CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Offensive Shifts, Offensive Policies: Cybersecurity Trends in the Government-Private Sector Relationship

by Tom Robertson & Simon Van Hoeve

August 2019

POLICY PERSPECTIVE

OFFENSIVE SHIFTS, OFFENSIVE POLICIES: CYBERSECURITY TRENDS IN THE GOVERNMENT-PRIVATE SECTOR RELATIONSHIP

by Tom Robertson & Simon Van Hoeve

August 2019

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
1800, 421 – 7th Avenue S.W., Calgary, AB T2P 4K9
www.cgai.ca

ISBN: 978-1-77397-082-0

Cyber-security is a key risk for decision-makers at both the state and corporate level. There is a relative lack of academic literature examining the impact of foreign cyber-attacks on business and the private sector. This paper examines foreign, state-sponsored threats facing the private sector, investigates the key shortcomings of recent Western government policies, and proposes a series of considerations for future policies that will help mitigate the impact of state-sponsored hostile activity toward the private sector.

Foreign Threats, Domestic Effects

States tend to use cyber-attacks against the private sector in equal or greater frequency as they do against governments. The Dyadic Cyber Incidents Dataset (version 1.5), a database created by several prominent cybersecurity scholars to record all publicly available cyber-incidents from 2000 through 2016, demonstrates this trend.[1] This dataset lists 85 major cyber-attacks by foreign governments against the private sector. Of those, 43 were against the American private sector compared to a total of 96 cyber-attacks against the American government, military and the private sector combined. Thus, 45 per cent of cyber-attacks directed at America targeted the private sector, dramatically more than those suffered by any other state's private sector. Only Ukraine and South Korea had near double-digit numbers of cyber-attacks against corporations; they are two countries under the near-constant threat of attack from a close neighbour.

With the caveat that the private sector in the U.S. and other Western countries includes services often deemed essential and thus government-controlled in other countries, such as utilities and communications, it is clear that the private sectors in Western nations are targeted for more than simple cyber-crimes. Many geopolitical rivals, notably Iran, North Korea, China and Russia, view the private sector as a legitimate target and they see successful attacks as advancing their geopolitical objectives.

North Korea

North Korea uses cyber-operations to further two strategic objectives. First, cyber-operations are a relatively inexpensive and easy way to undermine foreign governments and attempt to impose North Korean will abroad. A prominent example of the success North Korea can have deploying cyber-operations was the 2014 Sony Pictures hack, when North Korean hackers installed malware to prevent the release of, and in retaliation for, Sony's satirical comedy, *The Interview*, depicting Kim Jong Un's assassination.[2]

Second, North Korea is increasingly using cyber-operations as a source of revenue for the regime, benefiting from the anonymity and fluidity of digital crime to offset and limit the success of

[1] Ryan Maness, Brandon Valeriano and Benjamin Jensen, "The Dyadic Cyber Incident and Dispute Data, Versions 1, 1.1, and 1.5." Available at https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset. Accessed on June 27, 2019.
[2] Devlin Barrett and Ellen Nakashima, "U.S. Charges North Korean Operative in Conspiracy to Hack Sony Pictures, Banks," *Washington Post*, Sept. 6, 2018.

economic sanctions. UN experts have estimated that over the past few years, North Korea has stolen around $650 million from financial institutions via cyber-attacks and ransomware.[3] Within that number is $81 million stolen from the Central Bank of Bangladesh, one of the largest bank heists in history. The North Koreans originally intended to steal $1.1 billion, and were only stopped when U.S. Central Reserve systems blocked the transfer. Interestingly, North Korea is one of the few countries to use cyber-operations for financial gain at the state level. Other states tend to stick to more traditional means, namely espionage.

North Korea suffers little retaliation for its cyber-operations, as the international community's deterrent efforts focus primarily on North Korea's nuclear ambitions and other higher priority targets; moreover, North Korea's aged and often antiquated cyber-infrastructure limits the effectiveness of the modern offensive cyber-programs. Former NSA deputy director Chris Inglis captures this paradox nicely: "Cyber is a tailor-made instrument of power for them … There's a low cost of entry, it's largely asymmetrical, there's some degree of anonymity and stealth in its use. It can hold large swaths of nation state infrastructure and private-sector infrastructure at risk. It's a source of income."[4] North American corporations especially remain targets for North Korea, as they have the money to be stolen, and they serve as effective propaganda targets for the regime.

Iran

Along with China and Russia, Iran tends to pursue offensive cybersecurity operations more for geopolitical capital.

Iran was one of the original targets of state-sponsored cyber-operations, and in response quickly became one of the original antagonists. Concerned about Iran's rising nuclear abilities and aspirations, the United States and Israel jointly developed Stuxnet, a computer worm which infects nuclear reactor computers by subtly changing certain functions to sabotage uranium production. It was released on the Iranian nuclear program between 2010 to 2012, severely setting back the program.[5]

In response, Iran has been steadily increasing investments in both defensive cyber-capabilities and offensive operations. Unsurprisingly, since this increased investment began, Iran has been identified as a culprit in numerous cyber-attacks. Prominent examples include cyber-attacks on American casinos in 2014 and attacks on dozens of North American banks in 2012. Iran claims these attacks were committed by Islamic groups not associated with the Iranian government; however, experts point to analyses which strongly suggest these groups were sponsored by and operating for the Iranian government.

[3] UN Security Council, "Final Report of the Panel of Experts Submitted Pursuant to Resolution 2407 (2018)," March 5, 2019. Available at https://www.undocs.org/S/2019/171 48-52.
[4] David Kirkpatrick, Nicole Perlroth and David Sanger, "The World Once Laughed at North Korean Cyberpower. No More," *New York Times*, Oct. 15, 2017.
[5] David Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012.

Given the recent rise in tensions between Iran and the West, escalating cyberwarfare appears to be looming. In May 2019, the United States launched cyber-attacks against an Iranian intelligence group in response to Iran downing an American drone.[6] However, the administration was aware that American industry might feel the effects, as reports state that administration officials had warned industry to be aware of potential cybersecurity threats emerging from Iran.[7]

China

The majority of Chinese cyber-operations are for gaining economic advantages over rivals through espionage, intellectual property theft and disruption.

Chinese theft of IP and trade secrets has long been a problem. The National Counterintelligence and Security Center (NCSC) pointed to numerous examples in its 2018 report, Foreign Economic Espionage in Cyberspace, and ultimately concluded: "We believe that China will continue to be a threat to U.S. proprietary technology and intellectual property through cyber-enabled means or other methods. If this threat is not addressed, it could erode America's long-term competitive economic advantage."[8]

Other Chinese cyber-operations exist to undermine business competitors. Concrete examples of such Chinese cyber-attacks include the 2017 breaches into IBM and Hewlett Packard, which allowed Chinese operatives access to client computers, and the more-publicized 2018 Marriott breach, which exposed the data of over 500 million customers.

Russia

Russia uses cyber-attacks more as a political tool to undermine public confidence, send a message to a foreign state or coerce. Two notable examples are the involvement in the 2007 cyber-attacks on Estonia and the 2016 U.S. presidential elections. In 2007, the Estonian government created a tense situation between Estonia and its Russian-backed Russian minority after moving a statue that had sentimental meaning. Over the next 22 days, Estonia was hit with a massive directed denial-of-service (DDoS) attack which knocked out much of the country's internet capability. Estonian officials determined that Russia was the only likely instigator of these attacks.[9]

While the purpose of the Russian attacks on Estonia was political, it also damaged sectors with little political motivation, including the private sector. One dramatic instance of such an attack was the computer malware called NotPetya, deployed in 2016. Part of a cyber-attack on Ukraine by Russian-sponsored activists, the virus achieved the intended goal of disrupting a significant number of Ukrainian corporations. However, it then went on to infect numerous non-Ukrainian companies, causing around $10 billion in damage worldwide, most of it outside Ukraine. The

[6] Julian Barnes and Thomas Gibbons-Neff, "U.S. Carried Out Cyberattacks on Iran," *New York Times*, June 22, 2019.
[7] Ellen Nakashima, "Trump Approved Cyber-Strikes against Iran's Missile Systems," *Washington Post*, June 22, 2019.
[8] National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace," 2018. Available at https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf 7.
[9] Rain Ottis, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective," *Proceedings of the 7th European Conference on Information Warfare and Security*, Plymouth, 2008 (2008): 163-168.

Maersk shipping line was one of those accidentally affected; the virus destroyed sensitive Maersk operations data. Beyond the reported $200 million Maersk suffered in damages, normal shipping was severely disrupted for hundreds of customers, affecting many companies not targeted by the cyber-attack.[10]

Similarly, Russian cyber-attacks often exploit existing services and prevent corporations from achieving their goals. The Russian government's interference in the 2016 U.S. presidential election demonstrates this well. Instead of committing DDoS attacks against election servers, or some other form of direct attack, the Russians ran a more subtle cyber-campaign through infiltrating and utilizing previously trusted sources to attack election integrity.[11] By exploiting North American corporations such as Facebook and Twitter, Russia was able to conduct a sophisticated "influence operations" attack on a rival's integrity and credibility while avoiding most forms of hard evidence linking it to the attacks. This subtle form of cyber-attack is often as detrimental to a corporation as a large-scale attack, as it erodes public trust and confidence in these companies and forces the company to be both a victim of an attack and an unwilling perpetrator of a crime.

What are the Responses?

Given these threats, most Western governments have been creating cyber-units to deal with protecting national cyber-assets, defending the private sector and individuals, and carrying out offensive cyber-attacks of their own. Traditionally, most Western countries have adopted a more reactive and defence-oriented strategy. However, this appears to be changing. With shifting administrations, certain states with traditionally more defensive cyber-policies are adopting more offensive ones.

Notably, in the United States the U.S. Cyber Command (the division of the Department of Defense in charge of cyber-operations) has been adopting a new, more aggressive doctrine, which we saw played out recently with increased American offensive cyber-operations. Numerous scholars have spoken out about these changes. Some, such as Brandon Valeriano and Benjamin Jensen, have written against adopting an offensive strategy, claiming an active defence is much more effective. They note that under the previous defensive strategy, cybersecurity has been fairly acceptable, with the cyber-operations being relatively ineffective and serving more to relieve tensions.[12] These benefits would only be heightened if the U.S. were to increase defensive cybersecurity practices such as target hardening. Others, such as retired Gen. Keith Alexander and Jamil Jaffer, have called for a more offensive aspect to U.S. cybersecurity, claiming that a more robust offensive ability is needed to deter attacks.[13]

---

[10] Lee Matthews, "NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million," *Forbes,* Aug. 16, 2017.
[11] U.S. Congress, Senate Select Committee on Intelligence, *Russian Interference in the 2016 U.S. Elections,* 115th Cong., 1st sess., 2017.
[12] Brandon Valeriano and Benjamin Jensen, "The Myth of the Cyber Offense: The Case for Restraint," *Cato Institute Policy Analysis* no. 862 (January 2019), 5-7.
[13] Keith Alexander and Jamil Jaffer, "Ensuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition," *Georgetown Journal on International Affairs* 19, Fall (2018), 57.

Lacking in the current debate about the direction of state responses to cyber-attacks is a discussion about how governments can react to foreign cyber-attacks in a manner that remains conducive to a healthy business environment. Many regulations and actions a government can take to protect the private sector may have unanticipated and negative repercussions for the private sector itself. In some cases, legislation is ineffective, outdated and overly costly. In others, government action has actually imposed unreasonable additional burdens on the private sector. Let us explore these pitfalls and examine how to prevent them from imposing costs.

Speed of Regulation

One major issue between government and the private sector is the speed at which legislation about cybersecurity can be created and passed, as it is typically much slower than the speed of technological change. This can cause a mismatch between policy and current situation. Proper legislation can take years to study, draft, present, formalize and then put into practice. In that time, cybersecurity technology has often already moved on, which can make these new laws outdated and obsolete. Also, technology companies themselves are often better at discovering and implementing new standards of safety and security than the government, due to a vested interest in keeping their data secure. Many companies work hard to uphold a reputation of security and privacy when dealing with data. Others have valuable trade secrets, designs and data which give them advantages over competitors.

Both of these issues can be seen when looking at the Cybersecurity Strategy Report, released by the Energy and Commerce Committee in December 2018.[14] At the end of 2013, the public learned that Target (a major American and then-Canadian department store) had suffered a massive data breach affecting credit card scanners. This incident sparked the start of this report in late 2013. However, the final report's reception was not as well received as the creators might have hoped. As Joseph Marks wrote in the *Washington Post*, "Five years later, their [the committee's] laborious process of roundtables, formal requests for information and letter writing campaigns to companies has only nudged the Internet ecosystem toward mildly better cybersecurity."[15] In essence, from this five-year report the committee was unable to produce any form of policy recommendations, only providing an overview of the field and highlighting risk areas.

One particular incident in the report highlights the disconnect between government and business. In January 2018, the committee members sent several letters to top American technology companies expressing concern about chipset security and vulnerabilities. These letters emphasized the need for collaboration and information sharing to have a collective response against these threats. According to the final report, the recipients acknowledged these concerns and provided some more insight into their process. However, in a letter to Roberta Stempfley, director of the Software Engineering Institute at the CERT Coordination Center at Carnegie

[14] Committee on Commerce and Energy, "Cybersecurity Strategy Report," December 2018. Available at https://www.hsdl.org/?view&did=819388
[15] Joseph Marks, "The Cybersecurity 202: Internet Ecosystem Needs a Complete Overhaul to be Cybersecure, House Panel Warns," *Washington Post*, Dec. 10, 2018.

Mellon University, the chairs of the Committee on Commerce and Energy and the Committee on Commerce, Science and Transportation described industry's responses in a bit more detail. All these corporations had been aware of these vulnerabilities months before the committee and other U.S. government organizations had known about them. These companies also explained that their best-practice standards were to disclose information of such vulnerabilities to as small as a group as possible to avoid bad actors learning of and exploiting them, until they had released a patch eradicating the vulnerability.[16] Seemingly unknown to the government, corporations had been a step ahead of the government the whole time.

To combat such inefficiencies, the government-industry collaboration that is often talked about within documents such as the USCYBERCOM Command Vision and the Canadian defence policy should be implemented to a greater extent than it already is. For the American Energy and Commerce Committee, the issue was one of communication and mistrust. The private sector and the government were not on the same page, and the private sector did not trust the government with certain information the government needed to craft effective policy. These relationships need to be fostered via desirable incentives, such as giving leading industry experts a better seat at the table than they already have.

Too Costly

A common critique by those leaning to the right of the political spectrum is the costs that government puts on business. Regulation can be an effective tool in forcing standards of compliance and security on an industry. However, there are concerns that while regulation may be effective, the costs of cybersecurity regulation are unnecessarily high.

Arguably, a more potent critique of certain governments' regulation attempts for cybersecurity is that regulation implies a failure to secure. Consider the 2016 Network and Information Security (NIS) directive, which the EU is currently implementing. This directive requires EU member states to create legislation which demands minimal security standards in critical networks such as health care, natural resources and telecommunications. While the directive's net goal of increasing resilience to cyber-attacks might be desirable for most businesses, the implications of certain sections of the NIS are not. Particularly, under section 14(1), there is a passage which reads:

> Member States shall ensure that operators of essential services take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in their operations.

[16] Letter to Roberta Stempfley. Available at https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2018/jul/cs2018_0306.pdf. Retrieved June 27, 2019.

> Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.[17]

In the above passage, the European Parliament is claiming that the burden of protecting an essential corporation from any cyber-attack, including a foreign one, lies primarily with the corporation itself and therefore the corporation can be held accountable. The notion of a private entity being responsible for protecting itself from a foreign government's attack is unique to the field of cybersecurity. As Alexander and Jaffer state, "we do not expect Target to employ surface-to-air missiles to defend itself against Russian planes dropping bombs in the United States. Rather, that responsibility belongs to the DoD."[18] While this is not to say that corporations should be entirely off the hook when it comes to security against foreign cyber-attacks, it does make the possibility of receiving multi-million-dollar fines after a foreign cyber-attack for poor security appear very unfair. To continue Alexander's metaphor, we can assign blame to Target for getting robbed if they fail to install security cameras or hire nighttime security guards. But it seems a stretch to assign blame to Target for failing to prevent a foreign state's attack.

In the end, regulation poses a difficult question – namely, what is a reasonable cost to ask of private corporations for ensuring proper cybersecurity, and what is an unreasonable cost to ask?

If imposing regulation, these costs need to be clearly communicated, with the government presenting itself as a partner to help solve lapses in protection, rather than a watchdog. Governments should look at the changes implemented in the air travel industry worldwide after 9/11 as a guide. Antony Tyler, former director general and former CEO of the International Air Transport Association (IATA), wrote that two key lessons from the 9/11 fallout were that airlines should not be expected to be alone in the face of foreign threats – both government governance and financial assistance are expected for an appropriate defence.[19] The cyber-industry needs similar drastic security improvements to prevent a cyber-9/11.

Forcing Companies into the Fray

There is also the fear that a government may indirectly force a corporation into a cyber-conflict through narrowing its options, such as forcing a telecommunications company to assist in a government-sponsored attack. The U.S. government has passed various acts in the last few years which set a worrisome outlook for the private sector's freedom to deny the federal government access to sensitive data stored or intellectual property owned in the name of homeland defence. One particularly high-profile case was that of FBI vs. Apple.[20] While this case did not concern a cyber-attack, there are various parallels. In 2016, the FBI was investigating the 2015 San

[17] "European Parliament and Council Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union," (2016) *Official Journal* L194 20.
[18] Keith Alexander and Jamil Jaffer, "Clear Thinking about Protecting the Nation in the Cyber Domain," *The Cyber Defense Review* 2, no. 1 (2017), 33.
[19] International Air Transport Association, "The Impact of September 11, 2001 on Aviation." Available at https://www.iata.org/pressroom/Documents/impact-9-11-aviation.pdf
[20] Eric Lichtblau and Katie Benner, "Apple Fights Order to Unlock San Bernardino Gunman's iPhone," *New York Times*, Feb. 17, 2016.

Bernardino terrorist attack, and wanted to access some information on one of the perpetrators' iPhones. However, the FBI couldn't bypass the encryption. After Apple refused to write them software which would allow them to bypass iPhone security, the FBI obtained a court order to get Apple to assist them. Apple opposed this order; however, the FBI was eventually successful in bypassing the encryption themselves and dropped the lawsuit. Many present this episode as a case of the government's willingness to override privacy in favour of national security, but it also demonstrates that the government is willing to put national security threats ahead of the private sector's interests.

Unfortunately, there is no easy answer here either, as to how future situations like these should be handled. When faced with national security and protecting intellectual property, the duties of the government and those of the private sector to the people and the shareholders conflict.

Government Negligence to Private Harm

Finally, there are a few select cases where a government's own negligence directly caused harm to the private sector's cybersecurity. In 2017, the National Security Agency (NSA) lost control of a cyber-weapon it developed called EternalBlue after a data breach. EternalBlue works off a security vulnerability in Microsoft platforms. It proved so successful and valuable that the NSA did not inform Microsoft about the vulnerability for years. After EternalBlue was breached to the public, it became a vital component of numerous cyber-attacks, including the NotPetya malware discussed above. Somewhat ironically, many cities across the U.S., such as Baltimore and San Antonio, have suffered massive ransomware attacks targeting municipal systems using the NSA-created EternalBlue exploit.

It is easier said than done, but governments cannot let such breaches happen. Beyond directly putting a country's own citizens at risk via the tools crafted to protect them, such breaches undermine the government's reputation and authority to make and enforce regulations for the private sector.

Risks of Escalation

Most distressing is the fear of escalation in cyber-conflict driven by government responses. Today, more and more countries are stepping up their offensive cyber-operations alongside the host of traditional rogue actors using these tactics, such as China and Russia. One of these apparent new converts to offensive cyberwarfare is the United States. We can see evidence of this in both defence documents such as the 2017 National Security Strategy and increased American activities in the cyber-sphere, such as the recent actions against Russian infrastructure and the aforementioned Iranian cyber-operations. However, new concerns accompany these new offensives.

In particular, scholars are beginning to fear that if these offensive cyber-engagements are not handled deftly, they may lead to escalating cyber-conflict around the world. Valeriano and Jensen

specifically outline their objections to the new offensive cyber-strategy in their paper, The Myth of the Cyber Offense. They describe how under former president Barack Obama and the previous, more defensive-oriented policy, tit-for-tat escalation did not develop. Because America did not respond aggressively to offensive cyber-attacks aimed at it, cyber-attacks became a release valve for international tensions, as they allowed a country to take what it viewed as meaningful action against its rival, but not suffer a strong response, thus often seeing no escalation occur.[21] However, under the new offensive cyber-policy, responding to cyber-attacks aggressively would destroy this de-escalatory feature of one-sided cyber-conflict.

Also, Valeriano and Jensen say that unprovoked offensive actions make it easy for rivals to mistakenly escalate, claiming "What the United States call(s) defending forward, China and Russia will call preemptive strikes."[22] This sentiment is shared by other scholars, such as Mischa Hansel, who in his article, Cyber-Attacks and Psychological IR Perspectives: Explaining Misperceptions and Escalation Risks, discusses the susceptibility of states to misinterpreting and then unnecessarily escalating certain cyber-incidents.[23]

With the very real threat of escalation, it becomes clear that adopting an offensive cyber-policy runs the real risk of increased cyber-attacks against the U.S. and American businesses. Considering the already high numbers of major cyber-attacks against American corporations, the prioritization of projecting American power abroad seems turned around from where the real need for improvement lies – strengthening American cyber-defences at home.

Conclusion

Throughout this paper, we have established that there is a plethora of cybersecurity risks facing the North American private sector from a host of rival foreign states, including North Korea, Iran, Russia and China. However, in attempting to protect the private sector from threats like these, governments cannot forget that their own protections may also cause additional hardships for corporations. These concerns must be kept in the forefront when creating policy to ensure a healthy government-corporation partnership to fight off foreign threats.

[21] Valeriano and Jensen, "The Myth of the Cyber Offense," 7.
[22] Ibid.
[23] Mischa Hansel, "Cyber-Attacks and the Psychological IR Perspectives: Explaining Misperceptions and Escalation Risks," *Journal of International Relations and Development*, 21 no 3. (2018).

About the Author

Tom Robertson *is the managing partner of 3i Partners, a Toronto-based risk consultancy firm. He also holds ownership interests in several technology companies, including Xpresschek Inc., and Identity First Corp. Earlier in his career, Tom spent a decade in the financial services sector where he developed an appreciation for the intersection of state security and the private sector. Tom has an undergraduate degree from RMC, completed graduate studies at Carleton University, and holds several industry certifications.*

Simon Van Hoeve *is an analyst at 3i Partners, specializing in qualitative research and analysis in strategy and cybersecurity. He will be completing his studies at the University of Waterloo in December 2019.*

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.