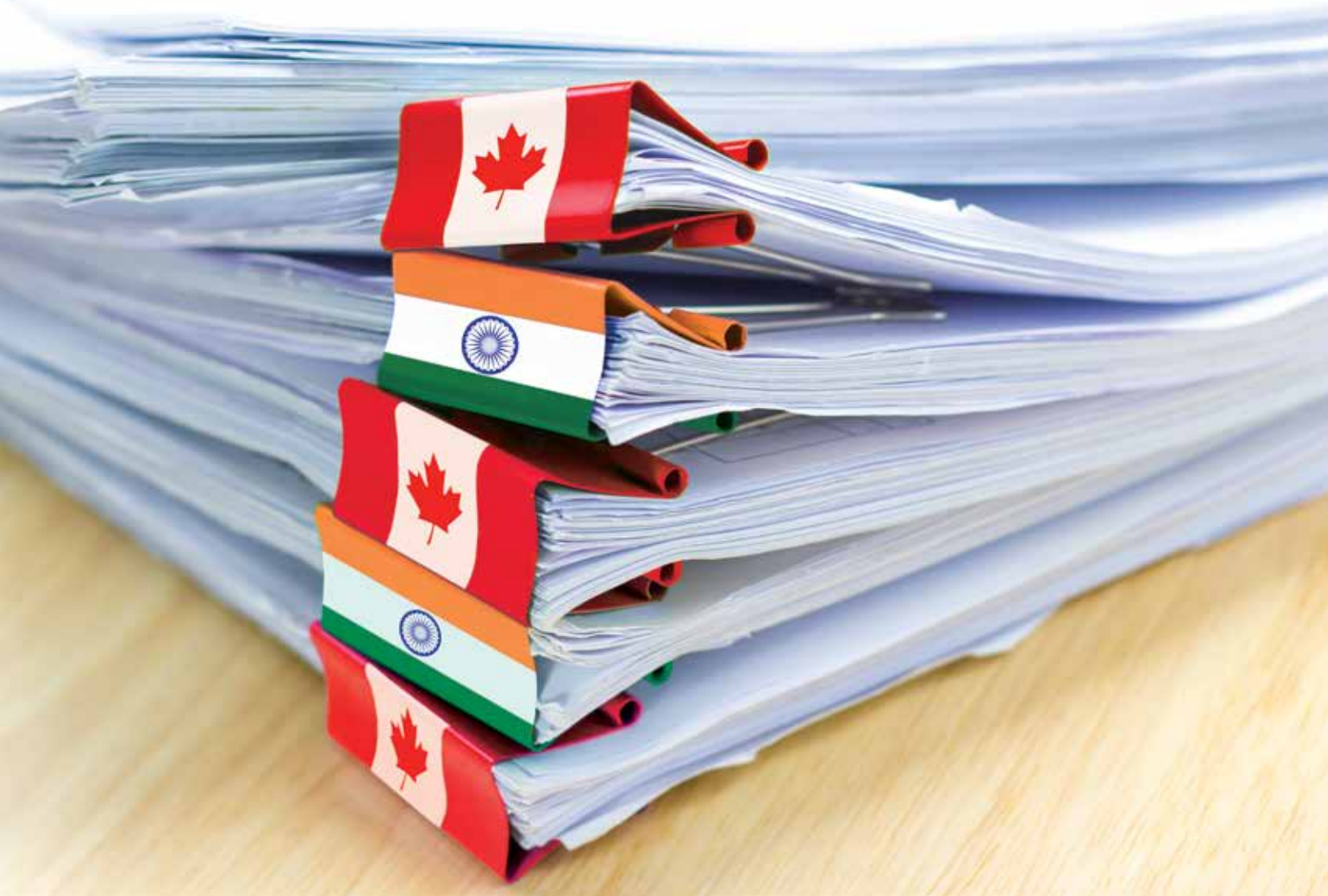
Centre for International Governance Innovation

GATEWAY HOUSE
INDIAN COUNCIL ON GLOBAL RELATIONS
भारतीय वैश्विक संबंध परिषद्

Canada-India Track 1.5 Dialogue Paper No. 1

Opportunities for Cooperative Cyber Security

Aaron Shull



Canada-India Track 1.5 Dialogue Paper No. 1

Opportunities for Cooperative Cyber Security

Aaron Shull

Centre for International Governance Innovation

GATEWAY HOUSE
INDIAN COUNCIL ON GLOBAL RELATIONS
भारतीय वैश्विक संबंध परिषद्

Centre for International Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

GATEWAY HOUSE
INDIAN COUNCIL ON GLOBAL RELATIONS
भारतीय वैश्विक संबंध परिषद्

Cecil Court, 3rd floor, Next to Regal Cinema,
Colaba, Mumbai – 400 005,
India

Table of Contents

About the Author

As CIGI's managing director and general counsel, Aaron Shull acts as a strategic liaison between CIGI's research programs and other departments while managing CIGI's legal affairs and advising senior management on a range of legal, operational and policy matters.

A member of CIGI's executive team, Aaron provides guidance and advice on matters of strategic and operational importance, while working closely with partners and other institutions to further CIGI's mission. He also serves as corporate secretary.

Prior to joining CIGI, Aaron practised law for a number of organizations, focusing on international, regulatory and environmental law. He has taught courses at the University of Ottawa's Faculty of Law and Carleton University's Norman Paterson School of International Affairs and was previously a staff editor for the *Columbia Journal of Transnational Law*.

Aaron graduated from the University of Waterloo, placing first in his class as a departmental scholar, with a B.A. (honours) in history and political science. His keen interest in international affairs and political history led him to pursue an M.A. in international affairs at the Norman Paterson School of International Affairs, where he graduated with distinction. He concurrently pursued his LL.B. from the University of Ottawa, where he graduated *cum laude* with first-class honours. Aaron received his LL.M. from Columbia Law School, where he graduated as a Harlan Fiske Stone scholar.

About the Project

The Canada-India Track 1.5 Dialogue on Innovation, Growth and Prosperity is a three-year initiative between the Centre for International Governance Innovation (CIGI) and Gateway House: Indian Council on Global Relations, to explore areas for closer cooperation. Experts, government officials and business leaders will convene annually to promote bilateral economic growth and innovation in today's digital economy.

Canada and India maintain strong bilateral relations built on the foundation of shared values and healthy economic ties. Economic exchanges between Canada and India are on an upward trajectory, but there continue to be unexplored areas for mutually beneficial growth, especially in light of rapid developments in technology that are changing every facet of the economy and society in both countries. To address these challenges, the partnership is helping to develop policy recommendations to promote innovation and navigate shared governance issues that are integral to the continued growth of Canada-India bilateral relations.

The Canada-India Track 1.5 Dialogue on Innovation, Growth and Prosperity strives to build closer ties between Canada and India and nurture the relationship to its full potential. Canada and India can be global leaders in innovation, and the Canada-India Track 1.5 Dialogue seeks opportunities to work jointly on multilateral issues and identify areas where improved cooperation could benefit both countries.

In addition to its focus on innovation, the partnership examines topics such as collaboration on research and higher education, promotion of Canada-India trade and investment, energy cooperation and issues pertaining to global governance.

Through this partnership, Canada and India can be intellectual partners and cooperate in the design of their global governance frameworks.

Executive Summary

While India and Canada are each individually taking steps to enhance their cyber security capacity, increased collaboration between the two countries in the realm of cyber security would increase systemic trust while creating opportunities to promote the nations' strategic and economic interests. There are several similarities in the cyber security threats that both countries face, including being the subjects of attacks with suspected Chinese origins, and mutual concerns over terrorism and election manipulation.

Four suggestions for how India and Canada can further cooperate in cyberspace are presented. First, implementing a revised memorandum of understanding (MOU) between the Indian Ministry of Electronics and Information Technology and the new Canadian Centre for Cyber Security would ensure that the most capable organizations are engaged in essential resource and information sharing.

The second recommendation is to move beyond the general framework of the Mutual Legal Assistance Treaty in place between the two countries to a cyber-specific treaty that contains enhanced evidence sharing and forensic cooperation, mirroring the provisions of the Budapest Convention related to the collection of digital evidence.

The third recommendation involves supporting domestic companies engaged in cyber security technology and services through increased bilateral trade in these sectors. The final recommendation for increased Canada-India cooperation in cyberspace is to facilitate mechanisms through which the pool of cyber talent in India can help fill the cyber talent gap in Canada.

Introduction

There is now a strong, albeit recent, history of regular high-level government interactions in India-Canada bilateral relations. In 2015, the two countries agreed to elevate their relationship to a strategic partnership, and to expand cooperation in a number of areas, including trade and investment, civil nuclear cooperation, and — most importantly here — defence and security (Government of Canada 2015).

This more robust cooperation includes the cyber domain. There is a 2015 MOU between the Indian Ministry of Communications and Information Technology and the Department of Public Safety and Emergency Preparedness Canada (now Public Safety Canada) relating to collaboration in the area of cyber security (ibid.). More recently, Indian Prime Minister Narendra Modi and Canadian Prime Minister Justin Trudeau agreed that India and Canada would "coordinate on cyber security and addressing cyber crimes at bilateral and multilateral forums going forward" (Prime Minister of Canada 2018).

In addition to these general statements and less formal MOU, Canada and India also have in place a mutual legal assistance treaty (MLAT). The MLAT, in force since 1995, includes the basic elements of criminal investigatory cooperation, ranging from search and seizure, to gathering physical or documentary evidence, to assisting in the location and identification of suspect persons.[1]

However, in the intervening period since the MLAT's entry into force and the 2015 MOU, the scale and sophistication of both state-sponsored and criminal cyber attacks directed at the government and private networks in both countries have grown (Centre for Strategic and International Studies 2018). Hardly a day goes by without another front-page story cataloguing the latest cyber attack. The number of companies and governments that have fallen prey are almost too numerous to count: Equifax, JP Morgan Chase, eBay, Aditya Birla, the Union Bank of India, the Bank of Montreal and CIBC offer ready examples. The volume of these events

1 *Treaty between the Government of Canada and the Government of the Republic of India on Mutual Assistance in Criminal Matters,* Canada and India, 24 October 1994, 1995/18 (entered into force 25 October 1995) [*MLAT*].

lays bare the paradox of the digital economy and cyber security. On the one hand, technology has led to convenience, efficiency and wealth creation — and, so, companies connect everything that can be connected. On the other hand, this push to digitize society has meant building inherent vulnerability into the core of the economic model. This is all taking place atop a deeply fragmented and undeveloped system of global rules.

Given the existing national and international context, this paper makes one overarching argument: there is scope for additional cooperation in cyberspace that enhances systemic trust and creates opportunities for India and Canada to advance their respective (and collective) strategic and economic interests. The evidence used to support this argument is twofold. First, Canada and India face a similar threat environment in cyberspace from both adversarial state actors and cyber criminals. Second, each state is taking important steps to enhance its cyber security capacity, creating greater scope to combat existing threats. More specifically, the two states could:

- implement a revised MOU between the new Canadian Centre for Cyber Security (which took over the bulk of core cyber functions of Public Safety and Emergency Preparedness Canada) and the Ministry of Electronics and Information Technology (which assumed the relevant functions from the Ministry of Communications and Information Technology);
- move beyond the general framework of the MLAT toward enhanced evidence sharing and forensic cooperation, mirroring the salient provisions of the Convention on Cybercrime of the Council of Europe (Budapest Convention);[2]
- support domestic industry and scaling companies through increased bilateral trade in both cyber security technology and services; and
- create enhanced opportunity for cyber talent labour mobility between the two countries.

2 *Convention on Cybercrime*, Council of Europe, 23 November 2001, Eur TS 185 arts 29–34 (entered into force 1 July 2004) [*Budapest Convention*].

Canada and India Face a Similar Threat Environment in Cyberspace

In the relatively brief period since the advent of the internet, it has quickly become both ubiquitous and indispensable to the functioning of modern economies. Accordingly, cyberspace has become a new front along which states vie for geostrategic advantage. The digital theatre transcends physical barriers, and states such as Canada and India, which escaped the twentieth century relatively unscathed by violent conflict due to favourable geographic positions, may not prove so fortunate in the digital era.

Both Canada and India have fallen victim to acts of cyber espionage directed against national government agencies. Despite being geographically antipodal to one another, the two countries share a common interest in that they have been affected by numerous acts of cyber espionage suspected to have emanated from China, whether perpetrated by an organization within the Chinese state, a nominally private actor working at Beijing's behest or third-party actors located within the country.

A 2015 investigation by cyber security firm FireEye uncovered an espionage operation infiltrating government and commercial targets in India that had been in operation since at least 2005 (FireEye 2015). Given that organizations with information regarding Chinese-Indian defence relations and contested border regions were deliberately targeted, the report's authors concluded that "[s]uch a sustained, planned development effort, coupled with the group's regional targets and mission, lead us [FireEye] to believe that this activity is state sponsored—most likely by the Chinese government" (ibid., 3).

Similarly, in 2014, Canada's National Research Council was infiltrated by actors believed to have been based in China. This prompted the Canadian government to forego typical diplomatic niceties and take the unprecedented action of publicly denouncing China, with Canada's chief information officer blaming "a highly sophisticated Chinese state-sponsored actor" for the infiltration (Barton 2014).

In 2008, the Office of the Dalai Lama, based in India, requested investigators from the University of Toronto's Citizen Lab to perform a security review of its computer systems. The forensic investigation revealed an extensive system of malware infiltration, subsequently named Ghostnet, which had infected computers in high-value targets, such as government ministries and embassies, with Indian targets being particularly prevalent (Deibert and Rohozinski 2009). In many instances, the perpetrator's Internet Protocol addresses could be traced back to China.

Moreover, the lowered barriers to communication and heightened opportunity for anonymity afforded by digital technologies have allowed terrorist organizations to conduct recruitment and more sophisticated organization in the cyber realm. India has had to contend with religious extremists exploiting social media for recruitment and propaganda (Mirchandani 2017). Likewise, Canada has become increasingly concerned about the possibility of terrorists executing cyber attacks on the country's critical infrastructure (Gendron and Rudner 2012).

Recent events have also raised concern over the potential of malicious actors seeking to disrupt and manipulate the outcomes of democratic elections. Targeted persuasion campaigns and the proliferation of disinformation online may render democratic states asymmetrically vulnerable to digital political disruption relative to autocratic governments. Therefore, Canada and India have a particularly strong interest in developing effective defences against these types of threats as well.

Canada and India Are Both Taking Important Steps to Enhance their Cyber Security Capacity

Canada and India are facing similar threats in cyberspace from adversarial state actors, criminals and terrorists. While these threats have become more pervasive, both nations have acted domestically in recent years to address the looming threat.

In the Canadian context, there are a number of initiatives underway. In June 2018, Canada unveiled its new National Cyber Security Strategy (the "Strategy"), which sets out Canada's vision for security and prosperity in the digital age. This marks an important step for Canada in advancing its national interests in the cyber domain. The Strategy recognizes that "cyber security is the companion to innovation and the protector of prosperity" (Public Safety Canada 2018, 2). It also notes that effective cyber security is now an essential element to a functioning innovation economy.

The Government of Canada's forthcoming efforts in this area are set out in three themes:

- security and resilience — to enhance cyber security capabilities to better protect Canadians and defend critical government and private sector systems;
- cyber innovation — to position Canada as a global leader in the development of cyber security technologies; and
- leadership and collaboration — to have the federal government work to shape the international cyber security environment in a way that will benefit Canada.

As it relates to security and resilience, the Government of Canada will aim to improve cyber security across all federal departments and agencies, enhance law enforcement capacity to respond to cybercrime, and "consider how its advanced cyber capabilities could be applied to defend critical networks in Canada and deter foreign cyber threat actors" (ibid., 17). On cyber innovation, the government will continue to support research and to "help innovative companies scale up to bring cyber security technologies and services to the global marketplace" (ibid., 19). With respect to international leadership, the Canadian government "will work with its international partners to advance Canadian interests" (ibid., 31).

There has also been a legislative push to implement key aspects of the Strategy. Bill C-59 received its second reading in the Senate at the end of September 2018. As the Honourable Senator Marc Gold put it when introducing the bill for debate in the Senate: "The last time we had a major overhaul of our national security framework was in 1984… the basic framework has not been amended in any substantive way since 1984. In 1984 the fax

machine was still a relatively new invention. Personal computers were only beginning to penetrate the market. The Internet? Dial-up at best. The World Wide Web, smartphones? Years away."[3]

Clearly, an update is overdue. While there are a number of important aspects to the bill, including significant changes to the review and oversight of intelligence agencies, there is one aspect that is of particular importance in the context of cyber security.

This proposed legislation expands and redefines the mandate of the Canadian Communications Security Establishment (CSE), adding defensive cyber operations and active cyber operations to the agency's existing duties of foreign intelligence, cyber security and technical operations assistance. In particular, the agency will now have a mandate to engage in active cyber operations "to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security" (CSE 2018a). This is a fairly significant expansion of the agency's role, which marks a considerable shift in the Government of Canada's approach to both offensive and defensive cyber security.

At present, the CSE "does not currently have the authority to take action online outside of Government of Canada networks to deter imminent or ongoing malicious cyber threats against Canada" (ibid.). Under Bill C-59, the CSE would be authorized to proceed with cyber actions to defend not only networks owned and operated by the Government of Canada, but also those owned by the private sector.[4] This is particularly important because the bulk of computer networks and information technology systems are owned by the private sector in Canada.

Additionally, on October 1, 2018, the Canadian Centre for Cyber Security became operational. Housed within the CSE, this organization will consolidate the key cyber security operational units of the Government of Canada into a single organization and will "enable faster, better-coordinated, and more focused Government responses to cyber threats" (CSE 2018b). With funding of CDN$155.2 million over five years and CDN$44.5 million per year thereafter, this new organization will help break down silos and allow for better coordination and collaboration with the private sector and civil society to proactively tackle the major cyber security challenges facing Canada.

India has also taken important steps domestically to be able to take a more robust cyber security posture. The Information Technology Act is the overarching law for regulating electronic, digital and online transactions in India. Based on the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law, initially, the act did not specifically address the issues of cyber security; however, it did introduce and penalize the incidence of hacking computer systems. Prior to this, India did not have a law addressing cyber security threats, although existing criminal laws have been used to prosecute instances of data theft (Joshi 2017).

A major step came with the creation of the Indian Computer Emergency Response Team (CERT-In), which was established in 2004 and continues to play a vital role in India's cyber security. CERT-In actively engages its users with early warning alerts and advisories. Initially, it was aimed at catering to the needs of critical sectors, law enforcement, judiciary and e-governance project owners (Indian Computer Emergency Response Team 2018).

The act was then amended in 2008 to define the role of CERT-In. It has been designated to serve as the national agency performing the following functions in the area of cyber security: collection, analysis and dissemination of information on cyber incidents; forecasts and alerts of cyber security incidents; emergency measures for handling cyber security incidents; coordinating cyber incident response activities; and issuing guidelines, advisories, vulnerability notes and white papers relating to information security practices and procedures, and prevention, response and reporting of cyber incidents as and when they occur (Ministry of Electronics and Information Technology 2018).

The revised act also amended several sections relating to digital data, electronic devices and cybercrimes. For instance, the law now explicitly covers data protection, hacking, possession of stolen computer resources or communication devices, unauthorized access, cyberterrorism, and privacy and confidentiality (Dharmaraj 2018).

3 Bill C-59, *An Act representing national security matters*, 1st Sess, 42nd Parl, 2018, (second reading 25 September 2018).

4 See Cyber Operation Authorizations in the *National Security Act, 2017*, ss 29–30.

In addition, the Ministry of Electronics and Information Technology introduced the first National Cyber Security Policy in 2013. This ministry is at the core of the Indian government's cyber security operations. The policy proposes to build a secure and resilient cyberspace for citizens, businesses and government by facilitating the creation of a secure computing environment; enabling adequate trust and confidence in electronic transactions; and guiding stakeholders' actions for the protection of cyberspace (Government of India 2013). While the policy delineates objectives for the government, some have criticized it for having vague and ambiguous definitions, failing to distinguish between national cyber security and cybercrime, and being unclear about the roles and responsibilities of existing government entities (Diamond 2013).

Notably, the policy created a National Critical Information Infrastructure Protection Centre (NCIIPC), which functions under the National Technical Research Organization, an intelligence-gathering agency controlled directly by the national security adviser in the Prime Minister's Office. The NCIIPC is the nodal agency that "protects and delivers advice that aims to reduce the vulnerabilities of critical information infrastructure, against cyber terrorism, cyber warfare and other threats" (NCIIPC 2018). The agency is also responsible for exchanging cyber incidents and other information relating to attacks and vulnerabilities with the Indian Computer Emergency Response Team and other concerned organizations in the field.

Lastly, the National Cyber Coordination Centre (NCCC) became operational in 2017 and is intended to serve as a multi-stakeholder cyber security and e-surveillance agency under the CERT-In and the Ministry of Electronics and Information Technology. Its mandate is to scan internet traffic and communication metadata coming into the country to detect real-time cyber threats. The system will alert various organizations, internet service providers and the intelligence agency for timely action against the threats (Tech2 2017). Apart from monitoring the internet, the NCCC will also investigate various threats posed by cyber attacks.

The government has also announced its plans to create a new Cyber Defense Agency. This new unit will focus on critical infrastructure relating to government and defence networks and will work in close coordination with the national cyber security adviser. Until now, India has practised more of a defensive strategy, and some security experts suggest that there is an urgent need for the country to move toward building an offensive cyber security posture (Goswami 2017).

Canada-India Cooperation in Cyberspace

Cyberspace presents both threats and opportunities — at the same time — and the collective challenge is to advance a cooperative position policy that can best maximize the opportunities while mitigating the threats in a constantly changing global environment. As set out above, there are four areas in which increased cooperation could enhance both Canadian and Indian cyber posture.

Implement a revised MOU between the new Canadian Centre for Cyber Security and the Ministry of Electronics and Information Technology

Previously, the Canadian Cyber Incident Response Centre played the role of Canada's national Computer Security Incident Response Team (CSIRT). Typically, a CSIRT is an organizational entity that coordinates and supports incident response reported by end users or observed through proactive network and system monitoring (United States Computer Emergency Readiness Team 2007). This organization was housed within Public Safety Canada, and therefore an MOU with this ministry made sense. However, with the consolidation of the key cyber security operational units within the Canadian Centre for Cyber Security, and their more significant funding package and increased capability, a revised MOU between the Canadian Centre for Cyber Security and the Ministry of Electronics and Information Technology would be an important step. This could facilitate the sharing of best practices, joint training and enhanced information sharing about threats, which could allow the two countries to make good on the promise of Prime Ministers Modi and Trudeau to enhance cooperation in cyberspace.

Move beyond the general framework of the MLAT toward enhanced evidence sharing and forensic cooperation, mirroring the salient provisions of the Budapest Convention

While the MLAT has a broad scope related to mutual assistance on criminal matters, a new treaty could particularize cybercrime cooperation and underscore the unique and time-sensitive circumstances surrounding the collection of digital evidence. It is telling that earlier this year, it was reported that the Indian Ministry of Home Affairs was "[m]aking a strong pitch to sign the Budapest Convention on cyber crime" (Tripathi 2018). However, it was also reported that Indian accession to the Budapest Convention was opposed by the Intelligence Bureau, which argued that "sharing data with foreign law enforcement agencies infringes on national sovereignty and may jeopardise the rights of individuals" (ibid.). Given the resistance of the Indian intelligence service, an agreement with the Government of Canada with more detailed provisions related to mutual assistance in cybercrime matters, including pertinent provisions from the Budapest Convention, could alleviate the broader concern about generalized sharing with foreign law enforcement and allow for targeted cooperation on cybercrime between two states that already have an MLAT in place.

This agreement would merely create certainty between Canada and India with respect to assistance on cybercrime matters and ensure that the two nations are cooperating with one another to address these crimes in a timely manner, in particular when a matter of minutes can mean the difference between preserving digital evidence or losing it forever. Articles 29 through 34 of the Budapest Convention provide detailed measures on how states shall offer mutual assistance to one another in cybercrime cases, including by preserving and providing access to stored computer data, disclosing preserved traffic data and assisting in the real-time collection of traffic data, among other measures. Given the volume of cybercrime facing both states, specific obligations that address the unique aspects of these types of criminal activity would be beneficial.

Support domestic industry and scaling companies through increased bilateral trade in both cyber security technology and services

On the Canadian side, the Strategy acknowledges that "Government has a role to play to support advanced research and to help innovative companies scale up to bring cyber security technologies and services to the global marketplace" (Public Safety Canada 2018, 19). This is — at the very least — an implicit acknowledgement that there is an increased opportunity for trade and trade in services in relation to cyber security technologies. Canada has a number of innovative and growing cyber security companies — including the Herjavec Group, SecureKey, eSentire and Magnet Forensics — and India has comparable companies. Through the offices of their respective trade ministries, Canada and India should explore initiatives specifically related to cyber security to ensure that both Indian and Canadian companies can bring their products to a global market, and to facilitate consumer acquisition of the best available technologies.

In November 2017, the Government of Canada organized a technology- and innovation-focused trade mission to India, led by the Honourable François-Philippe Champagne, minister of international trade; the Honourable Navdeep Bains, minister of innovation, science and economic development; and the Honourable Marc Garneau, minister of transport. The group brought Canadian businesses to India to interact with senior government officials and business leaders there. The mission had a number of focus sectors, including advanced manufacturing, cleantech, energy, information and communications technologies (ICT), life sciences and transportation. While these are important sectors, and there was a focus on ICT more generally, a trade mission at this level dealing expressly with cyber security would be a significant move toward supporting domestic industries in both countries.

Create enhanced opportunity for cyber talent labour mobility between the two countries

A recent report by Deloitte (2018) found "demand for cyber talent in Canada is increasing by 7 percent annually, with organizations needing to fill some 8,000 cybersecurity roles between 2016 and 2021. Business, government, and academia are all taking steps to close the cyber talent gap; however, their existing efforts and traditional

approaches may not be sufficient to solve the problem." If domestic efforts and traditional approaches are insufficient, inevitably Canada will need to turn to the international labour market. On this front, India is well prepared. A recent study by the Capgemini Digital Transformation Institute (2018) found that India and the United States have the largest cyber security talent pool out of the nine countries surveyed — France, Germany, India, Italy, the Netherlands, Spain, Sweden, the United Kingdom and the United States (Capgemini Digital Transformation Institute 2018, 8). Given the immediacy of the cyber talent gap in Canada, and the uncertain timelines regarding any bilateral trade deal that could address labour mobility, Canada should consider additional mechanisms that could attract Indian cyber talent for both short and longer durations.

Works Cited

Barton, Rosemary. 2014. "Chinese cyberattack hits Canada's National Research Council." *CBC News*, July 29. www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241.

Capgemini Digital Transformation Institute. 2018. *Cybersecurity Talent: The Big Gap in Cyber Protection*. www.capgemini.com/wp-content/uploads/2018/02/the-cybersecurity-talent-gap-v8_web.pdf.

Center for Strategic & International Studies. 2018. "Significant Cyber Incidents Since 2006." https://csis-prod.s3.amazonaws.com/s3fs-public/180910_Significant_Cyber_Events_List.pdf?IjP3fnWfsOPcRjUBLQ2XXM9lqqtiCHiE.

CSE. 2018a. "Foreign Cyber Operations." www.cse-cst.gc.ca/en/cse-act-loi-cst/cyberop.

———. 2018b. "Canadian Centre for Cyber Security." www.cse-cst.gc.ca/en/backgrounder-fiche-information.

Deibert, Ron and Rafal Rohozinski. 2009. "Tracking *GhostNet*: Investigating a Cyber Espionage Network." *Information Warfare Monitor*, March 29. www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

Deloitte. 2018. *The changing faces of cybersecurity: Closing the cyber risk gap.* www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF.

Dharmaraj, Samaya. 2018. "The current state of cyber security in India." *OpenGov*, August 1. www.opengovasia.com/the-current-state-of-cyber-security-in-india/.

Diamond, Jonathan. 2013. "India's National Cyber Security Policy in Review." The Centre for Internet & Society. https://cis-india.org/internet-governance/blog/indias-national-cyber-security-policy-in-review.

FireEye. 2015. *APT30 and the Mechanics of a Long-running Cyber Espionage Operation*. April. www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf.

Gendron, Angela & Martin Rudner. 2012. *Assessing Cyber Threats to Canadian Infrastructure*. CSIS Report, March. www.canada.ca/content/dam/csis-scrs/documents/publications/CyberTrheats_AO_Booklet_ENG.pdf.

Goswami, Suparna. 2017. "India to Create Cyber Defense Agency." Bank Info Security, November 13. www.bankinfosecurity.asia/india-to-create-cyber-defense-agency-a-10451.

Government of Canada. 2015. "India-Canada Joint Statement." Government of Canada press release, April 15. www.canada.ca/en/news/archive/2015/04/india-canada-joint-statement.html.

Government of India. 2013. *National Cyber Security Policy 2013*. www.india.gov.in/national-cyber-security-policy-2013.

Indian Computer Emergency Response Team. 2018. "Welcome to CERT-In." Ministry of Electronics and Information Technology. https://cert-in.org.in/.

Joshi, Divij. 2017. *A comparison of legal and regulatory approaches to cyber security in India and the United Kingdom.* The Centre for Internet & Society. https://cis-india.org/internet-governance/files/india-uk-legal-regulatory-approaches.pdf.

Ministry of Electronics & Information Technology. 2018. “ICERT.” http://meity.gov.in/content/icert.

Mirchandani, Maya. 2017. *Countering Violent Extremism: Lessons from India*. Observer Research Foundation, September. www.orfonline.org/research/countering-violent-extremism-lessons-india/.

NCIIPC. 2018. “NCIIPC.” www.nciipc.gov.in/.

Prime Minister of Canada. 2018. “India-Canada Joint Statement: Partnership for Security and Growth.” Prime Minister of Canada press release, February 23. https://pm.gc.ca/eng/news/2018/02/23/india-canada-joint-statement-partnership-security-and-growth.

Public Safety Canada. 2018. *National Cyber Security Strategy: Canada’s Vision for Security and Prosperity in the Digital Age*. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.

Tech2. 2017. “First phase of national cyber coordination centre made operational, says PP Chaudhary.” *First Post*, August 10. www.firstpost.com/tech/news-analysis/first-phase-of-national-cyber-coordination-centre-made-operational-says-pp-chaudhary-3914699.html.

Tripathi, Rahul. 2018. “Home Ministry pitches for Budapest Convention on cyber security.” *The Indian Express*, January 18. https://indianexpress.com/article/india/home-ministry-pitches-for-budapest-convention-on-cyber-security-rajnath-singh-5029314/.

United States Computer Emergency Readiness Team. 2007. “Defining Computer Security Incident Response Teams.” www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams.

About CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

À propos du CIGI

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan doté d'un point de vue objectif et unique de portée mondiale. Nos recherches, nos avis et nos interventions publiques ont des effets réels sur le monde d'aujourd'hui car ils apportent de la clarté et une réflexion novatrice pour l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos programmes de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques mondiales, et le droit international, et nous les exécutons avec la collaboration de nombreux partenaires stratégiques et le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

About Gateway House

Gateway House: Indian Council on Global Relations is a foreign policy think tank in Mumbai, India, established to engage India's leading corporations and individuals in debate and scholarship on India's foreign policy and the nation's role in global affairs. Gateway House is independent, non-partisan and membership-based.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline