Centre for International Governance Innovation

GATEWAY HOUSE
INDIAN COUNCIL ON GLOBAL RELATIONS
भारतीय वैश्विक संबंध परिषद्

Canada-India Track 1.5 Dialogue Paper No. 2

Partnering for Prosperity:

India-Canada Collaboration to Curb Digital Black Markets

Sameer Patil

Canada-India Track 1.5 Dialogue Paper No. 2

Partnering for Prosperity: India-Canada Collaboration to Curb Digital Black Markets

Sameer Patil

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

Sameer Patil is a fellow, National Security Studies and director of the Centre for International Security at Gateway House. His research focuses on cyber security, maritime security and counter-terrorism. Sameer previously served in the National Security Council Secretariat within the Indian Prime Minister's Office, where he focused on counter-terrorism and regional security. He is also a dissertation advisor at the Indian Naval War College.

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.

Acronyms and Abbreviations

ATT	Arms Trade Treaty
Europol	European Union Agency for Law Enforcement Cooperation
FBI	Federal Bureau of Investigation
G20	Group of Twenty
I2P	Invisible Internet Project
I4C	Indian Cyber Crime Coordination Centre
Interpol	International Criminal Police Organization
IP	internet protocol
IRC	internet relay chat
ISP	internet service provider
NCCC	National Cyber Coordination Centre
OECD	Organisation for Economic Co-operation and Development
P2P	peer-to-peer
PGP	pretty good privacy
PIPEDA	Personal Information Protection and Electronic Documents Act
RCMP	Royal Canadian Mounted Police
TOR	The Onion Router
VPN	virtual private network

Executive Summary

When Canadian Prime Minister Justin Trudeau visited India in February 2018, the two countries agreed to extend their cooperation on security issues to cover cyberspace, with a specific focus on cybercrime. The two countries face multiple common cyber security challenges. Digital black markets, where contraband and illegal services are bought and sold, pose an emerging threat. Using advanced security features to remain anonymous, hackers, organized criminal networks and terrorist groups use these sites, also known as the "dark net marketplaces," as force multiplier for their illicit activities. In the case of India and Canada, these markets have abetted drug smuggling, facilitated cybercrimes and contributed to terrorist activities. Despite frequent security crackdowns, these marketplaces have proved to be resilient.

India and Canada have implemented multiple steps domestically to address the growing threats. Canada has participated in multiple crackdowns against the digital black markets. India, however, lacks a comprehensive understanding of this illicit activity. Both countries have an opportunity to deepen their security cooperation by collaborating to tackle these markets. They can work bilaterally to track the encryption technologies, encourage informal collaboration between their respective law enforcement agencies, work with private stakeholders (such as cryptocurrency exchanges) and move to discredit these marketplaces. At the multilateral level, the two countries can contribute to international security and cyberspace stability by building the capacity to fight cybercrime, while raising them as issues at the Group of Twenty (G20) and the Conference on Disarmament and initiating a discussion on ways to identify the sources of cyber attacks. In shaping such collaboration, both countries will need to demonstrate out-of-the-box thinking in the manner already shown by the digital black markets.

Introduction

In recent years, India and Canada have seen unprecedented growth in ties across all sectors. Their bilateral security cooperation, however, has not kept pace with emerging cyber threats. Ottawa and New Delhi are well-positioned to advance their security cooperation to focus on the growing problem. Annual security dialogues and a counter-terrorism working group already provide useful platforms for the countries' respective national security establishments to share assessments of a range of security threats. The consensus to step up cyber cooperation with a focus on fighting cybercrimes in bilateral and multilateral forums, achieved during Prime Minister Justin Trudeau's India visit in early 2018, provides a foundation for even closer collaboration (India 2018b).

Although they are heterogeneous democracies and their economies have achieved different levels of digitalization, India and Canada face multiple common cyber-security challenges, including:

- → cybercrime and data breaches;
- → critical infrastructure protection;
- → cyber-enabled espionage;
- → securing election systems from sabotage; and
- → misuse of cyberspace by terrorists and extremists.

For India and Canada, an emerging concern on this cyber-security canvas are digital black markets or "dark net[1] marketplaces," which have emerged from the shadows to become the mainstay of online illicit activity.

1 The dark net consists of websites that are not indexed by standard search engines and can be reached only by The Onion Router (TOR) encrypted browser that imparts anonymity to users.

Digital Black Markets: The Internet's Murky Alleys

Clandestine online markets have existed since the advent of the internet and have evolved from simple chat rooms and forums to fully fledged e-commerce websites, deploying state-of-the-art technology and advanced security features. The arrival of TOR technology in the early 2000s added a crucial new dimension to such illegal activity (Dingledine, Mathewson and Syverson 2004).

Originally developed by the US Naval Research Laboratory for confidential communications, TOR was released to the public in 2003 as free downloadable software and has since become the core technology for dark net marketplaces (ibid.). TOR enables individual users to hide their internet protocol (IP) addresses (numerical identifiers assigned to computers or devices that log onto the internet).[2] Anonymous networks are largely resistant to both eavesdropping and traffic analysis (Syverson 2003). The technology itself is dual-use. It has been useful for human rights and political activists, investigative journalists and whistle-blowers, allowing them to protect their identity and bypass security agencies' surveillance systems. However, criminal elements have misused TOR technology, combining it with other widely available legitimate technologies and tools, such as Virtual Private Network (VPN),[3] and encrypted communication tools, such as TorChat, Protonmail and Lelantos, to create thriving digital black markets. Table 1 gives an overview of the commonly used technologies and tools used to maintain anonymity.

These clandestine, virtual marketplaces sell contraband, stolen products, banned commodities (including narcotics and controlled substances, child pornography, malicious software, personal and financial data and firearms) and illegal services (including trade in stolen credit cards and other personal financial information, money-laundering, counterfeiting and contract killing). Some of these marketplaces sell legal goods that were procured illegally, such as prescription drugs and consumer electronics. A high-profile example is the Silk Road marketplace, which grabbed the popular imagination when it launched in 2011 offering illegal goods. The US Federal Bureau of Investigation (FBI) shut it down in 2013, but not before it had generated revenues worth US$1.2 billion (FBI 2013).

Payments in these marketplaces are made in cryptocurrencies, such as Bitcoin, Monero and Ethereum, which have no central issuing authority and therefore enable anonymous transactions.

By its very nature, the dark net complicates the task of collecting data on the scope and extent of digital black markets. Only a handful of policy studies have been devoted to the subject.[4] The findings and arguments set out in this paper are based on a combination of desk research; consultations with cyber security analysts, officials of law enforcement and security agencies; and a perusal of digital black market sites to understand their modus operandi.

A review of the operations of these sites suggests that their average lifespan is one year to one-and-a-half years — with some lasting up to three years before they are removed (see Table 2 in the Appendix). They also have an ethical compass, if a relative one. Mainstream and popular marketplaces, such as Silk Road 3.0 and Wallstreet Market, forbid the buying and selling of weapons and poisons, anything related to terrorism, illegal pornography (such as child pornography), snuff movies, contract killing and human trafficking, among others. These marketplaces have listed this principle quite prominently on their websites. Regardless, non-mainstream fringe marketplaces, such as

2 However, TOR is not the only network encryption technology. There are others, such as Invisible Internet Project (I2P)/Garlic Router and Freenet, but they are not as widely used as TOR.

3 VPN anonymizes web traffic and is widely used by legitimate corporations.

4 Some of these studies are: Chertoff, Michael. 2017. "A public policy perspective of the Dark Web." *Journal of Cyber Policy* 2 (1): 26–38; Holt, Thomas J. and Eric Lampke. 2010. "Exploring stolen data markets online: products and market forces." *Criminal Justice Studies: A Critical Journal of Crime, Law and Society* 23 (1): 33–50; Ablon, Lillian, Martin C. Libicki and Andrea A. Golay. 2014. "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar." *RAND Corporation*. www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf; Jeffray, Calum and Tobias Feakin. 2015. "Underground web: The cybercrime challenge. *"The Australian Strategic Policy Institute Limited* March. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/SR77_Underground_web_cybercrime.pdf?awHWbEd8jXq47M7awzQ1AQCjDePZdhsY; and Malik, Nikita. 2018. "Terror in the Dark: How Terrorists use Encryption, the Darknet, and Cryptocurrencies." *The Henry Jackson Society*. https://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf.

Table 1: Tools and Technology Stock Associated with Digital Black Markets

Technology	Tools	Details
TOR-specific		
TOR	TOR Client/Browser	TOR Browser anonymizes web traffic using the TOR network. It prevents internet service providers (ISPs) and mass-surveillance programs from conducting internet traffic analysis. TOR consists of a three-layer proxy, similar to the layers of an onion. The browser connects at random to one of the publicly listed entry nodes, bounces that traffic through a randomly selected middle relay and exits the traffic through the third and final node.
	TOR network	
Search engines/ link directories	Ahima, Not Evil, Hidden Wiki	Search engines trawl through the TOR network to help find the websites. The link directories have a repository of website addresses, readily accessible to any user on the TOR network.
Communication tools	Messengers: TorChat, BitMessage Chat	TorChat is a decentralized, encrypted instant messenger that uses the Tor network and encryption based on public-key cryptography or asymmetric cryptography. It provides secure text messaging and file transfers. BitMessage Chat is used for peer-to-peer (P2P) encrypted messaging. It encrypts incoming and outgoing messages, using public-key cryptography, so that only the receiver of the message is capable of decrypting it.
	Forums: Dread Forum, Darknet Avengers Forum	Discussion forums on the TOR network dealing with digital black marketplaces and cryptocurrencies, among others. These forums use encryption that is based on public-key cryptography or asymmetric cryptography.
	Email: TorGuard Email, CounterMail, ProtonMail	Encrypted email services that use the TOR network and encryption, such as Pretty Good Privacy (PGP). The PGP uses pairs of keys — public keys that may be disseminated widely, and private keys that are known only to the owner — to encrypt and decrypt data.
Generic/Non-TOR specific		
VPN	IP Vanish, Nord VPN, StrongVPN, TorGuard, proxy.sh	VPN allows internet users to securely access a private network and share data remotely through public networks. VPN services use a combination of dedicated connections and encryption protocols to generate virtual P2P connections. The ISPs are unable to track internet traffic through a VPN. They also allow individual users to spoof their IP address, enabling them to bypass content filters.
Mainstream Encrypted Chats	Telegram, Facebook Messenger, Signal, WhatsApp	These messaging applications use end-to-end encryption, preventing the mass-surveillance programs from monitoring the content of the messages. Telegram uses its own encryption application programming interface, MTProto.
Cryptocurrency	Bitcoin, Monero, Ethereum	Use cryptography for secure transactions with decentralized control. It eliminates the need for a trusted middle authority, such as a bank. These are based on blockchain technology, where each block contains a cryptographic hash of the previous block, a timestamp and transaction data.
Email	GuerillaMail	A free disposable email address service that scrambles addresses.

Source: Gateway House Research.
Note: This data is accurate as of October 1, 2018.

Berlusconi, and many stand-alone forums on the dark net, do offer some of these goods and services.

Innovation is a key for the thriving business of cybercrime. For instance, Silkkitie/Valhalla (now closed) and Wallstreet Market offer rewards to users who avail of advanced security features to maintain the anonymity of their transactions, such as multi-signature transactions[5] and logging-in with the PGP encryption key.[6] Vendors employ various techniques to keep law enforcement agencies from seizing their shipments of contraband. The complexity of shipping the contraband varies depending on the product (Patil 2018a).

Illicit online marketplaces make every effort to ensure the quality of contraband and to address customers' grievances over quality, shipment and payment. In yet another effort to prove reliability, many marketplaces provide escrow services, where sellers receive money only after delivery of goods or services. Of course, as with any e-commerce activity, some fringe marketplace administrators dupe users by committing exit scams, failing to deliver goods and making away with escrow funds; in 2015, a site known as Evolution embezzled approximately US$12 million in bitcoins from its users (Woolf 2015).

With their offerings of contraband, malicious software and illegal services, these markets have lured organized criminal networks, terrorist groups and other non-state actors involved in cybercrime and terrorist attacks. For instance, in 2015, hackers, allegedly backed by the North Korean government, used malware available on dark net sites (Alpeyev and Huang 2014) to hack into Sony Pictures' servers, (Sony Pictures 2014) reportedly costing the company US$100 million, plus much more in reputational damage (Richwine 2014).

For India and Canada, the extent of the digital black markets' challenge is varied, but its implications are common. These can be understood through three dimensions:

→ Flourishing online drug trade: Digital black market sites offer buyers convenient and anonymous access to narcotic substances. This is particularly true in Canada, where authorities have disrupted multiple instances of the online drug trade. In early 2018, the Royal Canadian Mounted Police (RCMP) targeted online vendor "Mr. Hotsauce," who sold fentanyl, heroin, cocaine, ketamine and other narcotics to customers in Canada and around the world (RCMP 2018). For India, such online drug trade activity is currently limited, but it is only a matter of time before it increases. Between 2015 and 2017, India's Narcotics Control Bureau, a government agency responsible for drug-law enforcement, interdicted four cases involving purchases of narcotics on dark net marketplaces (India 2015; 2016; 2018a). At present, a handful of India-based vendors offer Indian opium, ketamine, hashish and prescription pills on the Dream Market and Tochka marketplaces to customers in India and abroad. Some vendors also list Xanax bars, a synthetic drug linked to drug abuse among teens, as sourced from India. Listings such as these generated an estimated US$14 million in monthly sales in 2016 (Kruithof et al. 2016).

This online drug trade complements well-entrenched offline smuggling syndicates that operate in India, in particular in the border regions (Patil 2018b). These syndicates have used India's proximity to the two global drug-trade hubs — the "golden triangle" (Thailand, Laos and Myanmar) in the east and the "golden crescent" (Iran, Afghanistan and Pakistan) toward the west, to create active illegal corridors. These are used not just for drug smuggling, but also for trafficking counterfeit Indian currency and small arms, facilitating movement of militants across borders and human trafficking, especially of women and children for commercial sexual exploitation.

→ Abetment to cybercrimes: Cybercrime is a more significant issue than the drug trade for India and Canada. Black hat hackers — hackers with mala fide intentions and involved with organized criminal syndicates — have actively explored the black markets for computer hacking tools, software vulnerability data, social engineering attack tools and malicious software (Algarni and Malaiya 2014). This has contributed to the burgeoning number of cybercrimes globally. In 2014, the cyber security firm Norton estimated that cybercrimes accounted for 0.21 percent (Center for Strategic and International Studies and McAfee

5 Multi-signature transactions are transactions that require multiple digital signatures for executing a transaction such as payment or fund transfer.

6 PGP encryption key is a tool to secure online communication through a public key (to encrypt) and a private key (to decrypt).

2014, 21) of India's GDP — approximately US$4.2 billion.[7] Canada also has seen repeated cyber intrusions in recent years. Between 2013 and 2015, the Canadian Communications Security Establishment detected, on average, 2,500 state-sponsored cyber activities against its networks annually (Canada 2017a). At present, there is no specific evidence connecting digital black markets to cybercrimes in both countries, but India's ambitious, ongoing transition to a digital economy and Canada's reliance on digital technology portends widening cyber vulnerabilities.

→ Catalyst for terrorist activities: Use of cyberspace by terrorist groups is a major concern for India and Canada. Daesh (also known as the Islamic State) and Al-Qaeda have used virtual space for propaganda and recruitment. Digital black markets offer these groups anonymity and provide a platform for fundraising, propaganda and easy access to weapons (Weimann 2016). Investigations show that weapons for two terrorist attacks linked to Daesh — the November 2015 Paris attack (DW 2015) and the July 2016 Munich shooting (Bender and Alessi 2016), which together killed 140 people — were purchased from black market sites. Canada has strict regulations on owning handguns, but on sites such as Berlusconi, some Canadian vendors offer weapons and 3D-printing blueprints for parts of handguns, such as the Remington pistol. These can be combined with other widely available components, such as pistol grips and trigger assemblies, to make deadly firearms. In calls for terrorist attacks, Daesh's virtual propaganda on social media and dark net platforms regularly targets India and Canada — apparently with success: since 2014, Canada has seen repeated instances of Daesh-inspired terrorist attacks, and Daesh has successfully recruited Indian youth to fight in Iraq and Syria. Recently, the terrorist group, Ansar Ghazwatul Hind — the al-Qaeda affiliate operating in the Indian state of Jammu and Kashmir — advised its cadres to use VPN and TOR to avoid interception by the security forces (Al-Hur Media 2018).

Additionally, the anonymity provided by TOR technology makes it difficult to ascertain perpetrators of cyber attacks and acts as incentive for hackers to launch more attacks.

Since digital black markets contribute to the illicit drug trade, facilitate cybercrimes and enable terrorist activities, they pose a national security threat to India and Canada. Therefore, carving out a joint India-Canada strategy to curb these marketplaces is critical.

Cracking Down on Digital Black Markets and Securing Cyberspace

Better intelligence and technical surveillance have helped security agencies worldwide intensify their crackdown on physical (or "street") black markets (see Table 3 in the Appendix). Between 2012 and 2018, major operations have shut down online drug traffickers and leading marketplaces, such as Silk Road and its subsequent iterations, AlphaBay and Hansa. Canadian authorities have been involved in these crackdowns — most prominently, Operation Bayonet in 2017, in which the RCMP seized AlphaBay's servers in Montreal, Quebec (Bellemare 2017). So far, these multi-nation operations have been restricted to North American and European security agencies — justifiably so, given black market sites' focus on these regions' vendors, customers and digital connectivity.

Despite these frequent takedowns by law enforcement agencies, illegal marketplaces have demonstrated resilience: sellers and users have moved to other marketplaces or created new ones to resume their activities, and newer marketplaces have learned from the experience and mistakes of their predecessors, becoming tougher and more complex to track and crack. A January 2018 study revealed that more than one-half of customers who had used closed websites to purchase narcotics did not consider themselves to have been affected by the crackdowns, just 15 percent of the clients were deterred (UN Office on Drugs and Crime 2018, 7) and only nine percent completely stopped using dark net sites.

7 Calculated on the basis of World Bank and Organisation for Economic Co-operation and Development (OECD) national accounts data for India, see World Bank (n.d.) https://data.worldbank.org/country/india.

Domestically, India and Canada have implemented multiple steps to address these growing cyber threats.

In 2013, India launched the National Cyber Security Policy (see Table 4 in the Appendix) to create a safer cyberspace. Additionally, it has set up a National Cyber Coordination Centre (NCCC) to scan cyberspace for threats and an Indian Cyber Crime Coordination Centre (I4C) to monitor cybercrimes. After intercepting the first few online shipments of narcotics in the country, the Narcotics Control Bureau has worked with other Indian security agencies to crack down on the online drug smuggling business. Yet, Indian authorities lack a comprehensive understanding of digital black-market activity and the necessary technological and forensic skills to deal with it.

In 2018, Canada unveiled a National Cyber Security Strategy, which seeks to protect Canadian citizens and computer networks from emerging cyber threats (see Table 5 in the Appendix). Under this strategy, the cyber-security functions of a variety of agencies will be consolidated under one new agency, the Canadian Centre for Cyber Security. There have been additional national measures dealing with different aspects of digital black-market activity. Since 2017, two major national crackdowns have targeted the online narcotics trade (see Table 3 in the Appendix). In a contentious move, Ottawa legalized recreational marijuana on October 17, 2018, becoming only the second country in the world to do so after Uruguay (Canada 2018a). Its goal is to tackle illicit sales and weaken black markets, both physical and digital (Hagar 2018). In 2004, Canada announced a National Strategy for the Protection of Children from Sexual Exploitation on the Internet (Canada 2018b) — a comprehensive all-agency initiative prohibiting all forms of child pornography and other illicit sexual activities, including prostitution. Under the strategy, Canadian authorities have actively removed pornographic material from the internet.

Aligned with their domestic efforts, India and Canada are well-positioned to collaborate to tackle the menace of digital black markets. Such collaboration will give the two countries an opportunity to expand current security cooperation through the annual Security Dialogue and the Joint Working Group on Counter Terrorism (India 2017).

Tackling Black Markets through India-Canada Digital Security Cooperation

Bilateral digital security collaboration between India and Canada must recognize that economic incentives propelling black-market activity will always exist, and that digital black markets are resilient and innovative, as evident from the aftermath of global crackdowns. Therefore, an ambitious partnership must aim to discredit and disrupt black-market activity, not merely shut down current operations.

Bilateral Collaboration

Canada and India should:

- *Monitor key technologies enabling dark net marketplaces:* India and Canada need to track technological advancements regularly. This should include not just TOR technology and encryption and cryptographic tools but other related technologies, such as 3D printing. Here, India can learn much from Canada's domestic crackdowns, disruption of online drug sales and participation in multi-nation crackdowns against black markets.
- *Encourage informal collaboration between respective law enforcement agencies:* Successful global crackdowns have demonstrated the importance of international partnerships that transcend national boundaries. While there are formal mechanisms for bilateral collaboration, such as the Mutual Legal Assistance Treaty (Canada 1994), data sharing and real-time information exchange remain persistent challenges for cybercrime investigations. Therefore, both countries must encourage informal cooperation between their respective law enforcement agencies to harvest IP addresses, use TOR browsers and jointly patrol digital black marketplaces so authorities know more about vendors, buyers, goods-in-demand and other relevant issues. American and European security agencies have jointly policed the marketplaces before in successful crackdowns, such as Operation

Onymous (The European Union Agency for Law Enforcement Cooperation [Europol] 2019) and Operation Bayonet (Europol 2017).

- *Consider establishing bug bounty programs*: Governments and technology companies regularly utilize such programs that reward individuals who discover and report software vulnerabilities for which no patch is currently available. A similar program can be established for unlocking encryption technologies used for anonymous internet traffic. Such programs require sustained financial support from both governments to succeed. This suggests that the creation of a joint fund may be required.

- *Identify non-government stakeholders to tackle black market-related activities:* Security agencies cannot tackle the challenge of digital black markets alone. A multi-stakeholder approach is needed. Identifying legitimate actors — such as cryptocurrency exchanges and VPN providers — is critical. This was demonstrated when American security agencies worked with bitcoin exchange companies during the Silk Road 2.0 investigation to gather details about the site administrator Blake Benthall (FBI 2014). India, with its large force of software engineers, and Canada, with its strong base in cyber forensics, must follow such an approach to track illicit transactions.

- *Work together to discredit digital black marketplaces*: Since mainstream digital black marketplaces thrive by being reliable and dependable for their customers, security agencies of both countries should collaborate to undermine their credibility, with the aim not just of putting them out of business but of tarnishing the reputation of potential successors. Some possible tactics include flooding these marketplaces with spam, circulating unsolicited warnings about government crackdowns, establishing fake seller accounts to confuse buyers (also known as "Sybil attacks" [Douceur 2002]) and lemonising — which involves duping buyers through exit scams or exposing anonymous transactions (Akerlof 1970). Since these tactics are risky, they will require oversight to avoid abuse and entrapment.

- *Keep pressure on offline black-market activity:* Online black markets cannot thrive without well-entrenched smuggling networks that deliver the actual goods. So, even as the focus is on disrupting online activity, India and Canada must enrich their understanding of the actual supply chains and modes of delivery of the contraband sold online.

Collaboration at a Global Level

In addition to addressing bilateral concerns, India and Canada could contribute to broader international attempts to crack down on cybercrimes. Specifically, they should:

- *Focus on building capacity throughout the Indo-Pacific region to thwart cybercrimes*: The Indo-Pacific region is facing several non-conventional threats from organized smuggling syndicates, terrorist groups and money launderers. These groups are inter-linked, and they capitalize on the weak institutional capacities of the littoral states. Digital black markets are critical enablers of these criminal enterprises. In the last few years, India has taken the lead in diplomacy on cyber issues with many countries in the region, including Bangladesh, Vietnam, South Korea and Japan (Patil 2018c). Canada and India can expand on this by focusing on technical cooperation by sharing best practices with and building the capacities of national cyber security agencies throughout the region. Another platform that must be explored for joint collaboration is the International Criminal Police Organization (Interpol) Global Complex for Innovation, based in Singapore, which focuses on training, digital crime investigation and providing operational support for solving cybercrimes (Interpol 2018).

- *Work together on agreements to tackle specific dimensions of online black-market activity*: Since black-market activity is as varied as narcotics smuggling, illicit arms trade and cybercrime, India and Canada can demonstrate their commitment to international security by shaping new agreements dealing with specific dimensions of the problem and by amending existing agreements to cover emerging issues. Modifying the Arms Trade Treaty (ATT), which seeks to reduce the illicit weapons trade, could be one goal. At present, India perceives the ATT as discriminatory and has refused to sign (India 2013), while Canada is preparing to sign (Canada 2017b). India should review its stance toward the ATT and work with Canada to include the role of the online black market in the ATT, especially in illicit small

arms sales. The effort should include a focus on non-state actors, in particular in small arms.

- *Expand the scope of the G20 Digital Economy Task Force:* In 2016, during the Chinese presidency, the G20 established a Digital Economy Task Force. The task force's focus has evolved over the years as different countries have assumed the G20 presidency, but still cyber security is not yet one of its core issues (G20 2018). Given the linkages between cybercrime and online black-market activity, India and Canada must press for expanding the task force's scope to include cyber security and digital black-market activity.
- *Initiate discussion on cyber attack attribution:* Encryption provided by TOR technology has complicated the task of identifying perpetrators of cyber attacks. Overcoming obstacles to clear attribution, whether to state or non-state actors, must be an important component of any strategy to deter cybercrime (Basu 2018). Unlike Canada,[8] India is yet to attribute a cyber attack to any state or non-state actor publicly.[9] To bring more transparency into the global cyber arena, India and Canada can initiate a discussion about this concern at the Conference on Disarmament, or it can seek to revive the UN Group of Governmental Experts process.

Conclusion

The ever-expanding business of black market sites suggests that the challenge of digital black-market activity must be tackled in the same innovative manner that these sites have followed to establish their operations. Since shutting these markets down completely and permanently is probably impossible, innovative and creative thinking is required to discredit and disrupt their operations. India, with its emerging economy and sophisticated technology industry, and Canada, with its enormous economic might and experience in dealing with such threats, are well-positioned to expand their existing security collaboration to tackle these black markets, thereby increasing their own safety and contributing to international security and cyberspace stability.

Acknowledgements

The author wishes to thank Gateway House researcher Sagnik Chakraborty for his research assistance in preparing this paper.

8 In 2014, Canada's Chief Information Officer blamed a "highly sophisticated Chinese state-sponsored actor" for breaching the National Research Council's computer systems. See Barton (2014).

9 Yet, there is enough anecdotal and technical evidence from private cyber security firms to indicate the involvement of China and Pakistan in hostile operations against India.

Appendix

Table 2: Major Digital Black Market Sites

Market Site	Years of Operation	Status	Major Products and Services Offered	Details
Silk Road	2011–2013	Shut down	Narcotics, forged identification documents, hacking software	Operated by Ross Ulbricht, a US citizen. Forbade sale of child pornography and weapons. Generated revenues worth US$1.2 billion. Shut down by the FBI in 2013.
Silk Road 2.0	2013–2014	Shut down	Narcotics, forged identification documents, hacking software	Recreated the Silk Road original site. Operated by Blake Benthall, a US citizen. The site was shut down in 2014 in a multi-nation crackdown, Operation Onymous.
Agora	2013–2015	Shut down	Narcotics, forged identification documents, hacking software	Shut itself down in 2015, fearing that potential attacks on the site might identify the site's servers and operators.
Evolution	2014–2015	Shut down	Narcotics, forged identification documents, hacking software	Closed itself down in 2015 in an exit scam; site administrators embezzled an estimated US$12 million in bitcoins.
AlphaBay	2014–2017	Shut down	Narcotics, forged identification documents, hacking software	At its peak, had 40,000 vendors selling to more than 200,000 buyers; transacted an estimated US$1 billion since its creation in 2014. Shut down in 2017 in a multi-nation crackdown, Operation Bayonet. Owner was Alexandre Cazes, a Canadian citizen.
Hansa	N.A.–2017	Shut down	Narcotics, forged identification documents, hacking software	One of the largest marketplaces from Europe. Taken over by Dutch law enforcement agencies for a month to obtain details about vendors, users and criminal activities on the site. Shut down in 2017 in Operation Bayonet.
Dream Market	2013–present	Operational	Narcotics, digital goods, services (hacking, cash outs for cards and PayPal accounts, money), counterfeit items, hacking tutorials	After the fall of Hansa and AlphaBay, this site is the leading black marketplace. Currently, it has more than 140,000 listings, predominantly narcotics. Site forbids buying and selling of weapons, poisons, child pornography and snuff movies.
Tochka	2015–present	Operational	Narcotics, prescription drugs, counterfeit currencies, hacking tutorials, European visa stickers	Smaller than its peers, but gaining popularity. Apart from cryptocurrencies, it allows payment from PayPal accounts.

Market Site	Years of Operation	Status	Major Products and Services Offered	Details
Wallstreet Market	2016–present	Operational	Narcotics, counterfeit items, jewellery and gold, consumer electronics, forged identification documents, hacking software, malware, security and hosting services, digital goods, social engineering tools, carding	Forbids the buying and selling of weapons, poisons, child pornography, snuff movies, contract killing and human trafficking. Modern, up-to-date, innovative market offering more than 11,000 products. As of October 1, 2018, claims more than 3,200 vendors and 630,000 customers. An award system exists for certain advanced security features such as multi-signature transactions, using escrow and logging in with the PGP key to encourage site users to follow security practices.
Silk Road 3.0	N.A.–present	Operational	Narcotics, prescription drugs, counterfeit items, carding	Not linked to original Silk Road sites. Forbids buying and selling of weapons, poisons, anything related to terrorism and child pornography.
Berlusconi Market	2017–present	Operational	Narcotics, prescription drugs, counterfeit items, digital goods, jewellery and gold, weapons, carding, hacking tutorials, malware	One of the major black marketplaces that sells weapons including ammunition, pistols, long-range guns, explosives, hand weapons and so forth.
Empire	2018–present	Operational	Narcotics, prescription drugs, counterfeit items, digital goods, jewellery and gold, weapons, carding, hacking tutorials, malware	Modelled after AlphaBay. Launched in early 2018, sells weapons *inter alia*. Lists more than 5,000 products.

Source: Gateway House research.
Note: This data is accurate as of October 1, 2018.

Table 3: Major Global Crackdowns on Digital Black Markets

Crackdown/Operation	Year of Crackdown	Target	Details
Operation Adam Bomb	2012	The Farmer's Market	Operation executed by the US Drug Enforcement Administration. When taken down, the site had processed US$2.5 million in orders for illegal drugs over several years.
FBI Crackdown	2013	Silk Road	The FBI operation specifically targeted Silk Road and its owner, Ross Ulbricht, who was convicted for continuing to conduct a criminal enterprise, narcotics trafficking, money laundering and computer hacking. He is serving a life sentence.
Operation Onymous	2014	Silk Road 2.0 and other sites	A multi-nation operation involving the FBI and Europol, resulting in 17 arrests of vendors and administrators running digital black marketplaces. More than 400 hidden services were taken down. The arrested included the operator of Silk Road 2.0, Blake Benthall. Bitcoins worth US$1 million were seized, along with €180,000 in cash.

Crackdown/Operation	Year of Crackdown	Target	Details
Operation Commodore	2014	Utopia	Operation by Dutch National Police resulting in the arrest of five Dutch citizens. The authorities also seized 900 bitcoins worth €400,000 during the crackdown.
Operation Shrouded Horizon	2015	Darkode forum	A multi-nation crackdown led by the FBI, involving security agencies from 19 countries, successfully targeted the 300-member forum.
Operation Bayonet	2017	AlphaBay and Hansa	A multi-nation crackdown involving the FBI, US Drug Enforcement Agency and Dutch National Police, with Europol support. Dutch authorities took covert control of Hansa's site.
Operation Darkness Falls	2018	Fentanyl and other narcotics vendors	The operation targeted people and organizations selling fentanyl and other narcotic drugs in digital black marketplaces. One of the targeted vendors, MH4LIFE, had the highest number of verified transactions worldwide of any fentanyl vendor on the Dream Market site.
Operation Disarray	2018	Narcotics traffickers	An FBI-led, US-wide law enforcement action against online drug traffickers that goes beyond arresting drug traffickers to educate users about the perils of drug addiction and trains law enforcement officials to disrupt online narcotics sales.
Crackdowns by Canadian Authorities			
Project E-Neophile	2017	Drug trafficking operation	Investigation by the RCMP specifically targeted a fentanyl and carfentanil trafficking operation, run on the Dark Web from Kelowna, British Columbia. The narcotics were trafficked throughout Canada and internationally to the United States, Australia and Europe.
Project Adoration	2017	Leakedsource.com	RCMP targeted the website, LeakedSource.com, hosted in Quebec, which sold stolen personal identities. The site's database of approximately three billion personal identity records and associated passwords could be purchased for a small fee. Authorities charged Jordan Evan Bloom of Ontario.
RCMP Crackdown	2018	Online vendor named "Mr. Hotsauce"	RCMP targeted online vendor "Mr. Hotsauce," who sold narcotics including fentanyl, heroin, cocaine and ketamine, among others, to customers in Canada and around the world.

Source: Gateway House research.

Overview of Relevant Indian Policy Measures

Table 4.1: Regulations

Act/Policy/Advisory	Year	Details
Cyber Security		
Information Technology Act	2000 (amended in 2008)	The act elaborates on offences, penalties and breaches and outlines the justice dispensation systems for cybercrimes. Sections 66E, 67 and 67A of the act provide for punishment and fines for voyeurism, publishing or transmitting obscene or sexually explicit material in electronic form. Section 67B of the act specifically provides stringent punishment for publishing, browsing or transmitting child pornography in electronic form.
National Cyber Security Policy	2013	The policy envisages protecting India's critical information infrastructure, reducing vulnerabilities, building capabilities to prevent and respond to cyber threats and minimizing damage from cyber incidents.
Reserve Bank of India Advisory on Virtual Currencies	2013	The advisory cautions users, holders and traders of virtual currencies — including bitcoins — about the potential economic, financial, operational, legal, customer protection and security-related risks associated in dealing with such currencies. The advisory was reiterated by the bank in 2017 to clarify that it had not given any licence or authorization to any entity or company to operate cryptocurrency schemes or deal with bitcoin or any other virtual currency.
Narcotics Trafficking		
Narcotic Drugs and Psychotropic Substances Act	1985	The act prohibits a person from producing, manufacturing, cultivating, possessing, selling, purchasing, transporting, storing or consuming any narcotic drug or psychotropic substance.
Prevention of Money Laundering Act	2002 (amended in 2005, 2009 and 2012)	The act deals with money laundering as linked to various offences, including crimes committed under the Narcotic Drugs and Psychotropic Substances Act.
Firearms Regulations		
Arms Act	1959	The act is aimed at curbing illegal weapons and violence stemming from their use.
The Explosive Substances Act	1908	The act defines explosive substances and states the punishment for explosion likely to endanger life or property.
Pornography and Trafficking of Women and Children		
Protection of Children from Sexual Offences Act	2012	The act provides legal framework for preventing all kinds of child sexual abuse, including use of children for pornography and storing child pornography material.
Immoral Traffic Prevention Act	1986	The act specifically deals with trafficking in relation to commercial sexual exploitation. An amendment to the bill pertaining to the rights of female sex workers has been under consideration of the government for many years.

Source: Gateway House research, based on data obtained from the official websites of the Indian government.

Table 4.2: Indian Government Agencies Dealing with Cyber Security

Agency	Year	Details
Computer Emergency Response Team India	2004	This is a nodal agency to deal with India's cyber-security threats. It aims to strengthen the security-related defence of the Indian internet domain.
NCCC and I4C	N.A.	These two agencies will work under the Ministry of Home Affairs. The NCCC will scan cyberspace for threats. The NCCC's phase 1 is operational. The I4C will monitor cybercrimes.

Source: Gateway House research, based on data obtained from the official websites of the Indian government.

Overview of Relevant Canadian Policy Measures

Table 5.1: Regulations

Act/Strategy/Policy	Year	Details
Cyber Security		
2018 National Cyber Security Strategy	2018	The Canadian National Cyber Security Strategy establishes three goals in response to evolving threats, emerging opportunities and the need for collaborative action: · secure and resilient Canadian systems; · an innovative and adaptive cyber ecosystem; and · effective leadership and collaboration.
Personal Information Protection and Electronic Documents Act (PIPEDA)	2000 (amended in 2015)	Canada's Privacy Law, PIPEDA, was amended in 2015 to include provisions related to privacy and data security, including mandatory data breach notification and mandatory record keeping for all breaches. The act maintains that individuals should also be assured that their information will be protected by appropriate safeguards.
Cyber Security Cooperation Program	2014	The program, launched in 2014, is a five-year, CDN$1.5 million initiative to support projects through grants and contributions to improve the security of Canada's vital cyber systems.
GetCyberSafe	2011	Part of the National Cyber Security Strategy, this public awareness campaign provides information on cyber security to help Canadian citizens protect themselves, their families, and their small and medium businesses online. The campaign also observes Cyber Security Awareness Month every October to inform citizens of the importance of cyber security.
RCMP Cybercrime Strategy	2015	The RCMP's Cybercrime Strategy focuses on ways to improve Canada's national police force in its fight against the threat of cybercrime. The strategy supports the National Cyber Security Strategy.
Narcotics Trafficking		
Controlled Drugs and Substances Act	1996	The act is Canada's main drug-control legislation. It criminally prohibits the possession, cultivation, production, importation or exportation of certain scheduled substances, including cannabis, cocaine, heroin, amphetamines, LSD and other narcotics.
Firearms Regulations		
Firearms Act	1995	The act regulates firearms possession, shipment and firearms-related offences in Canada.

Act/Strategy/Policy	Year	Details
Part V of Criminal Code (R.S.C., 1985, c. C-46)	1985 (amended in 2018)	Canadian laws addressing child pornography are set out in Part V of the Criminal Code dealing with Sexual Offences, Public Morals and Disorderly Conduct. It forbids the production, distribution and possession of child pornography.
National Strategy for the Protection of Children from Sexual Exploitation on the Internet	2004	The strategy aims to increase the capacity of law enforcement agencies to investigate and track down perpetrators of child sexual exploitation; to enhance public education and awareness on the issue; and to support further research on the issue. It also operates a national tipline (cybertip.ca) and conducts public awareness and education programming. It also uses Arachnid crawler — a search engine to scan websites — to quickly remove objectionable content from the internet.

Source: Gateway House research, based on data obtained from the official websites of the Indian government.
Note: This data is accurate as of October 1, 2018.

Table 5.2: Canadian Government Agencies Dealing with Cyber Security

Agency	Year	Details
Canadian Centre for Cyber Security	2018	Envisaged under the 2018 National Cyber Security Strategy, the new agency will consolidate the work of three other government departments : the Canadian Cyber Incident Response Centre (Public Safety Canada), Security Operations Centre (Shared Services Canada) and the Informational Technology Security Branch of the Communications Security Establishment.
RCMP	1920	The RCMP is the national federal police of Canada responsible for law enforcement. It has been behind many of the domestic crackdowns on online black markets.
Canadian Internet Registration Authority	1998	This agency manages the official Canadian internet domain (.ca) as a public resource for Canada. It manages 11 internet exchange points across Canada.

Source: Gateway House research, based on data obtained from the official websites of the Canadian government.

Works Cited

Akerlof, George. 1970. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." *The Quarterly Journal of Economics* August 84 (3): 488–500.

Algarni, Abdullah M. and Yashwant K. Malaiya. 2014. "Software Vulnerability Markets: Discoverers and Buyers." *International Journal of Computer, Electrical, Automation, Control and Information Engineering* 8 (3): 480–89.

Al-Hur Media. 2018. "Ansar Ghazwatul Hind: Security guidelines for the Mujahideen in Kashmir." Instructional poster, Rabi Al Awal 1440 (November).

Alpeyev, Pavel and Grace Huang. 2014. "Sony Hackers Seen Having Snooped for Months, Planted Bomb." *Bloomberg*, December 19. www.bloomberg.com/news/articles/2014-12-19/sony-hackers-seen-having-snooped-for-months-planted-bomb.

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.

Basu, Arindrajit. 2018. "Lessons from US response to cyber attacks." *Hindu Business Line*, October 30. www.thehindubusinessline.com/opinion/lessons-from-us-response-to-cyber-attacks-ep/article25372326.ece.

Bellemare, Andrea. 2017. "The secret life of Alexandre Cazes, alleged dark web mastermind." *CBC News*, July 23. www.cbc.ca/news/canada/montreal/alexandre-cazes-millionaire-cars-property-alphabay-1.4215894.

Bender, Ruth and Christopher Alessi. 2016. "Munich Shooter Likely Bought Reactivated Pistol on Dark Net." *Wall Street Journal*, July 24. www.wsj.com/articles/munich-shooter-bought-recommissioned-pistol-on-dark-net-1469366686.

Canada. 1994. *Treaty between the Government of Canada and the Government of the Republic of India on Mutual Assistance in Criminal Matters*. October 24. http://publications.gc.ca/collections/collection_2016/amc-gac/E3-1995-18.pdf.

———. 2017a. *Horizontal Evaluation of Canada's Cyber Security Strategy.* Public Safety Canada. September 29. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-cnd-scrt-strtg/index-en.aspx.

———. 2017b. "Canada prepares to join the Arms Trade Treaty." Global Affairs Canada, April 13. www.canada.ca/en/global-affairs/news/2017/04/canada_prepares_tojointhearmstradetreaty.html.

———. 2018a. "Cannabis Legalization and Regulation." Department of Justice, October 17. www.justice.gc.ca/eng/cj-jp/cannabis/.

———. 2018b. "Government of Canada consults allies in fight against online child sexual exploitation." Public Safety Canada, March 29. www.canada.ca/en/public-safety-canada/news/2018/03/government-of-canada-consults-allies-in-fight-against-online-child-sexual-exploitation.html.

Center for Strategic and International Studies and McAfee. 2014. "Net Losses: Estimating the Global Cost of Cybercrime." June. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

Dingledine, Roger, Nick Mathewson and Paul Syverson. 2004. "Tor: The Second-Generation Onion Router." US Naval Research Laboratory, Release number 03-1221.1-2602. www.nrl.navy.mil/itd/chacs/sites/www.nrl.navy.mil.itd.chacs/files/pdfs/Dingledine%20etal2004.pdf.

Douceur, J. R. 2002. "The Sybil Attack." In *Peer-to-Peer Systems*, edited by Peter Druschel, Frans Kaashoek and Antony Rowstron, volume 2429, 251–60.

DW. 2015. "Report: Evidence Paris attack weapons shipped from Germany." DW, November 27. https://p.dw.com/p/1HDKP.

Europol. 2017. "Massive Blow to Criminal Dark Web Activities after Globally Coordinated Operation." July 20. www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

———. 2019. "Operation Onymous." www.europol.europa.eu/activities-services/europol-in-action/operations/operation-onymous.

FBI. 2013. "Criminal Complaint against Ross William Ulbricht." United States Department of Justice. September 27. www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf.

———. 2014. "Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court." US Department of Justice, November 6. www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court.

G20. 2018. "The G20 confirms the importance of the digital economy for global development." August 24. www.g20.org/en/news/g20-confirms-importance-digital-economy-global-development.

Hager, Mike. 2018. "Canadian police face hurdles over staffing, lack of drug-screening devices as cannabis legalization nears." *The Globe and Mail*, October 1. www.theglobeandmail.com/cannabis/article-canadian-police-face-hurdles-over-staffing-lack-of-drug-screening/.

India. 2013. "Why India abstained on Arms Trade Treaty." Ministry of External Affairs, April 3. https://mea.gov.in/articles-in-indian-media.htm?dtl/21503/Why+India+abstained+on+Arms+Trade+Treaty.

———. 2015. *Narcotics Control Bureau 2015 Annual Report.* Ministry of Home Affairs, Government of India, New Delhi. http://narcoticsindia.nic.in/upload/download/document_id43e4e6a6f341e00671e123714de019a8.pdf.

———. 2016. *Narcotics Control Bureau 2016 Annual Report.* Ministry of Home Affairs, Government of India, New Delhi. http://narcoticsindia.nic.in/upload/download/document_idcfa45151ccad6bf11ea146ed563f2119.pdf.

———. 2017. "India-Canada Relations." Ministry of External Affairs, October. www.mea.gov.in/Portal/ForeignRelation/Canada_October_2017.pdf.

———. 2018a. *Narcotics Control Bureau 2017 Annual Report.* Narcotics Control Bureau, Ministry of Home Affairs, Government of India, New Delhi. http://narcoticsindia.nic.in/upload/download/document_id17c3433fecc21b57000debdf7ad5c930.pdf.

———. 2018b. "India-Canada Joint Statement during State Visit of Prime Minister of Canada to India." Ministry of External Affairs, February 23. www.mea.gov.in/bilateral-documents.htm?dtl/29512/IndiaCanada+Joint+Statement+during+State+Visit+of+Prime+Minister+of+Canada+ to+India+February+23+2018.

Interpol. 2018. "INTERPOL holds first DarkNet and Cryptocurrencies Working Group." April 3. www.interpol.int/News-and-media/News/2018/N2018-022.

Kruithof, Kristy, Judith Aldridge, David Décary Hétu, Megan Sim, Elma Dujso and Stijn Hoorens. 2016. "Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands." Wetenschappelijk Onderzoek-en Documentatiecentrum, Ministerie van Veiligheid en Justitie. www.rand.org.pubs/ research_reports/RR1607.html.

Patil, Sameer. 2018a. Interview with Indian police official, Mumbai, September.

———. 2018b. "Punjab's unshakable drug smuggling networks." Gateway House, April 18. www.gatewayhouse.in/punjabs-drug-smuggling.

———. 2018c. "India's lead on Cyber space Governance." Gateway House, August 15. www.gatewayhouse.in/india-cyber-space-governance/.

RCMP. 2018. "Greater Toronto Area RCMP arrest Darkweb Drug Trafficker." May 31. www.rcmp-grc.gc.ca/en/news/2018/greater-toronto-area-rcmp-arrest-darkweb-drug-trafficker.

Richwine, Lisa. 2014. “Cyber attack could cost Sony studio as much as $100 million.” *Reuters*, December 10. www.reuters.com/article/sony-cybersecurity-costs-idUSL1N0TT1YO20141209.

Sony Pictures. 2014. “Message for current and former Sony Pictures employees and dependents, and for production employees.” December 15. www.sonypictures.com/corp/notification/SPE_Cyber_Notification.pdf.

Syverson, Paul. 2003. “Onion routing for resistance to traffic analysis.” *Proceedings DARPA Information Survivability Conference and Exposition* 2: 108–10.

United Nations Office on Drugs and Crime. 2018. *World Drug Report 2018*. Vienna, Austria. June. www.unodc.org/wdr2018.

Weimann, Gabriel. 2016. “Terrorist Migration to the Dark Web.” *Perspectives on Terrorism* 10: 3. www.terrorismanalysts.com/pt/index.php/pot/article/view/513/1013.

Woolf, Nicky. 2015. “Bitcoin ‘exit scam’: deep-web market operators disappear with $12m.” *The Guardian,* March 18. www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars.

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