement calls for middle powers to deploy targeted cyber operations, specifically in instances when a malicious actor conducts cyber activity that is antithetical to tacitly accepted focal points. In turn, this strategy enables traditional middle powers to bolster focal points for cyber norms while upholding the rules-based international order.

CANADA: A CASE STUDY FOR EMPLOYING FUNCTIONAL ENGAGEMENT

As a variant of the United States' persistent engagement approach, we contend that functional engagement is better suited to states with limited resources but whose geopolitical ambitions render them targets of, and vulnerable to, adversarial state-sponsored cyber activity.

The Functional Principle and Its Application to Canada's Cyberspace Doctrine

In the post-Second World War period and throughout the Cold War, Canada leveraged the "functional principle" (from which functional perspective of middle power identity and the proposed functional engagement doctrine derive their names) to pursue its interests, justify a disproportionate influence in the international system, and cement its post-1945 status as a leading "non-great power."[75] First articulated by Canadian diplomat Hume Wrong, the functional principle stipulated that an individual small state's involvement in international affairs should be based on (1) the relevance of the state's interests, (2) the direct contribution of the state to the situation in question, and (3) the capacity of the state to participate.[76] Practically, the functional perspective holds that middle powers commit to maintaining the status quo, security, and order in the international system through leadership on specific global problems and foreign policy niches of their choosing.[77]

Indeed, growing instability and increasing strategic competition between states in cyberspace are both global problems and a foreign policy niche highly relevant to Canada's national security and foreign policy interests. Owing to the resource constraints that characterize middle powers, for the past two decades Canada has been struggling to demonstrate effective international leadership and respond to a highly competitive cyberspace environment. At least three factors continue to coalesce to make Canada a low-risk, high-payoff target for malicious cyber activity. First, Canada has limited soft and hard power resources, which constrains its ability to combine instruments of power or retaliate unilaterally. Second, Canada's economy is highly advanced, with a strong technology sector, high levels of digital connectivity, vast natural resource wealth, and cutting-edge research and development activities.[78] Third, Canada's special relationship with the US and its membership in an array of coveted security alliances and multilateral institutions provide potential adversaries with an efficient means of targeting both Canada and its great power allies.[79]

Threats to Canada in cyberspace are escalating in sophistication, quantity, and complexity, and the country's core national interests continue to be undermined by malicious, state-sponsored cyber actors. Canada's national security and its international interests have long been assured by its geographic location, the security assurances of multilateral institutions, and the legal and normative frameworks of the rules-based international order.[80] Cyberspace represents a unique departure from these assurances: it allows Canada's adversaries to bypass its geographic advantage entirely, while multilateral approaches to managing state behavior in cyberspace lack a foundation of stable laws, norms, and incentives to encourage malicious state actors to discipline their activities.

Threats to Canada in Cyberspace and Its Evolving Cyber Strength

Canada's tradition of liberal internationalism has reflexively inclined it toward supporting multilateral processes that attempt to establish explicitly (as opposed to tacitly) accepted

boundaries for state behavior in cyberspace. Since 2010, Canada has participated in at least forty-five multilateral statements, communiqués, and initiatives on cyber norms in the G7, G20, NATO, ASEAN, OAS, OSCE, the Commonwealth, and the UN.[81] Concerted cyber diplomacy efforts notwithstanding, the Canadian military unambiguously asserts that state actors are increasingly pursuing their agendas using hybrid methods below the threshold of armed conflict (including in cyberspace) to threaten Canada's defense, security, and economic interests.[82] Moreover, the director of Canada's domestic security service, the Canadian Security and Intelligence Service, has warned that Russian and Chinese state-sponsored commercial espionage remains the most significant threat to the Canadian economy and future economic growth.[83] According to Canada's 2020 and 2022 National Cyber Threat Assessments, cyber operations by China, Russia, Iran, and North Korea posed the greatest threat to Canada's national security and its strategic interests.[84] The assessments, which are the landmark documents by which the Government of Canada communicates updates about strategic cyber threats to the Canadian public, assert that state-sponsored cyber actors have carried out "large-scale, worldwide cyber campaigns" to influence the Canadian public and conduct espionage against Canadian industry, government, and academia, with intent to "advance foreign economic and national security interests while undermining the same within Canada."[85]

Although inevitably limited by challenges in collecting measures of national cyber capabilities, the Harvard Belfer Center Cyber Power Index (CPI) is a comprehensive effort to evaluate and compare the objectives and capabilities of states in cyberspace. That makes it a useful tool to examine the status and evolution of Canada's cyber capabilities. In the 2020 CPI ranking for overall comprehensive global cyber power, Canada ranked eighth (behind the United States, China, the United Kingdom, Russia, the Netherlands, France, and Germany, but ahead of Japan and Australia).[86] In the updated 2022 CPI, Canada dropped out of the top ten.[87] Ranked thirteenth, Canada not only ranked lower than all of its major adversaries (Russia, China and Iran), but also three of its Five Eyes partners (the US, UK, and Australia) and a handful of its other like-minded partners (the Netherlands, South Korea, France, Germany, and Ukraine).[88] Moreover, the 2022 CPI shows that, since 2020, Canada's measures have declined across all of the cyber power objectives.[89] Canada now lags its major adversaries, middle power peers, and Five Eyes partners in key objectives including the intent and capability to: conduct cyber-enabled foreign intelligence, control and manipulate the information environment, and destroy or disable an adversary's infrastructure and capabilities.[90] Since 2020, though, Canada moved also from a "high-intent, low-capability" cyber power, to a "high-intent, high-capability" cyber power, retaining notable strengths in cyber surveillance, cyber defense and cyber norms development initiatives.[91]

On the one hand, the CPI's assessment of Canada reflects two decades of careful focus on implementing and communicating cyber defense and cyber security initiatives. On the other hand, the rankings may indicate a strategic deficit and thus the need for a cyberspace

doctrine to harness a range of more assertive cyber espionage, subversion, and sabotage capabilities in pursuit of national strategic objectives.

In recent years, Canadian policymakers have made deliberate efforts to develop institutional and legislative mechanisms to support a more assertive cyberspace posture. Canada's 2017 defense policy, *Strong, Secure, Engaged*, recognized that cyberspace is essential for the conduct of modern military operations and complemented a strong defensive cyber posture with more assertive cyber operations.[92] In 2019, passage of Bill C-59, *An Act Respecting National Security Matters*, bolstered the prospect for Canadian cyber operations. Bill C-59 expanded the role and impact Canada could have in cyberspace by authorizing the Communications Security Establishment (CSE) to conduct offensive cyber operations, which the legislation parses into "active cyber operations" and "defensive cyber operations"—to supplement CSE's traditional role of ensuring cryptographic security and collecting foreign signals intelligence.[93] The addition of these capabilities to CSE's mandate was hailed as a major step in aligning Canada's cyber operations authorities with its Five Eyes allies.[94] For the first time in its history, the combination of foreign intelligence, active cyber operations, and defensive cyber operations mandates may enable it to conduct the full spectrum of cyber espionage, sabotage, and subversion operations.

In summary, Canada may be an ideal candidate for functional engagement since it (1) has a legacy of restraining its influence on geopolitics to foreign policy niches of particular relevance (the functional principle); (2) faces significant threats to its national and international interests as a result of malicious state-sponsored cyber activities and lacks a cyber strategic doctrine to organize its response; and (3) may already have, or is otherwise well on the path toward developing, the requisite cyber capabilities and authorities to begin upholding its interests in the cyberspace environment.

Functional Engagement in the Canadian Context

Canada may have an opportunity to demonstrate independent international leadership to reduce instability and uncertainty in cyberspace. In doing so, it can uphold and extend its strategic interests. According to cyber persistence theory, helping to establish and strengthen tacitly accepted cyber norms by regularly employing cyber capabilities may be an effective way for Canada to reduce uncertainty in cyberspace and limit threats to its national interests. Due to Canada's resource constraints and limited foreign policy ambitions (in comparison to the US and other great powers), functional engagement prescribes that Canada employ the full range of its nascent cyber capabilities to establish and reinforce a focused set of clearly defined and communicated focal points that define what it deems acceptable and unacceptable behavior in cyberspace. Instead of continuously and globally employing cyber capabilities to change the overall balance of power in the international system, functional engagement calls for Canada to employ its cyber capabilities more narrowly, in specific instances when a malicious cyber actor conducts activity that is antithetical to those focal points.

An initial set of focal points for unacceptable state-sponsored behavior in cyberspace could include malicious activities that (1) directly degrade Canada's sovereignty and the security of its people (e.g., cyber operations that target civilian critical infrastructure and ICS/SCADA systems); (2) degrade or subvert international law and the integrity of international, electoral, or democratic institutions (e.g., cyber operations that target electronic voting systems or the functioning of international institutions); and (3) directly undermine Canada's economic security, competitiveness, and prosperity (e.g., cyber operations that target intellectual property). In turn, this approach remains true to the fundamentals of cyber persistence but is more aligned within the limited resources and unique character of Canada's geopolitical identity as a middle power.

CONCLUSION

The volume and sophistication of state-sponsored activities in cyberspace has increased apace with deepening global dependence on the Internet and digital technologies. Twenty years of international interactions in cyberspace reinforce that cyber war is rare and that states prefer to employ cyber operations as tools of statecraft well below the threshold of armed conflict. While the immediate risk of cyber escalation appears to be low, campaigns of cumulative cyber operations aim to generate strategic effects over time, by degrading the integrity of international, democratic, and electoral institutions, undermining economic competitiveness, and/or generating strategic information advantage over an adversary. Meanwhile, multilateral initiatives to reduce instability in cyberspace and develop explicitly accepted cyber norms have failed to deliver significant advances in regulating the boundaries of state behavior in cyberspace.

Traditional middle powers, especially those with highly interconnected societies, advanced economies, world-renowned research institutions, and memberships in an array of multilateral and security institutions, face threats in cyberspace as acute as those faced by great powers, and possibly even more so given their limited economic and military capabilities and narrow influence in the international system. Traditional middle powers thus present a low-risk, high-payoff target for their adversaries in cyberspace, and consequently are accumulating a strategic deficit vis-à-vis other states that have more readily grasped such threats—and the opportunities of cyber operations as a tool of statecraft. By failing to shape adversarial behavior in cyberspace around tacitly accepted focal points cumulatively, Canada, the Netherlands, Australia, and other traditional middle powers are ceding the operational initiative to illiberal adversaries such as Russia and China, which will in turn seize that initiative to generate cyber norms that support their strategic interests.[95]

Faced with the prospects of a deleterious change to their environment as a result of growing instability and malicious activity in cyberspace, middle powers can *exit*, use *voice*, or demonstrate *loyalty.* Traditional middle powers such as Canada had hitherto pursued a *loyalty*

approach that prioritizes multilateral efforts and close partnerships with like-minded great powers to develop explicitly accepted cyber norms. These efforts have yet to yield significant payoff and have failed to stem the rising tide of adversarial activity that is sweeping traditional middle powers in cyberspace. As a variation on persistent engagement for the US, *functional engagement* for traditional middle powers is a *voice* approach that adapts cyber-strategic concepts of cyber persistence theory and persistent engagement to align with the limited resources and foreign policy ambitions of middle powers. Functional engagement in cyberspace seeks to harness the potential of tacit bargaining and normative shaping by focusing the limited cyber capabilities of traditional middle powers in pursuit of narrow strategic objectives. Traditional middle powers can leverage coalition cyber strategic campaigns to establish and reinforce a set of focal points that delineate acceptable from objectionable behavior by states in cyberspace.

ACKNOWLEDGMENT

Research for this article was supported by the Social Sciences and Humanities Research Council of Canada Partnership Grant 895-2021-1007.

NOTES

1. Leuprecht, C., Szeman, J., and Skillicorn, D.B. (2019), The Damoclean sword of offensive cyber: policy uncertainty and collective insecurity, *Contemporary Security Policy*, 40(3), 382-407, https://doi.org/10.1080/13523260.2019.1590960.
2. Council on Foreign Relations. (2022), Cyber Operations Tracker, Council on Foreign Relations, https://www.cfr.org/cyber-operations/#OurMethodology.
3. Maness, R. C., Valeriano, B., Jensen, B., Hedgecock, K., and Macias, J. (2022), The dyadic cyber incident and campaign dataset, version 2.0. Harvard Dataverse, https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/CQOMYV.
4. Ibid
5. Ibid
6. Ibid
7. Ibid
8. Mitrany, D. (1933), The progress of international government. Yale University Press.
9. Shin, Dong-Min. (2015, 4 December), A critical review of the concept of middle power. E-International Relations. https://www.e-ir.info/2015/12/04/a-critical-review-of-the-concept-of-middle-power/.
10. Glazebrook, G. (1947). The middle powers in the United Nations system, *International Organization*, 1(2), 307-18, https://doi.org/10.1017/S002081830000608.1
11. Cooper, D. (2011). Challenging contemporary notions of middle power influence: Implications of the proliferation security initiative for middle power theory, *Foreign Policy Analysis*, 7(3), 317-36, https://doi.org/10.1111/j.1743-8594.2011.00140; Patience, A. (2014). Imagining middle powers, Australian Journal of International Affairs, 68(2), 210–24. https://doi.org/10.1080/10357718.2013.840557.
12. Chapnick, A. (1999). The middle power, *Canadian Foreign Policy Journal*, 7(2), 73-82. https://doi.org/10.1080/11926422.1999.9673212.
13. Ibid.
14. Holbraad, C. (1984), Middle powers in international politics, Macmillan. Shin, 2015.
15. Chapnick, A. (1999), The middle power, *Canadian Foreign Policy Journal*, 7(2), 73-82, https://doi.org/10.1080/11926422.1999.9673212.
16. Ibid.
17. Holbraad, C. (1971), The role of middle powers. *Cooperation and Conflict*, 6(1), 77-90, https://doi.org/10.1177/001083677100600108.
18. Cooper, A., Higgott, R., and Nossal, K. (1993), Relocating middle powers. University of British Columbia Press.
19. Ibid.
20. Ibid.
21. Lee, G., and Soeya, Y. (2014). The middle-power challenge in East Asia: An opportunity for co-operation between South Korea and Japan, Global Asia, 9(2), 85-91.
22. Jordaan, E. C. (2003). The concept of a middle power in international relations: Distinguishing between emerging and traditional middle powers, *Politikon South African Journal of Political Studies*, 30(2), 165-81.
23. Ibid.
24. Ibid.
25. Ibid.
26. Grigsby, A. (2017). The end of cyber norms. Survival, 59(6), 109-22. https://doi.org/10.1080/00396338.2017.1399730; Maurer, T. (2020). A dose of realism: The contestation and politics of cyber norms, *Hague Journal on the Rule of Law*, 12(2), 227-49, https://doi.org/10.1007/s40803-019-00129-8; Tikk-Ringas, E. (2017). International cyber norms dialogue as an exercise of normative power, *Georgetown Journal of International Affairs*, 17(3), 47-59, https://www.jstor.org/stable/26395975.
27. Jensen, E. (2017). The Tallinn Manual 2.0: Highlights and insights, *Georgetown Journal of International Law*, 48(1), https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf.
28. Ibid.

NOTES

29. Stevens, T. (2012). A cyberwar of ideas? Deterrence and norms in cyberspace, *Contemporary Security Policy*, 33(1), 148-70. https://doi.org/10.1080/13523260.2012.659597.
30. Tikk-Ringas, 2017.
31. Hurwitz, R. (2014), The play of states: Norms and security in cyberspace. *American Foreign Policy Interests*, 36(5), 322-32, https://doi.org/10.1080/10803920.2014.969180, Maurer, 2020.
32. Grigsby, 2017. Maurer, 2020.
33. Sukumar, A. (2017). The UN GGE failed. Is international law in cyberspace doomed as well? *Lawfare*, https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.
34. Ibid.
35. Corera, G. (2016). How France's TV5 was almost destroyed by "Russian hackers." BBC News. https://www.bbc.com/news/technology-37590375; Cyber Law Toolkit (2015, 23 December), Power grid cyberattack in Ukraine (2015). Cyber Law Toolkit, https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015).
36. Greenberg, A. (2018), The untold story of NotPetya, the most devastating cyberattack in history, *Wired*, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
37. United States of America. (2018b). Findings of the investigation into China's acts, policies, and practices related to technology transfer, intellectual property, and innovation under section 301 of the Trade Act of 1974. Office of the United States Trade Representative Executive Office of the President, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.
38. United States of America. (2021, 19 July). The United States, joined by allies and partners, attributes malicious cyber activity and irresponsible state behavior to the People's Republic of China. White House, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.
39. Maurer, 2020.
40. Ibid.
41. Goldman, E. (2022). Paradigm change requires persistence—a difficult lesson to learn. *The Cyber Defense Review*, 7(1), 113-18. https://www.jstor.org/stable/48642031.
42. Fischerkeller, M., and Harknett, R. (2018b). Persistent engagement and tacit bargaining: A path toward constructing norms in cyberspace. *Lawfare*, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.
43. Healey, J., and Jervis, R. (2020). The escalation inversion and other oddities of situational cyber stability, *Texas National Security Review,* 3(4), 30-53, http://dx.doi.org/10.26153/tsw/10962; Kreps S., and Schneider, J. (2019), Firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics, *Journal of Cybersecurity*, 5(1), 1-9, https://doi.org/10.1093/cybsec/tyz007.
44. Fischerkeller and Harknett, 2017. Harknett, R., and Goldman, E. (2016). The search for cyber fundamentals. *Journal of Information Warfare*, 15(2), 81–8. https://www.jstor.org/stable/26487534; Harknett, R., and Smeets, M. (2022). Cyber campaigns and strategic outcomes, *Journal of Strategic Studies*, 45(4), 534–67. https://doi.org/10.1080/01402390.2020.1732354.
45. Harknett and Goldman, 2016.
46. Harknett and Smeets, 2022.
47. Fischerkeller, M., and Harknett, R. (2018a), Cyber persistence theory, intelligence contests and strategic competition. Institute for Defense Analysis, https://apps.dtic.mil/sti/pdfs/AD1118679.pdf.
48. Harknett and Goldman, 2016. Fischerkeller and Harknett, 2017. Fischerkeller, M., and Harknett, R. (2019). Persistent engagement, agreed competition, and cyberspace interaction dynamics and escalation. *The Cyber Defense Review–Special Edition.* https://cyberdefensereview.army.mil/Portals/6/CDR-SE_S5-P3-Fischerkeller.pdf.
49. Fischerkeller and Harknett, 2018b. Goldman, E. (2020), From reaction to action: Adopting a competitive posture in cyber diplomacy, *Texas National Security Review*, 3(4), https://repositories.lib.utexas.edu/bitstream/handle/2152/83957/TNSRVol3Iss4Goldman.pdf?sequence=2.
50. Fischerkeller and Harknett, 2018b. Fischerkeller and Harknett, 2019. Goldman, 2022.
51. Fischerkeller and Harknett, 2019.

NOTES

52. Farrell, H., Glaser, C. (2017). The role of effects, saliencies and norms in U.S. cyberwar doctrine, *Journal of Cybersecurity*, 3(1), 7-17, https://doi.org/10.1093/cybsec/tyw015.
53. Fischerkeller and Harknett, 2019.
54. Ibid.
55. Goldman, 2020.
56. Ibid.
57. Gallagher, S. (2019). Report: US cyber command took Russian trolls offline during midterms. Ars Technica, https://arstechnica.com/information-technology/2019/02/report-us-cyber-command-took-russian-trolls-offline-during-midterms/. Nakashima, E. (2019). U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms, *The Washington Post*, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.
58. United States of America. (2018a). Command vision for U.S. Cyber Command: Achieve and maintain cyberspace superiority, United States Cyber Command.
59. Ibid.
60. Pomerleau, M. (2022). Cyber Command has deployed to nations 27 times to help partners improve cybersecurity. *Fedscoop*, https://www.fedscoop.com/cyber-command-has-deployed-to-nations-27-times-to-help-partners-improve-cybersecurity/.
61. Ibid.
62. Srivastava, M., Murgia, M., and Murphy, H. (2022). The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion, Financial Times, https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471.
63. Harknett and Goldman, 2016. Fischerkeller and Harknett, 2017. Fischerkeller and Harknett, 2019.
64. Healey, J., and Caudill, S. (2020). Success of persistent engagement in cyberspace. *Strategic Studies Quarterly*, 14(1), 9-14, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-14_Issue-1/Healey.pdf.
65. United States of America, 2018a.
66. Ibid.
67. Ibid.
68. Fischerkeller and Harknett, 2017.
69. Smeets, M. (2019), There are too many red lines in cyberspace, *Lawfare,* https://www.lawfareblog.com/there-are-too-many-red-lines-cyberspace.
70. Lin, H., and Smeets, M. (2018). What is absent from the U.S. Cyber Command "vision," *Lawfare*, https://www.lawfareblog.com/what-absent-us-cyber-command-vision; Lin, H., and Zegart, A. (2018), Bytes, bombs, and spies: The strategic dimensions of offensive cyber operations. Brookings University Press.
71. Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity*, 5(1), 1-15. https://doi.org/10.1093/cybsec/tyz008.
72. Healey and Jervis, 2020.
73. United States of America, 2018a.
74. Holbraad, 1971. Cooper et al., 1993. Chapnick, 1999.
75. Chapnick, 1999. Chapnick, A. (2000), The Canadian middle power myth, *International Journal*, 55(2), 188-206, https://doi.org/10.2307/40203476.
76. Chapnick, 2000.
77. Cooper et al., 1993.
78. Siebring, J. (2021). Choosing complicated: The Canadian approach to national security in cyberspace [Master's directed research paper, Royal Military College of Canada], Canadian Forces Digital Library.
79. Canadian Security Intelligence Service. (2021). CSIS public report 2020. Government of Canada, https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/CSIS-Public-Report-2020.pdf
80. Macnamara, D. (2012), Canada's national and international security interests. In D. McDonough (Ed.), Canada's national security in the post-9/11 world: Strategy, Interests, and threats, 45-56, University of Toronto Press.

NOTES

81. Carnegie Endowment. (2022). Cyber norms index and timeline—Canada, Carnegie Endowment for International Peace, retrieved July 15, 2022, from https://carnegieendowment.org/publications/interactive/cybernorms#timeline-section.
82. Canada. (2017), Strong, secure, engaged: Canada's defence policy, Department of National Defence, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html.
83. Vigneault, D. (December 8, 2018), Remarks by Director David Vigneault at the Economic Club of Canada. Government of Canada, https://www.canada.ca/en/security-intelligence-service/news/2018/12/remarks-by-director-david-vigneault-at-the-economic-club-of-canada.html?fbclid=IwAR2VWCrD1F4aCznfNfeQrQoyZd_CMxAfCi8ihugtNmzjE_BrjFG4jPD-7Pag.
84. Canada. (2020), National cyber threat assessment 2020, Canadian Centre for Cyber Security, https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf; Canada. (2022), National Cyber Threat Assessment 2023-2024. Canadian Centre for Cyber Security, https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024.
85. Canada, 2020. Canada, 2022.
86. Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D., and Schwarzenbach, A. (2020), National cyber power index 2020, Belfer Center for Science and International Affairs, https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.
87. Voo, J., Hemani, I., and Cassidy, D. (2022). National cyber power index 2022, *Belfer Center for Science and International Affairs*, https://www.belfercenter.org/publication/national-cyber-power-index-2022.
88. Ibid.
89. Voo et al., 2020. Voo et al., 2022.
90. Voo et al., 2022.
91. Ibid.
92. Canada, 2017.
93. Bill C-59, (2019). An Act respecting national security matters, 1st sess., 42nd Parliament, 2017, SC 2019, https://www.parl.ca/LegisInfo/en/bill/42-1/c-59.
94. Carvin, S. (2018). Zero D'Eh: Canada takes a bold step towards offensive cyber operations. Lawfare, https://www.lawfareblog.com/zero-deh-canada-takes-bold-step-towards-offensive-cyber-operations.
95. Jordaan, 2003.