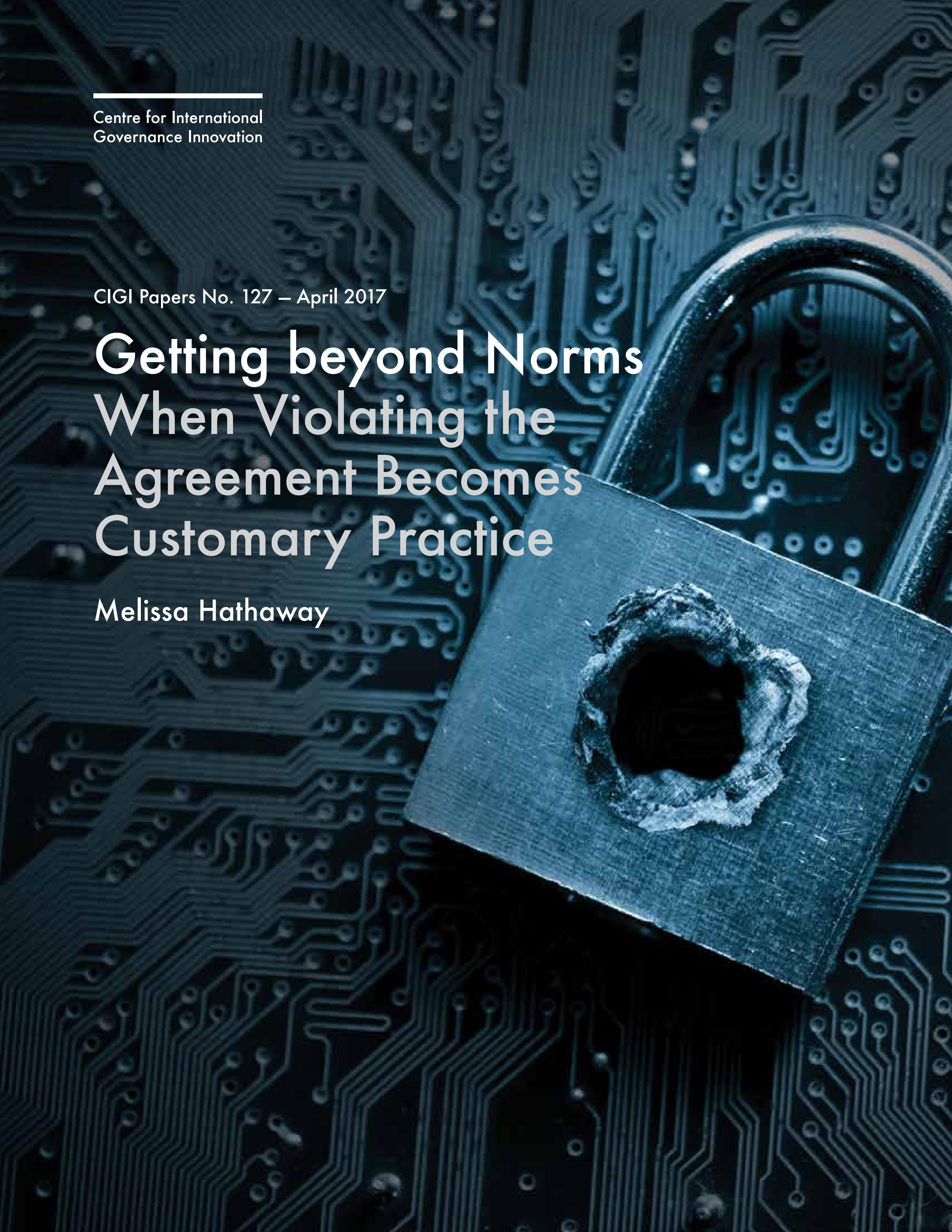
Centre for International
Governance Innovation



CIGI Papers No. 127 – April 2017

Getting beyond Norms
When Violating the Agreement Becomes Customary Practice

Melissa Hathaway

Centre for International
Governance Innovation

CIGI Papers No. 127 — April 2017

Getting beyond Norms

When Violating the Agreement Becomes Customary Practice

Melissa Hathaway

CIGI Masthead

Executive

President Rohinton P. Medhora

Director of Finance Shelley Boettger

Director of the International Law Research Program Oonagh Fitzgerald

Director of the Global Security & Politics Program Fen Osler Hampson

Director of Human Resources Susan Hirst

Director of the Global Economy Program Domenico Lombardi

Chief Operating Officer and General Counsel Aaron Shull

Director of Communications and Digital Media Spencer Tripp

Publications

Publisher Carol Bonnett

Senior Publications Editor Jennifer Goyder

Publications Editor Patricia Holmes

Publications Editor Nicole Langlois

Publications Editor Sharon McCartney

Publications Editor Lynn Schellenberg

Graphic Designer Melodie Wakefield

For publications enquiries, please contact publications@cigionline.org.

Communications

For media enquiries, please contact communications@cigionline.org.

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

Printed in Canada on paper containing 10% post-consumer fibre and certified by the Forest Stewardship Council and the Sustainable Forestry Initiative.

Centre for International
Governance Innovation

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

Table of Contents

About the Author

Melissa Hathaway is a distinguished fellow at the Centre for International Governance Innovation (CIGI), a senior adviser at Harvard Kennedy School's Belfer Center for Science and International Affairs, and the president of Hathaway Global Strategies, LLC. She is a leading expert in cyberspace policy and cyber security and served in two US presidential administrations, spearheading the Cyberspace Policy Review for President Barack Obama and leading the Comprehensive National Cybersecurity Initiative for President George W. Bush.

About the Global Security & Politics Program

The Global Security & Politics Program at CIGI focuses on a range of issues in global security, conflict management and international governance — a landscape that continues to change dramatically. Such changes are widely evident in the growing rivalry between China and the United States in the Asia-Pacific and the emergence of new economic powers in the region, such as Indonesia; the divergent ways Canada, Russia and the United States perceive Arctic security as melting ice opens up the Northwest Passage; continuing debates about the humanitarian imperative as the world confronts new crises in Africa and the Middle East; and new areas of concern such as cyber warfare and the security of the Internet.

With experts from academia, national agencies, international institutions and the private sector, the Global Security & Politics Program supports research in the following areas: Arctic governance; Asia and the Pacific; fixing climate governance; governance of conflict management, with a focus on Africa; global politics and foreign policy; and Internet governance.

Executive Summary

In recent years, countries have become increasingly concerned about the immediate and future threats to their critical services and infrastructures that could result from the misuse of information and communications technologies (ICTs). As such, countries have placed the development of normative standards guiding state behaviour in cyberspace at the top of their foreign policy agendas. Yet, despite broad international consensus regarding the basic principles to limit the misuse of ICTs in the digital age and to constrain state behaviour, the key tenets have been consistently violated.

All evidence suggests that states are not following their own doctrines of restraint and that each disruptive and destructive attack further destabilizes our future. States have turned a blind eye and have shirked their responsibility for curbing or halting cyber attacks originating from their own territories. Disruption or damage (or both) of critical infrastructures that provide services to the public has become customary practice — the "new normal." And this intentional misuse of ICTs against critical infrastructures and services has great potential to lead to misperception, escalation and even conflict.

This paper offers five standards of care that can be used to "test" individual states' true commitment to the international norms of behaviour. Only with a concerted and coordinated effort across the global community will it be possible to change the new normal of "anything goes" and move forward to ensure the future safety and security of the Internet and Internet-based infrastructures.

Introduction

Critical infrastructure sectors and services such as electricity generation, gas and oil production, telecommunications, water supply, transportation and financial services are becoming uniquely vulnerable to malicious attacks because of their increased automation, interconnectedness and reliance on the Internet. This infrastructure-Internet entanglement has become a strategic vulnerability for most countries around the world, which are realizing that this profound weakness can threaten their national security and, potentially, international peace and stability. This realization came to the forefront a decade ago, when a malicious computer worm known as Stuxnet was used to degrade and ultimately shut down Iran's nuclear facility in Natanz in 2007. The use of this military-grade cyber weapon against a state sparked intense and urgent conversations within the international community about the importance of norms for state responsibility in cyberspace to ensuring the future safety and security of the Internet and Internet-based infrastructures.

Cyber insecurity is both a sovereign issue and an international challenge. The volume, scope, scale and sophistication of cyber threats to critical services and infrastructures are outpacing defensive measures, while data breaches, criminal activity, service disruptions and property destruction are becoming commonplace (Hathaway 2016). The Stuxnet source code was analyzed by experts around the world and then replicated (as, for example, Flame, Gauss, DuQu, Wiper and so on), proliferated and traded on the black market by both state and non-state actors (Hathaway 2012). Countries are now increasingly concerned about the immediate and future threats that could emanate from the misuse of ICTs, and that could jeopardize international peace and security similarly to terrorism, transnational organized crime, infectious diseases, environmental degradation and nuclear, biological, chemical and radiological weapons. This makes it all the more necessary to advance a dialogue on how best to limit the misuse of ICTs in the digital age and constrain state behaviour in cyberspace.

Codifying Responsible State Cyber Behaviour

The development of normative standards guiding state behaviour — and especially the "norm of state responsibility" — is enshrined in the United Nations (UN) Charter (2001).[1] By signing the UN Charter, states not only commit to respecting the sovereignty rights of other countries, but they also accept certain responsibilities, which include avoiding harm to other states. Seeking to build on this common understanding and customary law, the United Nations initiated a series of diplomatic negotiations among a small group of nations known as the UN Governmental Group of Experts (UN GGE), established under the UN General Assembly, to identify fundamental first steps and behaviours to protect critical national and international infrastructures from cyber harm and ultimately to reduce collective risks posed by malicious activities (Lotrionte 2012, 829). Following various UN GGE meetings, national experts from member countries began to codify assessments and recommendations into voluntary, non-binding norms. In July 2015, member countries of the UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security — a group of representatives from 20 nations from all over the world[2] — endorsed and adopted a new set of voluntary, non-binding norms of responsible state behaviour in cyberspace (UN General Assembly 2015; see also UN Office for Disarmament Affairs n.d.).

Three norms stand out in particular. The UN GGE member countries agreed that:

→ "A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public" (UN General Assembly 2015, para 13(f));

→ "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs" (ibid., para 13(c)); and

→ "States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions" (ibid., para 13(g)).

The De Facto Norms

Despite unanimous consensus on this high-level set of international norms and endorsement by the UN General Assembly in December 2015, some of these key tenets have been consistently violated, thus undermining the integrity of the entire agreement. Even worse, not only has there been intentional disruption and damage to critical infrastructures and services of states since the approval of this agreement, none of the signatories have publicly objected to the wrongful use of ICTs and harm caused to nations. This silence is contributing to a new de facto norm — "anything goes" — and this is dangerous because it increases the risks to international peace, security and stability.

Disrupting or damaging critical infrastructures that provide services to the public has become customary practice — the new normal. In the past two years and since the UN GGE agreement, there have been an alarming number of harmful incidents targeting critical infrastructures around the world, ranging from power systems to telecommunications systems to transportation systems to financial systems. For example, in late December 2015, three Ukrainian regional electric power distribution companies were simultaneously targeted, bringing more than 50 substations off-line and leaving more than 225,000 residents without power for up to six hours. The malicious software used in this attack damaged equipment and prevented engineers from remotely restoring power. Months later, the distribution centres were still running under constrained operations, affecting quality

[1] Under customary international law of state responsibility, states bear responsibility for any act that is attributable to the state that is a breach of an international legal obligation applicable to that state. Following the 9/11 attacks, the "norm of state responsibility" under international law has been more broadly interpreted to include "state responsibility for the actions of non-state actors that follow from the state's failure to meet its international obligations to prevent its territory from being used as a platform or sanctuary for the non-state actors to attack other states" (Lotrionte 2012, 857).

[2] Member countries of the UN GGE are: Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, the Republic of Korea, the Russian Federation, Spain, the United Kingdom and the United States.

of service to citizens and businesses (Industrial Control Systems Cyber Emergency Response Team 2016). Almost exactly one year later, Ukraine suffered another sophisticated attack against the Pivnichna substation outside of its capital, Kiev (Goodin 2017). The attacks against Ukraine were successful and quite instructive, especially because they were clear instances in which intentional damage against a state's critical infrastructure was perpetrated (Lee, Assante and Conway 2016) — and likely conducted by a UN GGE member state — and the rest of the world did not condemn the actions. And while the UN GGE norm only applies during peacetime, others would say that this type of attack against a civilian target must still meet a necessary and proportional threshold, permissible during wartime under international law. Similar destructive malware has since been discovered in nuclear and electric power plants in Germany, South Korea, the United States and elsewhere, and the leaders of those nations have remained largely silent.

In the last quarter of 2016, Internet service providers (ISPs) and businesses around the globe were victims of a variety of disruptive and damaging distributed denial of service (DDoS) attacks. Even more worrisome is the fact that DDoS attacks that are significantly above 200 gigabits per second can be dangerous for network operators and cause collateral damage across service providers, cloud hosting environments and enterprise networks (NetScout 2016). Attacks of this size can also impair the functionality of the entire Internet infrastructure — disrupting the free flow of goods, services, data and capital across borders. Recent DDoS attacks have peaked at 1 terabit per second (Khandelwai 2016; Goodin 2016). The harm posed to nations by DDoS attacks underscores the importance of two of the international norms adopted by UN GGE and from the list above, specifically that "States should take appropriate measures to protect their critical infrastructure from ICT threats" and "should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."

In 2016, individuals in the United States created and deployed a malicious software called "Mirai" to turn Internet-connected devices into remotely controlled "bots" that were then used to mount large-scale network attacks.[3] For example, in October 2016, the Mirai malicious software was used to launch a DDoS attack against the Domain Name System (DNS) infrastructure and Internet provider Dyn in the United States (York 2016; Hilton 2016). The DNS is the "telephone directory" for the Internet, so when Dyn was knocked off-line, all of its customers were too, including PayPal, *The New York Times*, Spotify, Airbnb and others. Thousands of citizens and other businesses were adversely affected as well.

In November 2016, the Mirai software was used again in Europe, knocking nearly one million Deutsche Telekom customers off-line (Auchard 2016). This time, the malicious software attempted to infect routers and thus could have affected a much broader part of the Internet's infrastructure.

The Mirai attacks have highlighted various vulnerabilities and the lack of security of the "Internet of Things" (IoT) and the "smart" devices it comprises. This attack also highlights why the Internet's security and stability is an international issue. As countries continue to embrace the economic opportunities of becoming more connected to the Internet and adopting and embedding more IoT devices in every part of life, they must also prepare for the misuse of those same ICT-based devices.

Moreover, countries should be held accountable to the UN GGE norm that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs." Allowing infected devices within a country's territory to be harnessed to conduct illegal or illicit activity against another state, is, in fact, a clear violation of this norm. States must demonstrate that they are willing to take the necessary steps to protect the security and mitigate the misuse of the Internet in their own countries. By funding and fielding results-based initiatives, a state can demonstrate its active vigilance and commitment to minimize and mitigate the damages caused by any misuse of ICT-based devices and therefore become a steward for the promotion of safety, security and stability in cyberspace. For example, states should invest in technologies and regulations that could be used to mitigate malicious rerouting of Internet traffic and that would make

[3] The Mirai malicious software has two functions: it has an "attack now" component that harnesses and channels traffic from an infected device and directs it toward a victim's server, and a "go looking" function that uses traffic from an infected device to hunt for other insecure devices to infect.

it harder for machines (within a state's sovereign networked infrastructures) to be harnessed in a botnet and used in a scaled DDoS attack.

Earlier in 2016, Sweden also suffered a series of attacks against its critical infrastructures. The attacks began in May with the purposeful sabotage of the radio mast owned and operated by the state-owned broadcasting company, Teracom. Of particular importance, this mast supports the national command-and-control system of the country (Reuters 2016b). Swedish experts believe that this activity was a violation of the UN GGE norm of non-interference in the internal affairs of the state. It was also a clear violation of the norm against conducting activities that impair the use and operation of critical infrastructures. A few days later, air traffic control glitches were recorded in the computer systems at Stockholm's Arlanda and Bromma airports, as well as at the Landvetter airport in Gothenburg. At that time, aviation authorities said that a "communications problem" with a radar system forced them to ground all planes (*NT News* 2016; Roden 2016). Although the radar problem was fixed several hours later, subsequent delays and disruptions raised fears about the ramifications of a potential compromise of Sweden's air traffic control system. The possibility of sabotage was later dismissed, but the events caused great concern among Sweden's leaders.[4]

Beginning in November 2016 and culminating in January 2017, Saudi Arabia was the victim of a series of critical infrastructure attacks that used the Shamoon 2 virus. The original Shamoon virus was first observed in 2012 and was designed to collect, disrupt and damage targeted systems. The virus propagates through networked systems, compiles lists of files from specific locations on those systems, uploads files to the attacker and then erases the master boot record of the infected system to render it inoperable. The Shamoon 2 virus is even more virulent and effective. In January 2017, the Saudi government issued a warning notice to all telecommunications companies alerting them that they had "detected destructive electronic strikes against several government agencies and vital establishments" (Agence France Press 2017; Shamseddine et al. 2017). The Saudi government went on to claim that this was a systemic attack on crucial government agencies, including the transportation sector, and that the attacks were aimed at halting operations, stealing data, planting viruses and damaging equipment by overwriting the master boot record (which makes attribution difficult because it erases the intruder's tracks) (Chan 2016). These attacks have continued for months and are a clear violation of the UN GGE norm that a "State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public." At the time of this writing, members of the UN GGE have not publicly renounced the harm caused to Saudi Arabia by these attacks.

Finally, for the last several years and especially since December 2015, the global financial services sector has experienced a wide range of malicious activities ranging from DDoS attacks to breaches of core networks, which, in turn, have resulted in the loss of both personal identifiable information and real money. A number of breaches at major banks were caused by security weaknesses in their Society for Worldwide Interbank Financial Telecommunication (SWIFT) system — the interbank messaging system used by banks and companies to move money. In February 2016, hackers were able to use this electronic bank messaging technology to steal US$81 million — one of the biggest electronic heists in history — from the Bangladesh Central Bank's official account at the New York Federal Reserve Bank, and to transfer it to accounts in the Philippines. After intense investigation by law enforcement, SWIFT acknowledged that the scheme involved altering SWIFT software on Bangladesh Bank's computers to hide evidence of fraudulent transfers, and the Philippine Central Bank admitted that its accounts were illegally used to enable a web of transfers and currency conversions, before moving the cash through casinos in Manila and junket operators (Barrett and Burne 2016).

It was not until April 2016 that SWIFT finally warned customers that it was aware of "a number of recent cyber incidents" where attackers had sent fraudulent messages over its system and manipulated SWIFT's Alliance Access server software (Reuters 2016a, Finkle 2016). While the warning did not contain the names of any of the victims or discuss the value of any losses from the previous attacks, publicly available information reveals that at least a dozen other banks were victims of this software

[4] Personal interview with Richard Oehme, director, Office of Cybersecurity and Critical Infrastructure Protection, Swedish Civil Contingencies Agency, in Arlington, VA, on October 3, 2016.

vulnerability (Bergin and Finkle 2016; Riley and Katz 2016), some of which lost millions of dollars:

- Tien Phong Bank, Vietnam (thwarted attack in December 2015) (*RT News* 2016);
- Banco del Austro SA, Ecuador (lost US$12 million in January 2015) (Schwartz 2016; Townsend 2016);
- Bangladesh Central Bank, Bangladesh (lost US$81 million in February 2016) (Kovacs 2016); and
- Philippine Central Bank, Philippines (involved in the Bangladesh fraud) (ibid.).

The forensic analysis of the malware used against the Tien Phong Bank showed that the malware contained a "target folder" that included SWIFT coldes for many other banks (Riley, Robertson and Katz 2016), including:

- Industrial & Commercial Bank of China Ltd., China (world's largest bank by assets);
- Bank of Tokyo Mitsubishi UFJ Ltd., Japan (Japan's largest bank);
- UniCredit SpA, Italy (Italy's largest bank);
- Australia & New Zealand Banking Group Ltd., Australia and New Zealand;
- United Overseas Bank Ltd., Singapore;
- Kookmin Bank, South Korea; and
- Mizuho Bank Ltd., Japan.

SWIFT has publicly acknowledged that "the Bangladesh fraud was not an isolated incident," and that they were aware "of at least two, but possibly more, other cases where fraudsters used the same modus operandi" to compromise banks, obtain credentials to payment generation systems to send fraudulent payments and obfuscate the statements/confirmations from their counterparties (Leibbrandt 2016). They also have stated that "the threat is very persistent, adaptive and sophisticated — and it is here to stay," and that banks using the SWIFT network — which includes both central banks and commercial banks — had been hit with a "meaningful" number of attacks, about one-fifth of them resulting in stolen funds since the Bangladesh heist (Bergin and Finkle 2016).

While many of the banks affected are private entities, all central banks and federal reserve banks are also critical infrastructures of nations. The misuse of ICTs against the SWIFT system and the victimization of banks all around the world violate the UN GGE norm that "States should take appropriate measures to protect their critical infrastructure from ICT threats." The SWIFT vulnerability also highlights the needs for states to cooperate, exchange information, assist each other and prosecute the criminal use of ICTs and the Internet.

Five Standards of Care

The number of, and the extent of damage caused by, targeted attacks against power, telecommunication systems, transportation and financial systems since the unanimous endorsement of the UN GGE's set of international norms in December 2015 is alarming. All evidence suggests that states are not following their own doctrine of restraint and that each disruptive and destructive attack further destabilizes our future. States have turned a blind eye and shirked their responsibility for curbing or halting cyber attacks originating from their own territories. Furthermore, the intentional misuse of ICTs against critical infrastructures and services will eventually turn into widespread, transnational disruption of services essential to citizens. It also has great potential to lead to misperception, escalation and even conflict.

If states want these voluntary, non-binding norms of responsible state behaviour in cyberspace to be truly meaningful words that can achieve their desired goals, then their actions and practice must demonstrate those tenets. States must demonstrate that they are willing to take the necessary steps to protect the security and prevent the misuse of the Internet in their respective countries. They must also outwardly condemn harmful acts conducted or condoned by other states. These results-based initiatives would demonstrate individual states' vigilance and commitment to minimize and mitigate the damages caused by any misuse of ICTs, and therefore to become stewards for the promotion of safety, security and stability in cyberspace. The following five standards of care can be used to test individual states' true commitment to the international norms of behaviour they have ascribed to:

- States should take the necessary measures to stop malicious rerouting of Internet traffic and make it harder for machines to be harnessed in a botnet and to participate in a scaled DDoS attack. Specifically, states should require:
  - ISPs and the Internet Exchange (IX) community to do more to identify compromised devices, provide early warning of new infections and offer managed security services to clean up the networked infrastructures to significantly reduce, if not eliminate, the infections;
  - ISPs and the IX community to provide authentic and authoritative routing information, by adopting secure Border Gateway Protocol routing procedures and protocols; and
  - the Internet services community (manufacturers, distributors, suppliers, retailers and others who make digital products and services) to provide authentic and authoritative naming information as part of their product interface or service. DNS trust must be established throughout the DNS hierarchy, from root servers to browsers. (Hathaway 2016; Hathaway and Savage 2012)
- Today's flawed products are disrupting businesses, damaging property and jeopardizing economic and national security. States should focus on consumer protection and citizen safety, in order to mitigate the risks of next-generation threats now posed by the IoT, by introducing proactive responsibility and accountability into the marketplace through product liability. States need to take the necessary steps to hold accountable manufacturers, distributors, suppliers, retailers and others who make digital products and services available to the public for security flaws in their offerings, in particular when the security flaws are easily prevented by commonly accepted good engineering principles at that time.
- States should cooperate on investigations and provide technical, investigative and financial assistance to other states that lack the domestic capacity to do so.
- States should demonstrate commitment to protect their society against cybercrime by codifying domestic criminal legislation and using those laws to prosecute criminal offences both nationally and internationally.
- States should build capacity to investigate cybercrime by training legislative authorities and investigative personnel.

Conclusion

Leaders around the globe have come to recognize that cyber insecurity is both a sovereign issue and an international challenge. The risks to critical infrastructure and services have been shown to adversely affect international peace, security and stability. The UN GGE endorsed and adopted a set of norms for responsible state behaviour in cyberspace. To move from cyber insecurity to cyber stability, states need to enforce these norms, speak out when others violate them, and take steps to adopt and implement the standards of care outlined above. Only with a concerted and coordinated effort across the global community will it be possible to change the new normal of "anything goes" and move forward to ensure the future safety and security of the Internet and Internet-based infrastructures.

Works Cited

Agence France Press. 2017. “Saudi computer systems vulnerable to ‘Shamoon 2’ virus: telco chief.” *Arab News,* January 26. www.arabnews.com/node/1044566/saudi-arabia.

Auchard, Eric. 2016. “German internet outage was failed botnet attempt: report.” Reuters, November 28. www.reuters.com/article/us-deutsche-telekom-outages-idUSKBN13N12K.

Barrett, Devlin and Katy Burne. 2016. “FBI Investigating Bangladesh Bank-Account Heist.” *The Wall Street Journal,* March 18. www.wsj.com/articles/fbi-investigating-bangladesh-bank-account-heist-1458313232.

Bergin, Tom and Jim Finkle. 2016. “Exclusive: SWIFT confirms new cyber thefts, hacking tactics.” Reuters, December 12. www.reuters.com/article/us-usa-cyber-swift-exclusive-idUSKBN1412NT.

Chan, Sewell. 2016. “Cyberattacks Strike Saudi Arabia, Harming Aviation Agency.” *The New York Times,* December 1. www.nytimes.com/2016/12/01/world/middleeast/saudi-arabia-shamoon-attack.html.

Finkle, Jim. 2016. “Exclusive: SWIFT warns customers of multiple cyber fraud cases.” Reuters, April 26. www.reuters.com/article/us-cyber-banking-swift-exclusive-idUSKCN0XM2DI.

Goodin, Dan. 2016. “Record-breaking DDoS reportedly delivered by >145k hacked cameras.” *Ars Technica*, September 28. https://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/.

———. 2017. “Hackers trigger yet another power outage in Ukraine.” *Ars Technica*, January 11. https://arstechnica.com/security/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/.

Hathaway, Melissa. 2012. “Leadership and Responsibility for Cybersecurity.” *Georgetown Journal of International Affairs: International Engagement on Cyber: 2012* November: 71–80.

———. 2016. “What Trump Can Do About Cybersecurity.” *Bloomberg View*, November 30. www.bloomberg.com/view/articles/2016-11-30/what-trump-can-do-about-cybersecurity.

Hathaway, Melissa and John Savage. 2012. “Stewardship of Cyberspace: Duties for Internet Service Providers.” Cyber Dialogue Conference, University of Toronto, Munk School of Global Affairs, Toronto, March. www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_hathaway-savage.pdf.

Hilton, Scott. 2016. “Dyn Analysis Summary Of Friday October 21 Attack.” Dyn Company News, October 26. http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

Industrial Control Systems Cyber Emergency Response Team. 2016. “Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure.” February 25. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

Khandelwai, Swati. 2016. “World’s largest 1Tbps DdoS Attack launched from 152,000 hacked Smart Devices.” *The Hacker News*, September 27. http://thehackernews.com/2016/09/ddos-attack-iot.html.

Kovacs, Eduard. 2016. “Custom Malware Used in $81 Million Bangladesh Bank Heist.” *SecurityWeek*, April 26. www.securityweek.com/custom-malware-used-81-million-bangladesh-bank-heist.

Lee, Robert M., Michael J. Assante and Tim Conway. 2016. “Analysis of the Cyber Attack on the Ukrainian Power Grid.” Defense Use Case No. 5. Washington, DC: SANS Industrial Control Systems and the Electricity Information Sharing and Analysis Center. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Leibbrandt, Gottfried. 2016. “Gottfried Leibbrandt on cyber security and innovation.” Speech at the 14th annual European Financial Services Conference, Brussels, May 24. www.swift.com/insights/press-releases/gottfried-leibbrandt-on-cyber-security-and-innovation.

Lotrionte, Catherine. 2012. "State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights." *Emory International Law Review* 26: 825–919.

NetScout. 2016. "Arbor Networks Releases Global DDoS Attack Data for 1H 2016." Arbor Networks press release, July 19. www.netscout.com/press-release/arbor-networks-releases-global-ddos-attack-data-for-1h-2016/.

NT News. 2016. "Swedish air traffic glitch solved." *NT News*, May 19. www.ntnews.com.au/news/breaking-news/planes-grounded-at-stockholm-airports/news-story/dd8d1c5b483ff8fc058ffd352bbcbb43.

Reuters. 2016a. "SWIFT Bank Network Hit by Multiple Cyber Fraud Attacks." *Fortune*, April 25. http://fortune.com/2016/04/25/swift-cyber-fraud/.

———. 2016b. "Russia under suspicion after sabotage of Swedish telecom mast." *The Guardian*, May 18. www.theguardian.com/world/2016/may/18/russia-under-suspicion-after-sabotage-of-swedish-telecom-mast.

Riley, Michael and Alan Katz. 2016. "Swift Hack Probe Expands to Up to a Dozen Banks Beyond Bangladesh." *Bloomberg Technology*, May 26. www.bloomberg.com/news/articles/2016-05-26/swift-hack-probe-expands-to-up-to-dozen-banks-beyond-bangladesh.

Riley, Michael, Jordan Robertson and Alan Katz. 2016. "Bangladesh, Vietnam Bank Hacks Put Global Lenders on Edge." *Bloomberg*, May 17. www.bloomberg.com/news/articles/2016-05-17/global-lenders-on-edge-as-hacks-embroil-growing-list-of-banks.

Roden, Lee. 2016. "Delays after IT problems halt Stockholm air traffic." *The Local*, May 19. www.thelocal.se/20160519/stockholm-airspace-closed.

RT News. 2016. "Vietnamese bank reports another hacker attack on SWIFT money transfer system." *RT News*, May 16. www.rt.com/business/343196-vietnam-bank-attack-swift/.

Schwartz, Mathew J. 2016. "Another SWIFT Hack Stole $12 Million." Information Security Media Group, May 20. www.bankinfosecurity.com/another-swift-hack-stole-12-million-a-9121.

Shamseddine, Reem, Jim Finkle, Maha El Dahan, Mark Potter and Andrew Hay. 2017. "Saudi Arabia warns on cyber defense as Shamoon resurfaces." Reuters, January 23. www.reuters.com/article/us-saudi-cyber-idUSKBN1571ZR.

Townsend, Kevin. 2016. "Third SWIFT Attack Transfers $12 million to Hong Kong, Dubai and U.S." *SecurityWeek*, June 1. www.securityweek.com/third-swift-attack-transfers-12-million-hong-kong-dubai-and-us.

UN. 2001. General Assembly resolution 56/83, *Responsibility of States for Internationally Wrongful Acts*, art. 1-8. UN Doc A/RES/56/83, Annex (December 12). http://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

UN General Assembly. 2015. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. UN Doc A/70/174 (July 22). www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

UN Office for Disarmament Affairs. n.d. "Developments in the field of information and telecommunications in the context of international security." www.un.org/disarmament/topics/informationsecurity/.

York, Kyle. 2016. "Dyn Statement on 10/21/206 DDoS Attack." Dyn Company News, October 22. http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/.

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 qui formule des points de vue objectifs dont la portée est notamment mondiale. Nos recherches, nos avis et l'opinion publique ont des effets réels sur le monde d'aujourd'hui en apportant autant de la clarté qu'une réflexion novatrice dans 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.

Centre for International
Governance Innovation

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