A Comparison of the National Security and the Cybersecurity Approaches of the United States under Presidents Trump and Biden versus the National Security and Cybersecurity Approach of Canada

Donald L. Buresh
Ph.D., J.D., LL.M., Cybersecurity and Policy Department, Morgan State University, Baltimore, Maryland

DOI: https://doi.org/10.15520/jbme.v9i03.3265

Abstract: The paper compares the national security and cybersecurity approaches of the United States under President Trump and President Biden versus the national security and cybersecurity approach of Canada. The four pillars of the American national security strategy are outlined, and then the five pillars of America’s cybersecurity strategy are examined. Biden administration’s approach to national security and cybersecurity is also discussed. The Canadian approach to national security is highlighted, followed by a treatment of the Canadian cybersecurity strategy. The two national security strategies are compared, followed by contrasting the American versus the Canadian cybersecurity strategies. Although both nations are dedicated to protecting their citizens, Canada is less concerned about preserving the Canadian way of life than the United States. The American national cybersecurity strategy appears to be cloaked in the language of unification, whereas the Canadian approach to national security seems to be focused on practical strategic considerations. The United States’ national security is motivated to preserve peace through strength, while Canada promotes its national security via cooperation and collaboration. The conclusion is that the divergence between the strategies is due more to cultural differences than to a difference in technical approaches.

Keywords:
- Canada National Security Strategy
- Canada Cybersecurity Strategy
- Department of Homeland Security
- United States National Security Strategy
- United States Cybersecurity Strategy

INTRODUCTION

There are several reasons to compare the national security strategies of the United States and Canada. First, except for Quebec, Canada is an English-speaking nation, much like the United States, making it easier to collect data. Second, the two countries enjoy a common border of 8,891 kilometers (5,525 miles) long, which includes the maritime boundaries in the Great Lakes and the Atlantic, Pacific, and Arctic Oceans. This figure also consists of 2,475 kilometers (1,538 miles) that measure Canada’s and Alaska’s border. Eight Canadian provinces border 13 U.S. States. The provinces include Yukon, British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, Quebec, and New Brunswick from West to East. The thirteen U.S. states from West to East are Alaska, Washington, Idaho, Montana, North Dakota, Minnesota, Michigan, Ohio, Pennsylvania, New York, Vermont, Maine, and New Hampshire.

Third, in contrast to the U.S.-Mexican border, before the Covid-19 worldwide pandemic, individuals from both the United States and Canada could move almost freely between the two nations. There were usually only border checkpoints along most of the highways that run from one state to the other, with no walls on land. There was, and still is, no credible discussion of building a physical barrier separating the two nations. Finally, both the United States and Canada have enjoyed excellent political, economic, and cultural relations for nearly two hundred years. Thus, Canada is an excellent selection when comparing its national security and cybersecurity approach against the national security and cyber security approach of the United States.

The comparison will be two-fold. First, the American and Canadian national security approaches will be compared as a whole, where the national security approaches of President Trump and President Biden will be outlined. Second, both nations’ cybersecurity approaches will also be analyzed because, these days, cybersecurity is a burning issue in national security and cybersecurity strategic thinking. The very newness of cybersecurity demands that national security approaches be evaluated regarding their ability to address new digital threats. Thus, by making these two comparisons, the nuances of the two strategies will be revealed in a manner that would be less transparent if only the two national security approaches were compared en bloc.

UNITED STATES APPROACH TO NATIONAL SECURITY STRATEGY UNDER PRESIDENT TRUMP

Under President Trump, the United States approach to security is predicated on American principles, a focused assessment of U.S. interests, and a resolve to conquer the nation’s challenges. For the United States, a country born from recognizing the inalienable rights of life, liberty, and the pursuit of happiness, the thriving of American institutions, traditions, and principles is paramount. The United States is dedicated to responding to the economic, military, and political rivalries encountered worldwide. According to the Trump administration, the nation perceives that these rivalries are intermingled with long-term challenges that require
sustained consideration. The four pillars of American national security include:

- Protecting the American people, the homeland, and the American lifestyle;
- Promoting American prosperity;
- Preserving peace through strength; and
- Fostering American influence around the globe.

**Pillar I: Protecting the American People, the Homeland, and the American Lifestyle:**

The first pillar of the American national security strategy is protecting the American people, the homeland, and the American way of life. This includes defending against weapons of mass destruction (WMD) and strengthening border control and immigration policy. By pursuing threats to their source, the United States national security strategy is dedicated to defeating Jihadist terrorists and dismantling transnational criminal organizations. The approach promotes identifying and prioritizing risks, building secure government networks, improving information sharing and sensing, and employing layered defenses regarding cybersecurity.

Although the federal government cannot avert all American people’s hazards, the Trump administration’s strategy ensured that America remains resilient when facing opposition. According to the American national security approach, reducing risk and building robust communities is the best way to defend America.

**Pillar II: Promoting American Prosperity:**

According to President Trump, the second pillar of the national security strategy for the United States was to rejuvenate the American economy so that both American companies and workers’ profit. The policy demanded fair and mutual relations to address trade imbalances. The plan ensured that the United States led the world in technology, invention, and innovation by stimulating the U.S. national security basis for change.

**Pillar III: Preserving Peace through Strength:**

The third pillar of the American national security strategy espoused by the Trump administration firmly believed in rebuilding the United States military to remain the most powerful military on the planet. The strategy warranted that no region of the world would be dominated exclusively by one power. The national security approach under President Trump encouraged American capabilities in space and cyberspace, where Allies and partners bore a fair share of the burden of protecting all from common threats.

**Pillar IV: Advancing American Influence around the Globe:**

Under President Trump, the fourth and final pillar of the American national security strategy was to improve American influence throughout the world. The plan was to compete and lead multilateral organizations to promote American interests and values in liberty, democracy, and the rule of law. The approach was dedicated to fostering private-sector economic growth by helping would-be partners become trading partners in the future.

**UNITED STATES APPROACH TO NATIONAL SECURITY UNDER PRESIDENT BIDEN**

In contrast, the national security strategy of the United States under President Biden, as of this writing, is in a state of flux. According to the *Interim National Security Strategic Guidance* white paper, President Biden boldly stated that the United States needs “creative approaches that draw on all the sources of [American] national power: our diversity, vibrant economy, dynamic civil society and innovative technological base, enduring democratic values, broad and deep network of partnerships and alliances, and the world’s most powerful military.” The global landscape has changed, even from as little as four years ago. According to President Biden, the risk of a biological pandemic, the accelerating climate crisis, cyber threats, along with international economic disruptions such as recessions, prolonged humanitarian crises, violent extremism and terrorism, and the proliferation of nuclear weapons and other weapons of mass destruction establish acute existential dangers. According to President Biden, no one nation acting alone can effectively address these issues.

In other words, the United States must cooperate with other nations in its search to promote its national security. According to President Biden, the national security of the United States requires the country to:

- Defend and nurture the underlying sources of American strength, including its people, economy, national defense, and the country’s democracy at home;
- Promote a favorable distribution of power by deterring and preventing adversaries from directly threatening the United States and its allies, while at the same time inhibiting access of the country’s enemies to the global commons, or dominating critical regions of the world; and
- Lead and sustain a stable and open international law and governance system that is backed by strong democratic alliances, partnerships, multilateral institutions, and rules.

President Biden proclaimed that the United States should restore its leadership position in international institutions such as the United Nations to attack shared challenges like the climate crisis. For example, under President Biden, the United States has re-entered the Paris Climate Accord. He has appointed a Presidential Special Envoy for climate change to combat extreme weather conditions and future environmental stress. According to President Biden, by failing to act now, the United States may miss its last opportunity to avert the dire consequences of climate changes that may affect the health of the American people, the United States economy, the country’s national security, and the planet as a whole.

**UNITED STATES NATIONAL CYBERSECURITY APPROACH UNDER PRESIDENT TRUMP**

The United States Department of Homeland Security is charged to create a national cybersecurity strategy policy. Because the American people are becoming increasingly dependent on the Internet for daily conveniences, critical services, and economic prosperity, the U.S. federal government needs to take an active role in ensuring that cyberspace is both secure and resilient.
Internet-based technology has advanced by leaps and bounds in the past several decades. America experiences cyber threats daily that can adversely affect federal and non-federal computer systems. Ransomware events, including WannaCry and NotPetya, show how the asymmetric adversaries can effectively use the Internet-of-Things to engage in cybercrimes and terrorist threats. The far-reaching availability, the low cost, and ever-growing cyber tools capabilities ensure that future attacks will be far more sophisticated than their relatively primitive predecessors.

The cybersecurity goals for the Department of Homeland Security (“DHS”) are predicated on the following five pillars:

- Risk identification;
- Vulnerability reduction;
- Threat reduction;
- Consequence mitigation; and
- Enabling cybersecurity outcomes.

The guiding principles behind the DHS cybersecurity strategy encompass risk prioritization, cost-effectiveness, innovation and agility, collaboration, global approach, balanced equities, and national values.

**Pillar I: Risk Identification:**
For the DHS, risk identification means that the organization must become strategically aware of national and systematic cybersecurity trends by identifying ever-changing cybersecurity risks that influence national security, public health and safety, and the nation’s economic well-being. The DHS has been charged with creating plans to deal with gaps in risk management that affect cybersecurity stakeholders.

**Pillar II: Vulnerability Reduction:**
The DHS works to protect the federal government’s information systems from attaining a prescribed degree of cybersecurity. Its objective is to enhance cybersecurity via increased governance and oversight of information security policies through a cost-effective, formalized approach that reduces cyber risk. The DHS supports the necessary tools to safeguard the country’s national security information systems.

By partnering with key stakeholders, the DHS ensures that growing risks are managed at an acceptable level. The department periodically evaluates its risk management efforts to identify capability gaps, focusing on systematic dangers to critical infrastructure. The DHS understands, values, and assesses systematic risks that affect national security and public health, among other things. It should be noted that the DHS also improves cybersecurity capabilities that are offered to government agencies, regulators, and policymakers.

**Pillar III: Threat Reduction:**
In reducing cyber threats to the United States, the DHS is dedicated to disrupting transnational criminal organizations and state-of-the-art cybercriminals by opposing trans-border cybercrimes. When lowering risks, the DHS prioritizes investigative activities by employing high-impact inquiries into illegal uses of cyberspace. The idea is to investigate potential cyber threats to protect people, special events, federal facilities, and other critical roads and streets. The DHS collaborates with local law enforcement when investigating cybercrimes. The outcome is increased cooperation and better use of scarce law enforcement resources.

**Pillar IV: Consequence Mitigation:**
By mitigating consequences, the DHS minimizes the results from significant cyber events through a coordinated effort. The DHS recognizes that cyber incidents are increasing as the planet is becoming more connected. The DHS is working towards increased voluntary cyber incident reporting by the private sector or local law enforcement agencies. The DHS hopes to receive cyber incident reports to coordinate with other government agencies in mitigating and managing cyber incidents.

With increased cooperation among cyber victims comes better cyber incident reporting and more accurate cyber risk trend analysis. According to the Trump administration, the idea was to leverage DHS and non-DHS resources to develop comprehensive assessments of cyber adversaries, threats, and events to coordinate cyber planning and protective activities.

**Pillar V: Enable Cybersecurity Outcomes:**
The fifth pillar is a pledge by the DHS to further policies and activities that assure improved global cybersecurity risk management. By strengthening the security and reliability of cyber systems, conditions were established to promote cybersecurity goals. The objective of this pillar is to cultivate better software, hardware, and network cybersecurity.

Under President Trump, the DHS also desired to engage in advanced cybersecurity research, development, and innovative technology activities that support the DHS’s mission. By expanding international cooperation, the DHS proposed that the result would be a more reliable and secure Internet. The idea was for the DHS to implement cybersecurity efforts in an integrated and prioritized manner.

**COMPARING THE CYBERSECURITY APPROACHES UNDER PRESIDENTS TRUMP AND BIDEN**
The two national security strategies have much in common. For President Trump, protecting American national security and the prosperity of the American economy was paramount, where as President Biden stated that cybersecurity is a top priority for his administration, where strengthening the nation’s capability, readiness and resilience is imperative. President Trump suggested that the federal government work with the private sector to manage critical infrastructure, whereas President Biden declared that the federal government would collaborate with the private sector to manage and share risks, thereby securing a safe online environment.

According to President Trump, the federal government should update National Critical Infrastructure and Resilience Research and Development Plan, emphasizing new cybersecurity approaches to emerging technologies such as the next generation of telecommunications and information communications infrastructure. Under President Biden’s plan, his administration desired to defend the country effectively by delivering opportunities to Americans of diverse circumstances. President Trump wanted to improve...
international cooperation in investigating malicious cyber activities, while President Biden preferred the United States to reengage with its allies and partners on cyber-issues.\textsuperscript{79} Finally, President Trump sought to deter malicious cyber actors, whereas President Biden aspired to hold malicious actors accountable for their destructive, disruptive, and destabilizing cyber acts.\textsuperscript{80}

According to Lin, there were two significant differences between the cybersecurity approaches under President Trump and President Biden.\textsuperscript{81} First, President Biden stressed the significance of diversity in the national cyber talent pool, while President Trump failed to mention this national goal.\textsuperscript{82} Second, President Biden wanted the federal government to invest in cybersecurity, whereas President Trump desired the federal government to assist private sector investment in cybersecurity.\textsuperscript{83} According to Heckman, the recent SolarWinds breach that involved nine federal agencies was the reason why the Biden administration wanted the federal government to take a more significant role in national cybersecurity.\textsuperscript{84}

The second difference between the two approaches to national cybersecurity exemplifies the fact that Republican administrations defer to private enterprise, while Democratic administrations favor the federal government taking an active role. This is nothing new. However, the first difference is significant, and for the following reasons. According to Buresh, the talent pool for agile-driven and plan-driven software projects was approximately 85 percent male and 15 percent female.\textsuperscript{85} In 2020, (ISC)\textsuperscript{2} stated that women comprised 24 percent of the cybersecurity workforce.\textsuperscript{86} It appears that in the last 12 years, there has been a steady but small percentage (approximately 0.75 percent per year) increase in women entering the IT and cyber realm.

From a racial perspective, according to the Subcommittee on Cybersecurity, Infrastructure, and Innovation of the Committee on Homeland Security of the House of Representatives, only three percent of cyber professionals in 2016 were black. In contrast, African Americans comprised 13 percent of the American population.\textsuperscript{87} The (ISC)\textsuperscript{2} observed that as of 2020, 3.8 percent of cyber professionals were African American.\textsuperscript{88} In other words, in the four intervening years, the annual rate of increase in black cyber professionals was 0.2 percent, a percentage increase that could be attributed to sampling variation. Based on the statistics presented above, it is evident that the Biden administration will be hard-pressed in the coming four years to find African Americans to hire. It seems that what the Biden administration can expect is an incremental increase in hiring African Americans and other individuals of color to senior cybersecurity positions due to the apparent dearth of African Americans and other individuals of color in the cybersecurity talent pool. However, what can be accomplished relatively quickly is for the federal government and its agents to actively encourage African American college students and other college students of color to major and minor in cybersecurity and related fields with the understanding that employment with the federal government is readily available. It is this latter tactic that appears to be quite doable.

### CANADIAN APPROACH TO NATIONAL SECURITY STRATEGY

#### Overall National Security Approach

Canada’s national security approach balances national security needs against the country’s core values of openness, diversity, and respect for civil liberties.\textsuperscript{89} The three essential core national security interests for Canada include:\textsuperscript{90}

- Protecting Canada and its citizens at home and in other countries;
- Making sure that Canada is not a hub for threats to its allies; and
- Backing international security.

Canada’s national security policy employs the following organizations to build a unified security system consistent with the country’s policy goals:\textsuperscript{91}

- An Integrated Threat Assessment Centre that brings together all threat-related information so that it is accessible promptly to the individuals and organizations that need it;
- A National Security Advisory Council that consists of private security experts;
- A Cross-Cultural Roundtable on Security that is composed of different members of Canada’s ethnocultural and religious communities; and
- The Department of Public Safety and Emergency Preparedness is charged with testing and auditing the Canadian federal government’s essential security responsibilities and activities.

Canada’s national security policy’s key measures are intelligence, emergency planning and management, public health, transportation security, border security, and international security.\textsuperscript{92}

#### Specific National Security Issues

Canada’s approach to national security is that there is no conflict between its security and its values.\textsuperscript{93} The policy deals with the threats that can potentially destabilize the nation.\textsuperscript{94} Canada’s national security approach recognizes that security interests change over time as religious extremism, violent secessionist movements, state-sponsored terrorism, and domestic extremism manifest themselves.\textsuperscript{95} Canada desires to build an integrated national security system that can effectively respond to intentional and unintentional threats.\textsuperscript{96}

For Canada, intelligence is the foundation for protecting Canadians’ security, and working with its allies is paramount.\textsuperscript{97} Canada’s emergency planning and management approach is a decentralized and distributed methodology, dividing responsibilities among first responders, provinces, territories, and governmental departments.\textsuperscript{98} The SARS outbreak of 2003\textsuperscript{99} highlighted the challenges facing Canada’s public health system.\textsuperscript{100} The Canadian national security approach recognizes that public health is a strategic priority.\textsuperscript{101}

Because of Canada’s sheer size that spans the Atlantic and Pacific Oceans and the fact that terrorists have attacked mass transportation systems in the past, Canada realizes that it must participate with the United States in the security efforts protecting the North American transportation system.\textsuperscript{102} Part
of Canada’s national security strategy is to ensure that the U.S.-Canadian border is appropriately managed by improving border security and even more so in light of the Covid-19 pandemic. Finally, Canada’s approach is to cooperate effectively with international attempts to ensure that peace and security remain worldwide.

CANADIAN NATIONAL CYBERSECURITY APPROACH

The digital information revolution has changed the world. Digital technologies that were once hidden away in highly air-conditioned computer rooms are now an integral part of everyone’s daily lives. These technologies connect Canadians from coast to coast and involve nearly every Canadian’s action. The Canadian national security strategy foresees that there is seemingly endless potential for digital innovation benefiting communities, the nation, and the planet.

Canada’s federal government envisages a time in the not too distant future when Canadians actively shape the country’s cyber resilience efforts. The idea is that collaborative action while working together with advanced cyber research will ensure that the Canadian government is a global cybersecurity leader. The Canadian federal government intends to work closely with individual provinces to coordinate Canada’s cybersecurity environment. In this ever-changing environment, Canada desires to protect Canadians’ safety and security, promote personal freedoms online, and inspire business cybersecurity efforts across jurisdictions and economic sectors.

The Canadian national cybersecurity approach is a top-down effort beginning with the federal government. The plan seeks to be more inclusive by encouraging the Canadian government to work effectively with internal and external partners. Canada intends to align its national cybersecurity strategy with the mandate from the Minister of Democratic Institutions to protect the democratic electoral process from cyber threats and to ensure that the use of cyber weapons inadequately mitigated.

COMPARISON OF THE NATIONAL SECURITY STRATEGIES OF THE UNITED STATES AND CANADA

The first thing to notice when comparing the United States and Canada’s national security strategies is that U.S. strategic documents refer to strategic pillars. In contrast, the Canadian position papers possess no such corresponding imagery of edifices. The Canadian national security strategies seem to be much more practical. Canada does not suffer from the expectation that the nation will influence world events by advancing a Canadian strategic agenda.

Both countries are dedicated to protecting their respective citizens and their homeland. The Canadian national security policy is less concerned with preserving the Canadian way of life than the American security document. Currently, about 32.3 percent of Canadians consider themselves to be ethnically Canadian. Other major ethnic groups include English (18.3 percent), Scottish (13.9 percent), French (13.6 percent), Irish (13.4 percent), German (9.6 percent), and Chinese (5.1 percent). In contrast, the population demographics of the United States include white (61.3 percent), Hispanic (17.8 percent), African American (12.7 percent), and American Indian, Alaska Native, Asian American, Native Hawaiian, and Other Pacific Islander (8.2 percent).

Although many Canadian people identify themselves by nationality, the vast majority of Canadians are white. In some sense, the “Canadian Dream” is quite different from the “American Dream.” This means that the Canadian national security strategy can focus on practical strategic considerations rather than cloaking its national security strategy in a unified people’s myth like it is in America. In the United States, the first pillar of its national security strategy appears to be concerned with the American way of life, or the “American Dream.”

The second pillar of the American national security strategy is dedicated to promoting American prosperity. The Canadian document also discusses its citizenry’s economic well-being, but it does not appear to be such a burning issue in the United States. The third pillar of the American national security strategy is preserving peace through strength. This contrasts with the Canadian perspective that order is to be achieved by cooperating and collaborating with the country’s allies such as the United Kingdom, Australia, New Zealand (all of whom are members of the British Commonwealth), the United States of America, and other nations. The Canadian national security strategy also promotes cooperation and collaboration with the other countries of the world without the onerous burden of exercising its economic prowess.

Because Canada has a significant landmass, most of its 37 million citizens live reasonably to the U.S. border, but rarely above the Arctic Circle. The nation does not possess nearly the economic power of its nearest Southern neighbor. Canada is merely unable to dominate other countries. In fact, by being part of the British Commonwealth, the country’s national security strategy need not engage in political blustering. Instead, Canada quietly promotes its security interests via a more subdued approach consistent with the British understatement’s practical employment. In my opinion, as a whole, Canada’s national security strategy is more focused on specific security issues than its American counterpart.

The only caveat in the Canadian national security strategy is that to stay ahead of President Trump on security, the nation needs a holistic review of its security policies. In his first week in office, three of the first five executive orders from President Trump dealt with illegal immigration into the United States. These executive orders had international consequences. Being America’s Northern neighbor, Canada felt the brunt of their effect. Because President Trump initially chose three former military generals to fill America’s highest national security positions (i.e., Def. Sec. James Mattis, Sec. HL Sec. John Kelly, and Natl. Sec. Adv. H. R. McMaster), this trio was goal-oriented and mission-focused, demanding decisive security thought and planning. Canada’s reaction had been to assess President Trump’s seemingly unpredictable edicts and tweets.
quickly. In other words, to cope with a dynamic and unstable neighbor, Canada appeared to have been faced with the proposition of creating a much more holistic approach to national security. Canada was being prodded to become more aligned strategically with the United States without the luxury of resorting to Canadian hegemony. In other words, President Trump seemed to be implicitly demanding that Canada become more like a sycophantic vassal state than a strategic partner, possibly straining Canada’s ties with the United Kingdom and the British Commonwealth.

COMPARISON OF THE NATIONAL SECURITY CYBER STRATEGIES OF THE UNITED STATES AND CANADA

Regarding national security cyber strategies, the United States, having a much larger economy and population than Canada, the two countries’ policies seem to be intertwined. Given that the cyber policies of President Trump and President Biden is quite similar, with only the two differences discussed above. This may not be due to the disparities between the American and Canadian approaches to cyber threats, but rather because cyberattackers seem to have a culture of their own. Anyone on the planet can be a cyber attacker because cyberattack tools are either free or very inexpensive and because the Internet is both pervasive and ubiquitous. Canada, the United States, and other nations face the inevitable proposition of being electronically attacked daily.

A significant difference between the United States and Canada’s national security strategies is that Canada is more of a socialist country than America. Americans seem to pride themselves regarding their independence. This difference in philosophical perspective permits Canadian companies to work with the Canadian government cooperatively. In contrast, American companies and individuals are loathed to work with their government, even when it is in their best interest to do so. The result is that private American companies distrust the American government sufficiently to ensure that cyber attackers can exploit this chasm between government and private industry effectively. Even so, in contrast to the American cybersecurity approach under President Trump, President Biden seems to promote a more inclusive approach, remarkably similar to the Canadian approach to cybersecurity. This blending of the two cybersecurity strategies may positively affect cooperation between the two nations when addressing and mitigating cyber threats. Although the Biden administration’s document on strategic national security is an interim expression, it may turn out that in the succeeding four years, the United States and Canada’s cybersecurity strategies could become seemingly indistinguishable from one another. Only time will tell whether this suggested evolution will occur and whether the proposed progression will be in both country’s best interests.

CONCLUSION

In conclusion, the United States and Canada share many common goals and objectives. The strategic problems arise when these separate nations diverge not because of distinct technical approaches but because of the cultural differences that form the hidden basis of each country’s national security strategies. The Canadian culture is a blending of the culture of the British, French, and indigenous populations. Canada is a progressive, diverse, and multicultural society, where the government emphasizes the importance of immigration. The country tends to promote a just society where civil rights are constitutionally protected.

The culture of the United States is a mixture of Western European culture. Still, it has also been influenced by African, Asian, Latin American, Native American, and Polynesian peoples and their cultures. The United States is ethnically and racially diverse, probably far more than Canada. The American culture is also different depending on the region of the country. The result is that the national security strategies reflect the variations of cultures of the two nations. The international presence of the United States and Canada is striking. America is a dominant superpower, whereas Canada typically follows its neighbor’s lead. The result is that the two countries’ national security and national cybersecurity strategies effectively mirror these distinctions. It is the nature of the approaches that are being compared.

ENDNOTES

1 Steph Koyfman, Which Are The Most Spoken Languages in Canada?, Babbel Magazine, September 26, 2017, available at https://www.babbel.com/en/magazine/most-spoken-languages-in-canada/.
2 Janice Cheryl Beaver, U.S. International Borders: Brief Facts, CRS Report for Congress, November 8, 2006, available at https://fas.org/sgp/crs/misc/RS21729.pdf.
3Id.
4Id.
5 Ron Dungan, A Moving Border, and the History of a Difficult Boundary, USA Today, n.d., available at https://www.usatoday.com/border-wall/story/us-mexico-border-history/510833001/.
6Coronavirus Disease (COVID-19): Who Can Travel to Canada – Citizens, Persons Registered under Canada’s Indian Act, Permanent Residents, Foreign Nationals and Refugees, Government of Canada, February 21, 2021, available at https://www.canada.ca/en/immigration-refugees-citizenship/services/coronavirus-covid19/travel-restrictions-exemptions.html.
7 Johanna Read, Rules & Regulations for Crossing the Canadian Border, USA Today, July 26, 2018, available at https://traveltips.usatoday.com/rules-regulations-crossing-canadian-border-21206.html.
8Id.
9The Case for Building a Wall to Keep Canadians Out, The Economist, June 3, 2017, available at https://www.economist.com/united-states/2017/06/03/the-case-for-building-a-wall-to-keep-canadians-out.
Canada and United States Relations, Government of Canada, n.d., available at http://international.gc.ca/worldmonde/united_states-etats_unis/relations.aspx?lang=eng.

Daniele Hadi Irandoost, Cybersecurity: A National Security Issue?, E-International Relations Students, May 3, 2018, available at http://www.e-ir.info/2018/05/03/cybersecurity-a-national-security-issue/.

National Security Strategy of the United States of America, President of the United States, December 2017, available at https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Id. at 1.

Id. at 2.

Id. at 3.

Id. at 4.

Id. at 7.

Id. at 8.

Id. at 10.

Id. at 12.

Id. at 14.

Id. at 17.

Id. at 19.

Id. at 20.

Id. at 25-27.

Id. at 28-31.

Id. at 31-32.

Id. at 37.

Id. at 38.

Id. at 41.

Joseph R. Biden, Jr., Interim National Security Strategic Guidance, The White House, March 03, 2021, available at https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

Id. at 6.

Id. at 7.

Id.

Id.

Id. at 9.

Id. at 11.

Id.

Id. at 11-12.

Id. at 12.

U.S. Department of Homeland Security Cybersecurity Strategy, U.S. Department of Homeland Security, May 15, 2018, available at https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

Id. at 1.

Id. at 2.

Id.

Id.

Id. at 3.

Id. at 5.

Id. at 7.

Id.

Id. at 8.

Id.

Id. at 10-11.

Id. at 11.

Id. at 12.

Id.

Id. at 13.

Id. at 15.

Id. at 16.

Id.

Id. at 16-18.

Id.

Id. at 19.

Id.

Id. at 20.
67 Id. at 21.
68 Id.
69 Id. at 22.
70 Id.
71 Id. at 23.
72 Id. at 24.
73 Id. at 25.
74 Herb Lin, How Biden’s Cyber Strategy Echoes Trump’s, Lawfare, March 03, 2021, available at https://www.lawfareblog.com/how-bidens-cyber-strategy-echoes-trumps.
75 Id.
76 Id.
77 Id.
78 Id.
79 Id.
80 Id.
81 Id.
82 Id.
83 supra, note 86.
84 Jory Heckman, Biden Makes Cybersecurity ‘Top Priority’ in National Security Guidance, Federal News Network, March 04, 2021, available at https://federalnewsnetwork.com/cybersecurity/2021/03/biden-makes-cybersecurity-top-priority-in-national-security-guidance/.
85 DONALD L. BURESH, CUSTOMER SATISFACTION AND AGILE METHODS: ASSESSING CUSTOMER SATISFACTION AND AGILE METHODS (Verlag Dr. Mueller 2009).
86 (ISC)² Staff, Women in Cybersecurity: Young, Educated and Ready to Take Charge, (ISC)², 2020, available at https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx.
87 Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, Committee on Homeland Security of the House of Representatives, Serial No. 116-22, May 21, 2019, available at https://www.govinfo.gov/content/pkg/CHRG-116hhrg37868/pdf/CHRG-116hhrg37868.pdf.
88 (ISC)² Staff, supra, note 86.
89 Securing an Open Society: Canada’s National Security Policy, Canada Privy Council Office, April 2004, available at http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf.
90 Id. at vii.
91 Id. at vii-viii.
92 Id. at viii-xi.
93 Id. at 1.
94 Id. at 3.
95 Id. at 6.
96 Id. at 9-10.
97 Id. at 15-17.
98 Id. at 21.
99 CDC SARS Response Timeline, Centers for Disease Control and Prevention, n.d., available at https://www.cdc.gov/about/history/sars/timeline.htm.
100 Securing an Open Society at 29, note 89.
101 Id. at 31-34.
102 Id. at 35.
103 Id. at 41.
104 Id. at 47.
105 National Cyber Security Strategy: Canada’s Vision for Security and Prosperity in the Digital Age, Public Safety Canada, 2018, available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.
106 Id. at 2.
107 Id. at 3.
108 Id.
109 Id.
110 Id. at 4.
111 Id.
112 Id. at 5.
113 Id.
114 Id.
115 Canada Population 2018, World Population Review, June 12, 2018, available at http://worldpopulationreview.com/countries/canada-population/.
116 Id.
