Centre for International
Governance Innovation

Getting beyond Norms

New Approaches to International Cyber Security Challenges

SPECIAL REPORT

Centre for International
Governance Innovation

Getting beyond Norms

New Approaches to International Cyber Security Challenges

SPECIAL REPORT

Edited by Fen Osler Hampson and Michael Sulmeyer

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
Interim Director of the Global Economy Program Paul Jenkins
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 Susan Bubak
Publications Editor Patricia Holmes
Publications Editor Nicole Langlois
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.

Centre for International Governance Innovation

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

Contents

Acronyms and Initialisms

CBMs	confidence-building measures
CD	Conference on Disarmament
CIGI	Centre for International Governance Innovation
CWC	Convention on Conventional Weapons
DDoS	distributed denial of service
DNS	Domain Name System
GGE	UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
ICANN	Internet Corporation for Assigned Names and Numbers
ICTs	information and communications technologies
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
ISPs	internet service providers
IX	Internet Exchange
LOAC	law of armed conflict
SWIFT	Society for Worldwide Interbank Financial Telecommunication
W3C	World Wide Web Consortium

Introduction

Fen Osler Hampson and Michael Sulmeyer

Preamble

The international cyber security community has not been immune to the global political trend of diminished public trust in globalism and establishment institutions. The ideal of a universally accessible "open internet" is increasingly under stress. China is striving to assert more control of the internet by buying up international data centres, while Russia is more determined than ever to foster instability in the global system. Meanwhile, smaller and developing countries are growing skeptical that the vision of the open internet promoted by liberal democracies is in their interest.

At the same time, billions of consumer devices with questionable security are being connected to the internet. This Internet of Things (IoT) is posing risks to network infrastructure, and to everything attached to it — including critical infrastructure that increasingly relies on the internet, such as the power grid, water supply, telecommunications and financial services. The IoT represents a massive and growing security risk. Given the global interconnections of the internet and supply chains, any reasonable response will require broad international cooperation — something that is becoming more and more difficult to achieve.

With this in mind, the Centre for International Governance Innovation (CIGI) and the Belfer Center for Science and International Affairs at the Harvard Kennedy School brought together 28 academics, diplomats and other specialists for a one-day workshop in Cambridge, Massachusetts, in March 2017. Called "Getting Beyond Norms: New Approaches to International Cyber Security Challenges," the workshop fostered a frank discussion about matters such as the rapidly shifting geopolitical state of play; whether the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) remains the

best venue for addressing cyber security concerns; and how the ongoing challenges may be most effectively discussed going forward. The essays gathered in this special report were either presented by the authors at the workshop or based on the discussions that emerged.

The Rise of Cyber Security Norms

The GGE was established in 2004, comprised of independent experts representing 15 states, to advise the United Nations on how member states should promote peace and stability in cyberspace. The first GGE did not agree on a report, but the second GGE convened five years later was more successful, releasing a report in 2010. In 2013, the third GGE agreed on a set of foundational norms: in short, that international law, state sovereignty and human rights apply to cyberspace. It also stipulated that states must not use proxies to commit cyber attacks on other states, nor should they allow non-state actors to launch attacks from their territory. The next GGE, with 20 members, expanded and elaborated on those concepts with its 2015 report. It noted, among other things, the principle of non-intervention in other states' internal affairs; that states should not conduct or support cyber attacks that damage critical infrastructure; and that states should protect their own critical infrastructure from threats to information and communications technologies (ICTs).

But as Melissa Hathaway explains in her essay, "When Violating the Agreement Becomes Customary Practice," the consensus around these norms hasn't stopped them from being violated. For example, a suspected state-sponsored cyber attack in December 2015 targeted Ukraine's power grid — just months after the GGE released its report putting critical infrastructure off limits to attackers. Other attacks in the past year have targeted a Swedish radio tower used for rescue communications and Saudi government agencies, including the transportation sector. "Even worse," Hathaway writes, "...none of the [GGE] 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."

At the same time, the continued proliferation of insecure IoT devices allows the creation of powerful botnets that can launch destructive distributed denial of service (DDoS) attacks to disrupt the operation of critical infrastructure or damage the functioning of internet infrastructure. As Hathaway writes, the occurrence of these damaging events indicates that states are also disregarding the norms by failing to secure their critical infrastructure and by allowing botnet creators to operate inside their borders.

Upholding norms is not just a challenge for cyber security: we are living in an age where other norms that have been established for decades are also being challenged. For example, the Syrian government has violated international norms by using chemical weapons against its citizens, and the UN Security Council has failed to reach an agreement that would punish it for those actions.

Besides the direct harms that result from norm violations — such as the deaths of Syrians by chemical attacks, or the privations Ukrainians experienced when hackers attacked their power centres, leaving them without heat in the winter — there are other, indirect consequences for global security. If the international community's norms are no longer considered reliable or legitimate, states may come to believe that their best option when targeted is to act unilaterally, which could lead to escalation that has serious consequences.

Questions of Enforcement

As the 2015 GGE wrapped up, there were questions about whether its process still offered any utility, but no clear alternatives emerged. When a fifth GGE was convened, it was partly due to "the inability of the international community to identify a different way forward in its discussion of cyber security," James Lewis writes in his essay, "Revitalizing Progress in International Negotiations on Cyber Security." The group began meeting in August 2016, this time with 25 members, and failed to reach a consensus by the time it concluded its final meeting in June 2017.

The biggest question is how the GGE can expect to succeed, given how little heed has been paid to the norms it has already identified. In her essay, Hathaway calls for states to not just enforce the norms, but to speak out when they are violated. Joseph S. Nye, Jr., notes in his essay, "Normative Constraints on Cyber Arms," that the GGE must also raise awareness of its norms and their violations, or else it will be "just a group meeting in the basement of the United Nations."

But if it is determined that the current GGE model is not the best way to proceed, what would replace it? Alternatives could include a more regular diplomatic process, creating a specific UN office, or establishing an open-ended working group. In her essay, "Norms à la Carte," Eneken Tikk warns that replacing the GGE with an alternative forum without first addressing the underlying challenges of a global normative approach is not likely to be any more successful: "If the norms agenda runs dry in one venue, what is the prospect of being able to take the theme forward in another?" Instead, she suggests tackling cyber security issues through bilateral or multilateral agreements, or through technical-level cooperation — among, for example, computer emergency response teams, law enforcement

entities or judicial authorities — that avoids many of the political sensitivities that have contributed to the diplomatic gridlock around cyber security.

When it comes to identifying participants for cyber security talks, a continuing challenge will be achieving the right balance between inclusiveness and effectiveness. The GGE currently represents 25 of the UN's 193 member states. Broadening the process to include as many states as possible may enhance its representativeness, and thus its legitimacy, but it raises "concerns that the negotiating process would be captured by those nations that seek to control content and limit freedom of expression," Lewis writes. Countries that support the established norms will find it difficult, if not impossible, to advance their goals if they are trying to reach a consensus that includes parties who oppose those goals.

On the other hand, smaller countries — including many of the non-aligned — want a seat at the table with the major powers. Currently there is a sense that fora such as the GGE are dominated by major Western countries that have an interest in maintaining the status quo — a status quo that non-aligned, non-Western countries are not convinced has anything to offer them. A more inclusive forum could allow them to feel they are being heard by the leading powers, and give them more of a stake in upholding the norms agreed to in negotiations.

Technical Solutions and Public Awareness

While the long process of building norms plays out, technical and regulatory solutions can help shrink the attack surface that is vulnerable to cyber attacks. For example, in his essay, "How Should We Tackle the Challenges of Today's Cyber Security Environment?" Paul Twomey writes about the need to clean up network infrastructure, by means such as "naming and shaming" internet service providers into better securing their networks, and to build security into core technology and internet architecture by working with standards bodies such as the Internet Engineering Task Force and the Institute of Electrical and Electronics Engineers. The risks posed by vulnerable IoT devices could be mitigated through regulations and standards, or through the introduction of product liability.

But all levels of society play a role in cyber security, from multinational corporations to state governments to private individuals. In her essay, "The Need for a Paradigm Shift on Digital Security," Eileen Donahoe calls for a dramatic change of public consciousness, "such that citizens and consumers embrace responsibility for digital security." She says a global public education campaign — similar to a public health campaign — could help achieve this.

There are limits to this approach, however. As one participant at the March workshop said: "Any system that relies on end-users for security is bound to fail." As such, it might be necessary to shift responsibility for cyber security up the supply chain to ICT companies and manufacturers. And that raises more questions about which venue — or venues — would be appropriate and effective for negotiations with private-sector players.

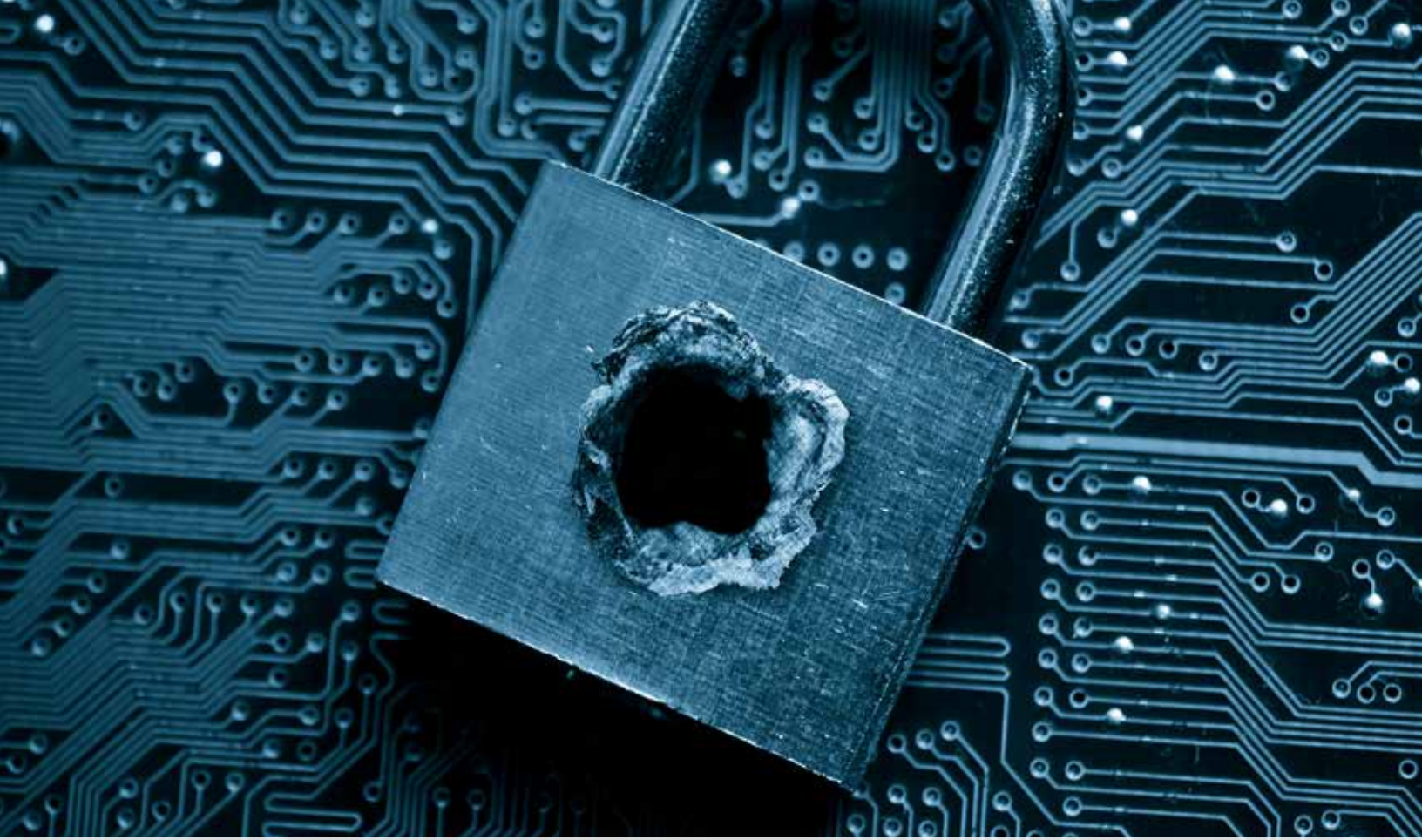
Conclusion

The global stalemate over cyber security may seem intractable, but finding a solution might not be as hopeless as it seems. History has shown that it is not impossible to reach international agreements on sensitive topics at times of tense global relations. After all, the Cold War antagonists were able to avoid nuclear conflict, thanks to arms-control agreements bolstered by norms against the use of nuclear weapons.

But while there is some public concern about cyber security, there has not been the level of widespread public mobilization seen in the climate change or nuclear safety movements, in which domestic political considerations influenced changes in state behaviour. We hope this collection of essays will contribute to wider public understanding of the challenges and opportunities for global cooperation in the cyber security realm.

Fen Osler Hampson is a distinguished fellow and director of CIGI's Global Security & Politics Program, overseeing the research direction of the program and related activities. A fellow of the Royal Society of Canada, he also served as co-director of the Global Commission on Internet Governance and is the co-director of the D-10 Strategy Forum, jointly managed with the Atlantic Council in Washington, DC. He was director of the Norman Paterson School of International Affairs (2002–2012), and continues to serve as Chancellor's Professor at Carleton University in Ottawa. He is the author or co-author of 13 books, most recently *Look Who's Watching: Surveillance, Treachery and Trust Online* (2016), with Eric Jardine.

Michael Sulmeyer is the director of the Cyber Security Project for the Belfer Center for Science and International Affairs at the Harvard Kennedy School. He is also a contributing editor for *Lawfare*. Before arriving at Harvard, he served as the director for Plans and Operations for Cyber Policy in the Office of the United States Secretary of Defense, working closely with the Joint Staff and Cyber Command on efforts to counter malicious cyber activity against US and Department of Defense interests. Previously, he worked on arms control and the maintenance of strategic stability between the United States, Russia and China. As a Marshall Scholar, Sulmeyer received his doctorate in politics from Oxford University, and was awarded the Sir Walter Bagehot Prize for the best dissertation in the field of government and public administration.



When Violating the Agreement Becomes Customary Practice

Melissa Hathaway

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 information and communications technologies (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 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 on Developments in the Field of Information and Telecommunications in the Context of International Security (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 GGE meetings, national experts from member countries began to codify assessments and recommendations into voluntary, non-binding norms. In July 2015, the GGE's member countries — a group representing 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 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 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 offline 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 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 GGE member state — and the rest of the world did not condemn the actions. And while the GGE norm only applies during

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 United Nations 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.

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 the 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 offline, 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 offline (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 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 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 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]

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.

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.

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 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 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 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 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 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 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.

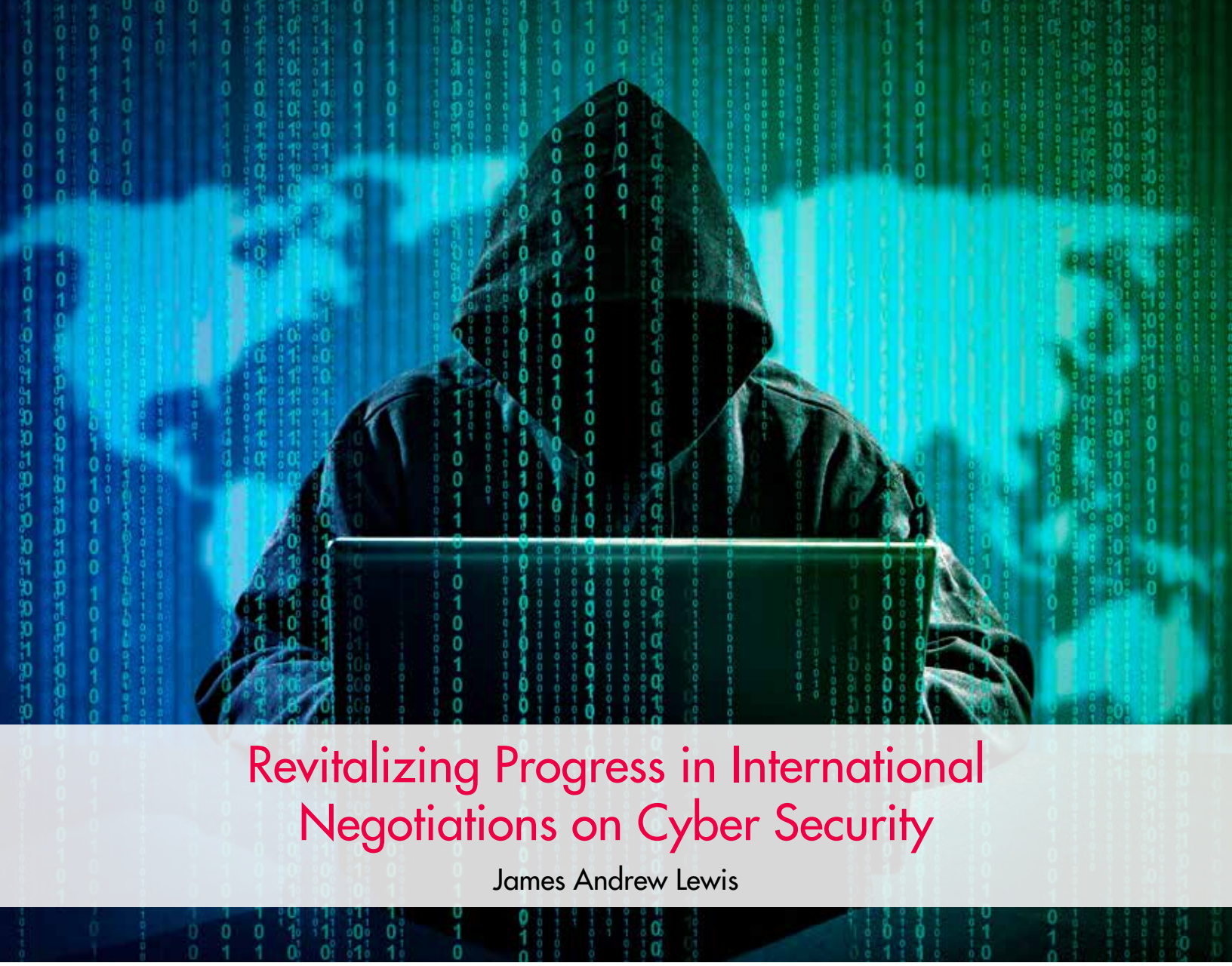
UN. 2001. General Assembly resolution 56/83, *Responsibility of States for Internationally Wrongful Acts*, art. 1-8. A/RES/56/83, Annex. December 12. http://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

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*. 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/.

Melissa Hathaway is a distinguished fellow at CIGI, a senior advisor 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.



Revitalizing Progress in International Negotiations on Cyber Security

James Andrew Lewis

Establishing Cyber Norms

Concern over the risk of cyber attack led Russia in 1998 to propose at the United Nations a treaty to limit the use of cyber attack and cyber weapons. The Russian proposal drew on the experience of arms control and disarmament, but it found little support and was opposed by the United States. During the same period, there were also various proposals from the academic community for some sort of formal international cyber security convention, but many of these proposals were impractical and they too garnered little support.

Agreement on a binding treaty or convention was politically impossible, given the high levels of distrust among major states, but an alternative approach seemed more promising. Research on an approach that used non-binding norms and confidence-building measures (CBMs), leading eventually to an environment in which formal agreement would be possible, created a credible alternative to a treaty. The norms-based approach drew on the experience in non-proliferation regimes, such as the Missile Technology Control Regime, and on CBM precedents from the Treaty on Conventional Forces in Europe and similar political-military arrangements developed during the Cold War.

These concepts helped to shape the 2010 report of the second UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) (UN General Assembly 2010). This report created a negotiating agenda for international cyber security in five recommendations using 94 words, calling for further dialogue among states on norms, "to reduce collective risk and protect critical national and international infrastructure" (ibid., 8); on CBMs, "including exchanges of national views on the use of ICTs [information and communications technologies] in conflict" (ibid.); and for the development of capacity-

building measures (ibid.).

From the work of the 2010 GGE and subsequent GGEs, several general observations can be derived for consideration in developing next steps for negotiation:

- The scope and degree of agreement among states determines the effectiveness and utility of a norm.
- Meaningful norms will touch on the vital interests of states. One implication of this is that states will be cautious in agreeing to any norm of substance and will consider norms through the lens of self-interest.
- Norms that build on the existing framework of law and practice that guides state behaviour in security matters will be most effective, as they will be easier for states to implement.
- Norms discussions do not take place in a vacuum, but are shaped and limited by the larger context for international security.
- There is an unavoidable tension between military stability and universal rights. Existing law and practice reflect accommodations between principles and power that define what is acceptable to sovereign states; agreement on cyber security will need similar accommodations.
- Fundamental differences in national approaches to cyber attack also create unavoidable tensions.
- The foundation for adherence to norms is the application of power, both "soft" and "hard," or the threat of the application of power.
- Process is as important as substance in winning agreement.

The GGE Process after 2017

Looking at the GGE process to date, it has been surprisingly successful. Agreement on norms and CBMs achieved in GGEs in 2013 and 2015 helped to catalyze international interest in cyber security. Between them, the two meetings produced 18 principles for responsible state behaviour in cyberspace.

In particular, the 2013 GGE identified foundational norms that embedded cyber security in the existing framework of international relations and law. These foundational norms are:

- the applicability of the principles of state sovereignty to cyberspace;
- the centrality of international law and the UN Charter for governing state behaviour; and
- the need to respect the rights set forth in the Universal Declaration of Human Rights and other international instruments. (UN General Assembly 2013, paras. 19–21)

The 2015 GGE, with some difficulty, elaborated and expanded the concepts laid out in 2013, with its most significant contribution being a commitment by states not to attack critical infrastructure in ways contrary to their obligation under international humanitarian law (UN General Assembly 2015). However, the larger security environment had deteriorated (and continues to deteriorate), revealing tensions and disputes that constrain progress toward further agreement. At the conclusion of the 2015 GGE, many participants asked if the GGE process had reached the end of its useful life, but deciding what should replace it proved to be difficult. In some respects, the rationale for holding another GGE in 2016-2017 was the inability of the international community to identify a different way forward in its discussion of cyber security.

A GGE is supposedly composed of independent experts whose task is to provide advice to the UN Secretary-General. In the cyber security GGE, however, experts represent their countries and are now usually drawn from foreign ministries. The GGE has evolved into a proxy for negotiation between states, and is an increasingly unsatisfactory substitute for direct, formal negotiation. The GGE format is limiting, since the report of the experts cannot exceed 7,000 words (including transmittal documents and the list of expert names and titles). GGE meetings are closed, leading to charges that secret negotiations among a small group of states deprive other nations of a chance to see their views reflected in the final text. While the cyber security GGE has grown from 15 members, in the first sessions in 2004, to the current 25, there are complaints that this number is too small to be fully representative, and although there are discussions on expanding significantly the number of participants — an idea with some merit, although it complicates the work and would require a longer negotiating schedule — expansion does not resolve the fundamental problems of format and proxy negotiations.

Holding another GGE would be a case of *faute de mieux*, postponing the question on whether it is possible to develop a more formal process. There have been suggestions that it might be time to move these discussions to regular diplomatic processes, such as the Conference on Disarmament (CD), or to a body similar to the UN Office for Outer Space Affairs Committee on the Peaceful Uses of Outer Space, or to create a new and open-ended working group. A change could bring advantages, such as more inclusivity or transparency, but also disadvantages, such as a record of ineffectiveness in reaching agreement — for example, the CD has been unable to agree on any major issue in decades. These proposals raise countervailing concerns that the negotiating process would be captured by those nations that seek to control content and limit freedom of expression.

The impulse for diffusion among UN bodies creates problems for coherence in cyber security negotiations.

Currently, the UN's First Committee (which considers all matters related to disarmament and international security within the scope of the charter) has been able to maintain leadership over cyber security, but other UN bodies, such as the International Telecommunication Union, the UN Economic and Social Council and others, have sought to assert a role in cyber security for themselves. Exactly what expertise a standards body or group focused on development brings to international security is unclear, nor would states be willing to let responsibility for the sensitive issues of conflict and survival fall to bodies that lack responsibility and competence for security. That said, a proxy negotiation using a GGE lacks the political heft to squelch these unhelpful challenges.

Arms Control, Disarmament and Sovereignty

A decision to adhere to a norm reflects three related factors: a state's decision on the norm's utility for its own interests, based on the state's assessment of the likelihood that others will observe it; the value the state places on appearance in the international community; and how well the norm comports with the state's own values. The dynamics of fragmentation in the international system limit the scope for global norms development.

A Western approach to cyber security norms would emphasize constraints on attack and the use of force, defining malicious behaviour as states' use of cyber techniques for force or coercion, and reiterate commitments to human rights and the existing internet governance structure. The non-Western alternative places emphasis on the political effect of information and the belief that content is used against states, to destabilize their regimes. This explains the long-standing Russian assertion that "information is a weapon." The non-Western alternative is accompanied by a desire for a greater recognition of sovereign rights in cyberspace and a greater role for sovereign states in internet governance. Western and non-Western views, while often diametrically opposed, do not preclude all possibility for agreement. The precedent of arms control shows that even opponents can agree on stabilizing measures.

Norms for sovereignty and the use of force by states in cyberspace offer the most promising field for agreement among disparate and competing groups of countries. These two issues are compelling as they directly affect the survival of the state. Sovereignty and warfare are, in some ways, facets of the same issue: the state's ability to remain as an independent actor. Fears about potential diminution of state independence, combined with concerns over what is perceived to be a new and powerful form of attack, have a destabilizing effect on international relations.

Nations share a concern over the possibility of cyber attacks that could damage their political independence, drawing on the experience of the 2007 actions against Estonia (Traynor 2007). They also share concerns over cyber attacks' ability to damage critical infrastructures, as shown by the Stuxnet and Aramco attacks. In these shared concerns, there is ground for agreement. While the nature of offensive cyber operations is poorly understood, it should be possible to build on the progress made by previous GGEs to define general principles for stability and security.

An informal tally of national experts suggests that there are areas where agreement is unlikely — internet governance and human rights, particularly involving freedom of expression and access to information. Previous GGEs simply took governance off the table as an issue, and papered over the difficulties with rights through the frequent invocation of the Universal Declaration of Human Rights and other instruments.

Cyber "terrorism" is also an area where agreement is unlikely. Since there has been no terrorist use of cyber attack and since no terrorist groups possess these capabilities, the discussion of norms on cyber terrorism becomes a debate over online content and of extraterritorial rules to restrict speech. Similarly, some nations would like to extend the Wassenaar Arrangement restrictions on exports of surveillance technologies, but given the difficulties of defining technologies of concern, it will be difficult to achieve meaningful agreement to restrict acquisitions or transfers.

There has been some discussion among Non-Aligned Movement member states of making cyberspace a zone for exclusively peaceful use or a weapons-free zone, building on the precedents of nuclear weapons–free zones, but this concept has several problems. First, it is difficult to verify if a nation is complying with the agreement or not. Weapons-free zones are often a commitment among nations who are incapable of violating it. Second, while those who possess nuclear weapons are bound by implicit norms that constrain use, they are unwilling to renounce these weapons. Third, cyber attack, unlike nuclear weapons, does not threaten mass destruction. Cyber attack does not match the ability of nuclear weapons to kill tens of millions of people and cause immense destruction in the space of minutes. This disparity between nuclear and cyber undercuts incentives for nations to forswear the use of cyber attack.

In only a few instances have states agreed to ban entirely some form of military activity, usually in cases involving weapons that have the potential for disproportionate suffering and mass effect. In other instances, the use of force is governed by rules to avoid unnecessary harm to non-combatants without forbidding military activities. Nuclear weapons are an anomaly. No treaty bans their use; acquisition is only

banned for those nations outside of an initial set of nuclear powers (and this ban has been conspicuously violated several times). Powerful emotions led to the creation of norms on use and acquisition of weapons of mass destruction; the absence of these emotions regarding cyber threats suggests that states will acquire cyber attack capabilities and use them when they believe it is in their interest to do so. This debate — arms control versus disarmament — goes back to the foundation of the United Nations. Badly managed, it can lead to paralysis, but with some skill an agenda can be designed to promote an arms-control approach (that accepts weapons will be built and used, and embeds their use in international humanitarian law) in the near term, while not foreclosing disarmament in the long term.

Similarly, debate over the balance between sovereign rights and universal obligations dates back to the United Nations' creation. Shifts in state attitudes about sovereignty occur slowly, if at all, but there is a discontinuity between Western preferences (especially Western Europe, after the cataclysm of 1939–1945) and non-Western nations, which tend to place a higher value on "traditional" sovereignty. The 1939–1945 experience leads Europe and other Western states to assign a higher potential risk to sovereignty than is the case elsewhere. Russia, which suffered as much as any other country in World War II, opposes the Western view of limited sovereignty as it is motivated by revanchism and a belief that the Western system is hostile to Russian interests. Russia's strong desire to reassert traditional sovereignty finds support in many non-Western nations.

Dispute over sovereignty and universal rights has implications for both the substance of norms and the chances of agreement. There is a fundamental divide in current international relations, between those states who argue for universal values and those who believe that universal values are really "Western," and the derogation of sovereignty that began with the Charter of the United Nations (1945) has gone too far. These nations would prefer to reassert a more traditional view of sovereignty in the relationship between the state and its citizens, one less accommodating of universal values and, as a consequence, in its relations with other states.

Such disagreements are not necessarily fatal to agreement. The most salient example is the UN charter itself, which in article 2.4 forbids member states from using force against another state, without the approval of the Security Council, and in article 51, recognizes their inherent right to use force for self-defence *without* Security Council approval. Underneath this apparent dissonance in the charter is a more complicated discussion of aggression versus defence, but the occasional ambiguity in an agreed text is essential for successful diplomatic negotiation.

Next Steps for Negotiations

Differing national views on the use of force, control of content, governance and international crime shape the space for agreement on cyber security norms and create the landscape for negotiation. There is no consensus among nations on these topics, which creates a challenging environment for continued, meaningful progress on cyber security norms. However, parsing different substantive aspects of the GGE's work, combined with developing a less ad hoc negotiating process, suggests a path forward.

A broad agenda for cyber security negotiations that attempts to address the full range of issues, including crime, intellectual property protection, espionage and military action, may have seemed appropriate in the early days of negotiating but is now impractical. A mature negotiating process would have a different structure than the GGE, with baskets of issues, working groups and a plenary body. This approach would require a greater investment of time and resources than countries, despite the salience of the cyber security issue, are prepared to make. If we discount the constant iteration of banal generalities, cyber security norms remain a tertiary issue for the international community.

The disjointed nature of the global discussion reflects a larger problem with the term "cyber security," which means different things to different communities, who define the problem and any solution in varying ways (usually through the prism of their own experience and expertise) and often assert that they naturally should lead. Dissonance can be reduced by defining the objective of international negotiation: to reach agreement on state responsibilities for peace and security in cyberspace, including states' responsibility for the actions of their citizens, companies or others subject to their laws, and a commitment to ensure that actions in cyberspace do not contravene their international commitments.

The nexus for negotiation lies at the intersection of political rights, sovereignty and use of force, and the primary purpose for cyber security norms is to limit the risk of conflict. Norms can also be used to reaffirm commitments to a free and open internet, but these issues are contentious and perhaps tertiary, and if it is possible to reach agreement on measures to improve security and stability using commitment from states to renounce certain behaviours, without compromising fundamental freedoms, this may be the best outcome now possible. A formal approach to negotiation focused on security would not address all issues or assuage all communities, but it would be the approach most likely to succeed in reducing risk.

Works Cited

Traynor, Ian. 2007. "Russia accused of unleashing cyberwar to disable Estonia." *The Guardian*, May 17. www.theguardian.com/world/2007/may/17/topstories3.russia.

UN. 1945. *Charter of the United Nations*. www.un.org/en/charter-united-nations/.

UN General Assembly. 2010. *Developments in the field of information and telecommunications in the context of international security*. A/65/201. July 30. www.unidir.org/files/medias/pdfs/information-security-2010-doc-2-a-65-201-eng-0-582.pdf.

———. 2013. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/68/98*. June 24. http://undocs.org/A/68/98.

———. 2015. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174. July 22. http://undocs.org/A/70/174.

James Andrew Lewis is a senior vice president at the Center for Strategic and International Studies (CSIS) in Washington, DC. Before joining CSIS, he worked at the Departments of State and Commerce on a range of politico-military and technology issues. He was the adviser for the 2010, 2013 and 2015 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and leads a long-running Track II dialogue on cyber security with the China Institute of Contemporary International Relations. James has authored many publications and is an internationally recognized expert on cyber security who has testified numerous times before Congress and is frequently quoted in the media. He received his Ph.D. from the University of Chicago.

Normative Constraints on Cyber Arms

Joseph S. Nye, Jr.

Introduction

At the February 2017 Munich Security Conference, Dutch Minister of Foreign Affairs Bert Koenders announced the formation of a new non-governmental Global Commission on the Stability of Cyberspace (Government of the Netherlands 2017). The commission will supplement the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), which began in 2010 to develop proposals for norms for responsible state behaviour in cyberspace. The commission will encourage more non-governmental input into the formulation of norms. Normative constraints arise over time from formal agreements among states, the practices of governments and the opinions of epistemic communities of non-governmental experts.

The GGE has issued reports in 2010, 2013 and 2015 that have helped to set the negotiating agenda for cyber security (UN General Assembly 2010; 2013; 2015b). Despite this initial success, the GGE has limitations and the 2017 session failed to issue a consensus report. The participants are technically advisers to the Secretary-General rather than fully empowered national negotiators, and although their number has increased from the original 15 (in the first GGE in 2004) to 25, most nations do not have a voice. But there is a larger question lurking behind the group of experts who meet at the United Nations. Can normative constraints really limit state behaviour?

Arms Control through Consensus Taboo

There is a range of normative constraints on states, ranging from formal treaties to conventional state practice — which create a common law that is allegedly binding on states — to codes of conduct and norms that are widely shared expectations of proper behaviour among a group. In scope, these constraints can vary from global, to plurilateral, to bilateral. Most experts agree that a binding treaty for cyberspace would be politically impossible at this time (although Russia and China have made such proposals at the United Nations; see, for example, UN General Assembly 2015a). What can history tell us about the effectiveness of these normative instruments of policy?

In the decade after Hiroshima, tactical nuclear weapons were widely regarded as "normal," and the US military incorporated nuclear artillery, atomic land mines and nuclear anti-aircraft into its deployed forces. In 1954 and 1955, the chairman of the joint chiefs of staff told President Dwight Eisenhower that the defence of Dien Bien Phu in Vietnam and the defence of offshore islands near Taiwan would require the use of nuclear weapons (although Eisenhower rejected the advice). Over time, this perception changed with the development of a norm of non-use of nuclear weapons, which has added to the cost that a decision maker must consider before taking an action to use them. The Nobel laureate economist Thomas Schelling has said that the development of a norm of non-use of nuclear weapons was one of the most important aspects of arms control over the past 70 years, and it has had an inhibiting effect (Schelling 2006). However, for new nuclear states such as North Korea, one cannot be sure whether the costs of breaking the taboo would be perceived as outweighing the benefits.

Similarly, a consensus taboo developed after World War I about poisons, and the 1925 Geneva Protocol[1] prohibited the use of chemical and biological weapons. Two treaties drafted in the 1970s prohibited the production and stockpiling of such weapons, which meant that there would be a cost associated with not only their use but even their very possession. Verification provisions for the Biological Weapons Convention, which came into force in 1975, are weak (namely, merely reporting to the UN Security Council), and such taboos did not prevent the Soviet Union from cheating by continuing to possess and develop biological weapons in the 1970s. The Chemical Weapons Convention, which came into force in 1997, did not stop either Saddam Hussein or Bashar al-Assad from using chemical weapons against his own citizens, but it did have an effect on the perceptions of costs and benefits of actions, such as the international dismantling of most Syrian weapons in 2014. With 173 states to date[2] having ratified the Biological Weapons Convention, states that wish to develop biological weapons have to do so secretly and illegally and face widespread international condemnation if evidence of their activities leaks.

Focus on Targets, not Weapons

Normative taboos may become relevant in the cyber realm, although the difference between a computer program that is a weapon and one that is a non-weapon depends on intent, and it would be difficult to forbid the design or possession of certain programs, or even their implantation for espionage. In that sense, cyber arms control cannot be like the nuclear arms control that developed during the Cold War, which involved elaborate detailed treaties regarding verification. It would be impossible to reliably prohibit possession of the whole category of cyber weapons, as can be done with physical weapons.

A more fruitful approach to normative controls on cyber arms is to focus a taboo not against *weapons* but against *targets*. The United States has promoted the view that the internationally recognized law of armed conflict (LOAC), or international humanitarian law, which prohibits deliberate attacks on civilians, apply in cyber space. Accordingly, the United States has proposed, not a pledge of "no first use" of cyber weapons, but a pledge of *no* use of cyber instruments against civilian facilities in peacetime.

This no-use approach to norms was adopted by the GGE. The taboo would be reinforced by confidence-building measures such as promises of forensic assistance and non-interference with the workings of computer security incident response teams. The GGE report of July 2015 focused on restraint on attacks on certain civilian targets rather than on proscription of particular code (UN General Assembly 2015b). At the 2015 summit between American President Barack Obama and China's President Xi Jinping, the two leaders agreed to set up an expert commission to study the GGE proposal. Subsequently, the GGE report was endorsed by the leaders of the Group of Twenty and referred to the UN General Assembly. On the other hand, the attack on the Ukrainian power system occurred in December 2015, shortly after the submission of the GGE report, and, in 2016, Russia did not include the election process in the United States as critical civilian infrastructure. At this point, the development of normative controls on cyber arms remains a slow and incomplete process.

In general, the multilateralization of norms helps raise the reputational costs of bad behaviour. It is worthy of note that the Missile Technology Control Regime,

1 In full, the Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare.

2 See www.un.org/disarmament/geneva/bwc/membership/.

an informal voluntary association of countries acting to limit trade in unmanned delivery systems that can deliver weapons of mass destruction, and the Proliferation Security Initiative, a multinational response to the challenge posed by the threat of the proliferation of weapons of mass destruction, began as voluntary measures and gathered momentum, members and normative strength over time. In the cyber realm as in other domains, theorists have hypothesized that norms have a life cycle starting with norm entrepreneurs, progressing to tipping points and cascades and, finally, internalization into costs that deter actions (Finnemore and Sikkink 1998). Today, the world is largely at the first stage, perhaps entering the second.

There is a range of views about the next steps for the GGE process after its failure to issue a consensus report in 2017. One group of states advocates norm development in a plurilateral format of like-minded states. Others argue that the GGE should continue in the UN context with an expanded membership. At a panel at the 2017 Munich Security Conference the current GGE chair had argued that the group should not try to rewrite the 2015 report but should instead say more about the steps that states should take in peacetime. Two new norms might be included on data integrity and maintenance of the internet. And he believed that there should be more discussion of confidence-building measures and capacity building. In his view, the "elephant in the room" was whether states would implement what had been agreed.

If the GGE is ever to be more than just a group meeting in the basement of the United Nations, states must raise awareness of the norms to the point where they affect state behaviour. It is noteworthy that the Ukrainian grid disruption in December 2015 was not flagged and debated as contrary to the GGE report. At the 2017 Munich Security Conference, a representative of a small country argued that international law was crucial to small states without power, and made the case for more attention to the *Tallinn Manual 2.0*, which examines the applicability of the laws of armed conflict in cyberspace (Schmitt 2017), but Russia and China remain cautious about this approach. The representative of a major power said the GGE should dig deeper on questions such as what is meant by "civilian processes" (for example, if an electric grid supports both a hospital and a military facility, is it part of a civilian process?). Another representative also urged more attention to capacity building. A UN undersecretary argued that the norm development process had to be broadened to include more countries to increase its legitimacy among the 193 UN members, and should relate cyber to other issues, such as arms control in space and terrorism. Then the 193 members of the UN should debate the report and task another GGE to examine specific areas. This might enhance legitimacy, but also increase unwieldiness.

Conclusion

The GGE process reflects the positions of the states that nominate the experts and their strong views on state sovereignty. Certain normative issues are not discussed. The questions of contents and human rights are finessed by saying that all states agreed to the Universal Declaration of Human Rights, although they interpret and implement it in different ways. Further progress on such subjects would probably be limited to plurilateral discussions among like-minded states rather than universal agreements. Other norms that may be ripe for discussions outside the GGE process could include a protected status for the core functions of the internet; supply chain standards and liability for the Internet of Things; treatment of election processes as protected infrastructure; and, more broadly, norms for sub-LOAC issues, such as crime and information warfare. All of these are among the topics that may be considered by the new Dutch-sponsored commission.

Works Cited

Finnemore, Martha and Kathryn Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization* 52 (4): 887–917.

Government of the Netherlands. 2017. "Minister Koenders launches international cyberspace commission." News item, February 18. www.government.nl/latest/news/2017/02/18/minister-koenders-launches-international-cyberspace-commission.

Schelling, Thomas. 2006. "An Astonishing Sixty Years: The Legacy of Hiroshima (The Nobel Lecture)." In *Micromotives and Macrobehavior*, 245–62. New York, NY: Norton.

Schmitt, Michael N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge, UK: Cambridge University Press.

UN General Assembly. 2010. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/65/201. July 20. www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf.

———. 2013. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/68/98*. June 24. http://undocs.org/A/68/98.

———. 2015a. *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*. A/69/723. January 13. http://undocs.org/A/69/723.

———. 2015b. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174. July 22. http://undocs.org/A/70/174.

Joseph S. Nye, Jr., is a university distinguished service professor and former dean of the John F. Kennedy School of Government at Harvard University. He has served as assistant secretary of defense for International Security Affairs; chair of the National Intelligence Council; and deputy under the secretary of state for Security Assistance, Science and Technology.

Norms à la Carte

Eneken Tikk

Introduction

Since 1998, many small battles to clarify what rules apply in cyberspace have been fought under the umbrella of the UN General Assembly's First Committee, which deals with disarmament, global challenges and threats to peace that affect the international community.

The First Committee process started with a Russian-sponsored resolution (UN General Assembly 1999), which, over the past decade, has come to be supported by more than 100 nations. Under the resolution, 64 countries have used the opportunity to share their national positions on the issue of information and communications technologies (ICTs) as a threat to international peace and security, and to propose remedies to address the threat.

In 2004, the first UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) was established, to study existing and potential threats in the sphere of information security and possible cooperative measures to address them. Meeting in a series of sessions every few years, the GGEs have provided a controlled environment in which leading cyber powers can test each other's red lines and feel out the rest of the international community on the issues. Thirty-eight states, in differing configurations, have participated in the five GGEs, resulting in three reports that have built an ambitious agenda of "cyber norms and offered a set of voluntary, non-binding norms for States to consider, in addition to highlighting rules of international law that can be applied to issues pertaining to State uses of ICTs."[1] It was widely anticipated that the 2016/2017 GGE would be able to offer concrete guidelines on the implementation of the 2015 norms.

1 UN General Assembly (2010, 2013, 2015); see also Adamson (2017) for an excellent overview of developments during the UN GGE process.

However, the seemingly lively process and alleged breakthroughs[2] in 2013 and 2015 do not seem to adequately satisfy the international community. As a closed and exclusive working format, the GGE cannot accommodate all countries willing to be part of the deliberations. It cannot produce a compromise between the many and diverse world views, capacities and priorities at a time of governments' increasing (self-) awareness when it comes to their ICT issues. The GGE reports do not change the fundamental differences between the great cyber powers. They do not, as such, make much practical difference in preventing or reducing cyber incidents. Especially after the lack of consensus among 2016/2017 GGE experts, time is ripe to critically think about actual common ground and real priorities in the norms discourse.[3]

Flawed Format or Uninformed Expectations?

The many criticisms[4] about the GGE, however, are based on different assumptions about its purpose and format. Regarding the GGE reports as an assault on international law — by way of not enough, too much or inaccurate reference to it — misses the political nature of the GGE format and downplays the significance of the fragile legal consensus it has been able to forge. The sentences within GGE reports are not precision tools. They are not shared attitudes. At best, they confirm that the international community is not falling back from recommendations it has considered useful and applicable in other fields of issues.

Those who attack the GGE for the lack of action[5] resulting from its guidance ignore its political and legal reality — the GGE is not a tribunal or an international aid program. It is a group of governmental experts, most of them diplomats and policy decision makers, many with backgrounds in the area of disarmament, holding their governments' fronts in fundamental questions and devising strategies to push the front whenever they see an opening. What the GGE offers is recommendations, and only that. Moreover, these recommendations are limited to dealing only with threats to international security, as the work of the GGE falls under the mandate of the First Committee.

The Question of Alternatives

In light of these critiques and discontent, the question of alternatives is key. If the norms agenda runs dry in one venue, what is the prospect of being able to take the theme forward in another? If the GGE is not up to the task of settling norms of responsible behaviour in state use of ICTs, whose task shall it be? Is there a need for a venue that falls outside the purview of the First Committee, so as not to limit discussions only to ICT use that could threaten international security?

These questions do not have one possible or satisfactory answer. For countries that prefer inclusion, and for the least-developed states that regard international conventions as the playbook, the Russian open-treaty discussion proposal[6] may seem attractive. Yet, in a field as contested and diverse as cyber security, the prospect of achieving meaningful binding consensus is slight. As opponents have explained, it would entail a lengthy process, with unclear scope and focus and involving diverse and strong interest groups (Starks 2015; Lyngaas 2015). These factors, aligned with the overall declining trend of open multilateral agreements, do not make negotiations a viable option.

Those who long for more legal clarity may be attracted by a Sixth Committee process, that is, handing it over to a dedicated legal consultant group, or reactions from the International Court of Justice or the International Law Commission. However, a theme as complex and politically loaded as international cyber security may not find much useful common ground there. For those who seek an open-ended venue, the UN Conference of Disarmament would be an option; however, it is known for not being able to agree on its agenda, let alone to produce anything tangible or implementable (Ki-moon 2011; Meyer 2006). For those seeking a Nobel Peace Prize, the Convention on Conventional Weapons (CWC) offers avenues to pursue it.[7]

2 The United States and other like-minded states referred to the 2013 report (UN General Assembly 2013) as a breakthrough in its agreement that existing international law is applicable to states' uses of ICTs — thus, these states claim, achieving a turn away from the 1998 proposition that a new legal instrument was needed to address ICT-related threats to international peace and security. At the same time, Russia holds the view that this conclusion does not rule out the need for new instruments. The 2015 report (UN General Assembly 2015) was praised for offering a set of new, voluntary norms to contribute to international cyber security. However, critics have pointed out that these norms have no more than recommendation status and have not been socialized within the international community. Some authors go so far as to say that the GGE norms have no impact on international practice whatsoever (see Melissa Hathaway's essay in this special report).

3 See account by Russian news agency Tass (2017) and remarks of Michele Markoff, the US expert of the GGE (2017).

4 See Hathaway's essay in this special report; see also Maurer (2016); Valeriano and Pytlak (2016); Schmitt and Vihul (2017).

5 See Hathaway's essay in this special report.

6 See UN General Assembly (2011) and the original resolution, since revised every year (Ministry of Foreign Affairs of the Russian Federation 2011).

7 See, for instance, the campaign to stop killer robots (fully autonomous weapons) by creating an additional protocol within the CWC: www.stopkillerrobots.org/.

For those who wonder why an international security issue as burning as cyber security has not been picked up in the Security Council, the question to consider is what the shared endgame of the Permanent Five — China, France, Russia, the United Kingdom and the United States — might be. That is, how much appetite is there to come up with any binding agreement of any sort?

Mixed and Modular Approaches

Given these near-dead ends, real issues might best be taken up bilaterally or multilaterally between countries and entities that have mutually agreed priorities and issues. Given political sensitivities, technical-level cooperation — be it between computer emergency response teams, law enforcement entities or judicial authorities — is likely more efficient than politicized formats.

For those who want actual change in behaviour, international processes offer few effective remedies. Cyber threats are not a force of nature. With self-inflicted vulnerabilities and interdependencies, governments across the world are looking no further than making their security stand up to their economic and societal interests and ambitions — approaches observable in the activities of the European Union (single market), North Atlantic Treaty Organization (shared standards of cyber defence), Shanghai Cooperation Organisation (common normative ground), Organization of American States (cooperation among relatively homogeneous South American countries), African Union (countering cyber crime) and many other regional and specialized organizations.

Answers to real cyber security issues, and further cues for responsible behaviour in cyberspace, are to be found in what states say and do. National cyber security strategies, policies, laws, court rulings and best practices in policing individual states' jurisdictions will inform international normative coalitions, expectations of behaviour and possible further norms processes. Occasional reactions to other countries' behaviour is equally indicative of accepted and contested norms. Next steps in the international norms development may also come from non-State actors. Notable examples are Microsoft's campaign for a Digital Geneva Convention seeks to commit governments to protecting civilians from nation-state attacks in times of peace (Smith 2017) and Elon Musk's call to address the issue of lethal autonomous weapons.[8]

Possible (and not mutually exclusive) moves in international norms discussion include a strategic pause in global talks, focus on national responsibility and implementation, bilateral consensus building and more emphasis on structured academic research. Any successful intergovernmental process has to be modular to produce targeted and feasible norms, effective means of their implementation and long-term commitment. An "à la carte" approach would enable willing countries to contribute according to their strategic ambitions, political priorities and available, realistic capabilities. Such contributions do not need to be restricted to, or perhaps even start with, coining new norms. They may take the form of enforcing compliance with existing rules by way of countermeasures or other forms of self-help.

8 See "An Open Letter to the United Nations Convention on Certain Conventional Weapons," www.cse.unsw.edu.au/~tw/ciair/open.pdf; see also Holley (2017).

Works Cited

Adamson, Liisi. 2017. "Cumulative Recommendations in the UN GGE Reports (2010–2015)." Tartu, Estonia: Cyber Policy Institute. Available through The Hague Program for Cyber Norms, Insitute of Security and Global Affairs, Leiden University, the Netherlands. www.universiteitleiden.nl/binaries/content/assets/governance-and-global-affairs/isga/cumulative-recommendations-of-un-gge-reports.pdf.

Holley, Peter. 2017. "Elon Musk calls for ban on killer robots before 'weapons of terror' are unleashed." *The Washington Post*, August 21. www.washingtonpost.com/news/innovations/wp/2017/08/21/elon-musk-calls-for-ban-on-killer-robots-before-weapons-of-terror-are-unleashed/?hpid=hp_hp-more-top-stories_elon-robots-1155am%3Ahomepage%2Fstory&utm_term=.a88479aa1522.

Ki-moon, Ban. 2011. "Dysfunctional Disarmament." *Project Syndicate,* May 18. www.project-syndicate.org/commentary/dysfunctional-disarmament.

Lyngaas, Sean. 2015. "Cyber treaty not in the cards.'' *FCW*, April 27. https://fcw.com/articles/2015/04/27/cyber-treaty.aspx.

Markoff, Michele. 2017. "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.'' US Mission to the United Nations, June 23. https://usun.state.gov/remarks/7880.

Maurer, Tim. 2016. "UN Body Considers International Cyber Norms." *IHS Jane's Intelligence Review,* December 1. http://carnegieendowment.org/2016/12/01/un-body-considers-international-cyber-norms-pub-66510.

Meyer, Paul. 2006. "The Conference on Disarmament: Getting Back to Business." *Arms Control Association*, December 1. www.armscontrol.org/print/2285.

Ministry of Foreign Affairs of the Russian Federation. 2011. Convention on International Information Security (Concept). September 22. www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.

Schmitt, Michael and Liis Vihul. 2017. "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms." *JustSecurity* (blog), June 30. www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

Smith, Brad. 2017. "The Need for a Digital Geneva Convention." Keynote address at the RSA Conference, San Francisco, February 14. https://mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf.

Starks, Tim. 2015. "The State Department's Weary Soldier in America's Cyber War.'' *Foreign Policy*, May 13. http://foreignpolicy.com/2015/05/13/the-state-departments-weary-soldier-in-americas-cyber-war-christopher-painter/.

Tass. 2017. "Some countries seek chaos in cyber space, Russian presidential envoy says.'' Tass, July 11. http://tass.com/politics/955734.

UN General Assembly. 1999. *Developments in the field of information and telecommunications in the context of international security*. A/RES/53/70. January 4. http://undocs.org/A/RES/53/70.

———. 2010. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/65/201. July 20. www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf.

———. 2011. *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*. A/66/359. September 14. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf?OpenElement.

———. 2013. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/68/98*. June 24. http://undocs.org/A/68/98.

———. 2015. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174. July 22. http://undocs.org/A/70/174.

Valeriano, Brandon and Allison Pytlak. 2016. "Cyber Security and the Coming Failure of the UN's Group of Governmental Experts.'' *Foreign Policy & Defense* (blog), August 31. https://niskanencenter.org/blog/cyber-security-coming-failure-uns-group-governmental-experts/.

Eneken Tikk is a senior fellow at Leiden University's Institute of Security and Global Affairs. Her work focuses on the development and implementation of law and policy pertaining to uses of information and communications technologies. Eneken has served as adviser to the Estonian Expert in the United Nations GGE (2012-2013, 2014-2015 and 2016-2017). She teaches international cyber security law and policy at the University of Tartu, Estonia.

How Should We Tackle the Challenges of Today's Cyber Security Environment?

Paul Twomey

Introduction

The challenges that cyberspace presents to the international community have evolved dramatically since the initiation in 2013 of the United Nations' Group of Governmental Experts (GGE) process[1] and the international cyber norms agenda. This growth is a product of not only the expanded range of threats but also the accompanying recognition in the international community's discussion that not all threats originate from the actions of state actors.

Further, the community has come to recognize that the security paradigm often applied to the cyber challenge could be usefully complemented by taking an approach closer to that of public health, by broadening and making more transparent the roles of all layers of the internet ecosystem in addressing causes of vulnerabilities and infection — particularly in addressing market failures.

This essay outlines five areas for action by the governments and the information technologies sector, explored below.

International Cyber Norms

First, within the context of the international cyber norms agenda, the energy and purpose for further exploration of possible norms may be fading, at least for the group of liberal democracies and fellow interested countries ("like-minded countries"). The perceived non-compliant behaviour of some other parties to the 2015 norms agreement means that for the like-minded group, there is a need to regroup and build a consensus

1 This UN-mandated group's full name is the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

among themselves as to what they want to achieve, considering the following questions.

- If the norms negotiated to date are to be respected, what should the consequences be for breaking the norms, and how will those consequences be coordinated?
- What approach should the like-minded countries take to the future of the GGE process?
- If "swing states" are starting to see the status quo not serving their interests, what can be done to address these concerns? This is particularly the case for African states where the sort of technology influence asymmetry outlined in the final paragraph of this essay should be addressed.
- What sort of open approach and process will allow other countries to join over time?
- Where should this consensus be built?
- Who should participate, and who should lead in bringing the group together?

Network Infrastructure

A second priority area is the need to clean up the network infrastructure ecosystem to limit its capacity to be used for malware distribution and attack vectors. Market failures are resulting in network operators and device manufacturers not being incentivized to ensure improved cyber security practices in their operations. The result is a large global base of vulnerable computers, modems/routers and Internet of Things (IoT) devices that can be manipulated by cybercriminals.

Distributed denial of service (DDoS) attacks exhaust the available resources of computers by overwhelming them with data. There are two primary causes of this flooding on the internet: reflectors, remote applications that amplify and reflect small amounts of data from many individual devices into large data flows directed to specific servers, and spoofing of addresses, which hides or forges the identity of the senders. The DDoS vulnerability shows the implications of internet service providers (ISPs) and network operators not taking care to ensure their modems, routers and other systems are deployed or maintained properly. Even failing to maintain best practices in managing just four risk indicators — OpenDNS, the Network Time Protocol, the Simple Network Management Protocol and the Simple Service Discovery Protocol — could mean that an ISP could pollute the entire network, if these risks were exploited by botnet and DDoS exploiters. But the pollution impact is greater to the users as a whole than to the operators, who individually do not have an economic incentive to clean up their own networks. Data from the non-profit CyberGreen Institute shows that the potential attack capacity of existing polluted network devices is five times larger than the biggest DDoS attacks to date. The failure to address this negative externality will place government agencies, enterprises, financial institutions and consumers at even greater risk than they face today.

Similarly, the manufacturers of components and end devices for the burgeoning IoT market are driven by costs and the search for new features rather than by the costly process of designing security into the products. Because many products incorporating IoT devices are not replaced on a short-term basis (think manufacturing plants, cars, refrigerators and so on), it is not sufficient to rely on the market to reward suppliers who do improve security swiftly over time, such as mobile phone and laptop manufacturers.

Individual governments, especially leading states, should address market failures through:

- their communications regulators or computer emergency response teams, using public data (such as the curated and validated statistics provided by the non-profit CyberGreen Institute[2]) to "name and shame" ISPs about the status of their network deployments and encourage adoption of technical community norms for routing security; and
- by promoting transparency in the IoT component supply chain and patching for IoT devices, and by coordinating the careful introduction of accountability into the software/IoT value chain, after multi-stakeholder input.

Cybercrime

Cybercrime is the third area demanding focused attention. Many citizens are more concerned about predictability of everyday use of the internet than about periods of crisis or policy around freedom of choice. In this sense, citizens are more likely to care about the actions of non-state actors, especially cybercriminals. Some consider that citizens would like to see states focus more on countering cybercriminals. Despite tools such as the Budapest Convention, the difficulty of effecting cross-border investigations and prosecutions, especially involving suspects from Asia and Eastern Europe, is thwarting this aim. Considering the seemingly modest success of the 2015 US-Chinese Heads of Government agreement concerning cyber economic espionage, perhaps the best way to address the cybercriminal issues will require similar engagement of heads of government.

2 See www.cybergreen.net/.

Core Technology

Fourth, the international community needs to recognize that the current core technology is not serving security outcomes well and that the direction of technological evolution needs to change to incorporate security in its design. This is particularly the case in the deployment of the IoT. But there is also a need to look for higher-level security approaches to internet and software design to achieve a multiplicative impact. These issues demand specific and concerted new work by the existing standards bodies — the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), the World Wide Web Consortium (W3C) and others — that moves beyond the preoccupation with encryption to bigger-impact architectural and code-development approaches. At the same time, the technical community (and democratic governments) need to ensure that the work does not inadvertently result in a future network built for control and human rights abuse.

Developing Countries

Finally, the international community needs to recognize that developing and emerging countries are expressing a fear that they are being subjected to the risks generated by the leading economies' use of networked technologies without having the levers to alleviate these risks. To give one example: Sub-Saharan African countries may be suffering from the criminal exploitation of vulnerabilities in the Windows operating system but they have no recourse to Microsoft or access to its facilities and relevant staff to help address this. The problem set expands with the creation of cyber weapons. The information and communications technology industry (and the like-minded governments) need to practically engage these countries to ensure the industry's long-term stability, and to counter any risk of a developing-country push in UN institutions for a significant change to the international regulatory framework. Empowering developing countries with such facts as outlined in the "Network Infrastructure" section above about specific things they can do to help improve the cyber health of their own ISP networks could be an effective way to persuade these countries that the status quo/like-minded countries can help deliver to their needs.

Paul Twomey is a distinguished fellow at CIGI. He is a co-founder of Stash, the secure digital storage and messaging company.

Paul is also a founding figure of the Internet Corporation for Assigned Names and Numbers (ICANN), the international organization that coordinates many of the key functions of the global internet. After four years as chair of its Governmental Advisory Committee (charged with conveying observations and concerns of its national government members to the ICANN board and to other ICANN constituencies), Paul served from 2003 to 2010 as ICANN's president and CEO.

Paul founded Argo P@cific, a cyber security consulting firm for governments and Fortune 500 companies worldwide. He was formerly the CEO of the Australian government's National Office for the Information Economy and the federal government's special adviser for the information economy and technology. Paul was the executive general manager of the Australian Trade Commission from 1994 to 1997, and a senior consultant with McKinsey & Company.

A recognized thought leader, Paul is also the chairman of CyberGreen Institute, a non-profit organization dedicated to promoting a public health approach to improving global cyber safety; a commissioner of the Global Commission on Internet Governance; and a member of the Global Information Infrastructure Commission. He is an advisory board member of *Electronic Markets — The International Journal on Networked Business* and has also served since 2007 on the board of the Atlantic Council of the United States. He is founding chair of the Global Agenda Council on the Future of the Internet, World Economic Forum, 2008-2009. Paul holds a Ph.D. from the University of Cambridge.

The Need for a Paradigm Shift on Digital Security

Eileen Donahoe

Introduction

The single-most crucial cyber security issue facing the international governance community is systemic, society-wide digital insecurity brought on by the digitization of society and global connectivity. This is not merely one issue — it is *the* issue. Citizens, consumers, businesses — even government agencies — seem powerless to protect themselves as their confidential, proprietary or personal digital communications and data are hacked. The international community must not stand by as a "new normal" develops — an environment in which daily data breaches, digital identity theft, ransomware attacks and weaponization of information are passively accepted. We need a society-wide paradigm shift on digital security for everyone and everything. This paradigm shift must start with the recognition that in the global digital ecosystem, everything we say and do is captured in digital form. As we move rapidly toward the Internet of Things (IoT), the gamut of physical objects, from doorbells and toothbrushes to surgical instruments and aircraft, are being digitally connected. Connectivity of everything, combined with the transborder mode of operation of the internet, means that instantaneous extraterritorial cyber reach is available to criminals, governments, terrorists and anarchists alike.

This combination of features obviously makes us — states and ordinary citizens alike — vulnerable in new ways. National security experts, who traditionally focused on norms to constrain states' offensive use of weapons, have not figured out how to provide security in this interconnected, digitized environment — where anyone, anywhere, can attack anyone or anything, anywhere else.

New thinking on targets, relevant actors and responsibilities is warranted. A new paradigm on digital and cyber security would entail four elements:

- a broadened perspective on what constitutes an important target;
- a greater focus on non-state actors;
- a shift of focus from offence to defence; and
- an extension of responsibility for security to everyone.

The following sections consider each element in turn.

What Constitutes an Important Target?

A new paradigm on cyber security must start with the recognition that hits on small targets, from baby monitors[1] to Gmail accounts, can have great impact. Admittedly, given the existential threat posed by nuclear weapons, we must heed the dire warnings by former US Secretary of Defense William Perry and others, about the urgent responsibility to prevent any type of cyber-to-kinetic attack involving nuclear weapons or facilities (Harris and Bender 2017). Protection of all critical military and civilian infrastructure from cyber attack, including core internet infrastructure, must also be prioritized. But interconnected people, things and data can also function as avenues of attacks on critical infrastructure, over and above the harm they may themselves experience through cyber attacks.

In this regard, the compromise of the Democratic National Committee headquarters' computer and email systems, and a phishing attack of the Gmail account of Hillary Clinton's campaign manager, John Podesta, during the 2016 US presidential election brought home the realization that digital security for information, data, services and devices is as important as digital security for critical infrastructure (Waddell 2016). It served as a reminder that democratic processes should count as critical infrastructure to be protected and that weaponized private communications can become a potent arsenal with which to attack a democratic society.

The digital security paradigm must recognize the interrelation between security for individuals, personal devices, confidential communications and national security. What might whole-society digital security look like in practice? As a starting place, to protect citizens' and consumers' personal communications and data, government resistance to ubiquitous encryption, because it makes surveillance more difficult, must be addressed. To protect IoT and smart devices, security standards combined with liability frameworks for failures in meeting those standards must be developed. For infrastructure, emphasis on systemic resilience must become the design priority.

The bottom line: in an interconnected ecosystem, cherry-picking a few things for protection is not an effective approach to security: *all* interconnected digital communications, devices, data, networks must be kept secure, along with critical infrastructure that could be targeted through these other vectors of cyber attack.

Greater Focus on Non-state Actors

The second element of the paradigm shift requires looking beyond states to non-state actors as a primary adversary. A range of differentially motivated non-state actors engage in cyber attacks, from lone criminals to terrorists and from anarchists to digital mafia gangs. One characteristic they share: none of them follows norms, whether acting as state proxies or on their own. The international governance community needs to deal with the reality that it does not have normative sway over many dangerous actors in cyberspace.

Even holding states accountable for actions of their non-state proxies is more difficult than it sounds, both in establishing attribution convincingly, and in crafting appropriate, proportional responses. It has been relatively easy for states to deflect responsibility for hacks committed by their proxies, and relatively difficult to identify effective cyber responses that won't "spiral out of control" and have unintended effects (Zakaria 2017). Investment in creative strategies to defend against non-state actors should be given higher priority.

Shift Focus from Offence to Defence

Beyond focusing on norms that constrain offence, states must put greater focus on their responsibilities to provide adequate defence. Doing so would include deploying state-of-the-art digital security across government agencies, as well as developing regulatory frameworks to motivate private-sector actors to optimize their systems and networks for consumer and citizen security.

Up until now, national security and law enforcement actors have prioritized the collection of digital information as a primary way to keep us safe. But governments generally have failed in their obligation to keep information and data secure. When top-secret security clearance records of the most powerful country in the world can be hacked (see Adams 2016), it is a good indicator that digital security has not been taken seriously enough.

1 Baby monitors were among the networked household items used by hackers in a major distributed denial of service attack in the United States in October 2016 (Perlroth 2016).

A core aspect of a digital security paradigm shift would be to see defence as the new offence: the idea being that having the capacity to thwart an attack, and the resilience to withstand an attack, is the best way to demotivate those who would attack. In effect, capacity to thwart and resilience to withstand a cyber attack could together become the new deterrence.

Expand Responsibility for Security to Everyone

Finally, we need a dramatic cultural shift so that responsibility for digital security runs throughout the entire society. This shift will require a change from the view that government alone bears responsibility for keeping citizens safe.

The private sector owns, operates and secures much of the critical internet infrastructure, and government should not undermine the security of this infrastructure, even "in the name of security." In addition, producers of IoT products must internalize the costs of security for consumers and be held liable for negligent design of products that could have been built more securely.

Finally, public consciousness needs to change dramatically, such that citizens and consumers embrace responsibility for digital security. A massive global public education campaign must be developed — similar to an urgent, sustained public health campaign — to educate citizens about digital hygiene and their own role in protecting themselves. If John Podesta didn't understand the importance of two-factor authentication[2] for his Gmail account, it is hard to expect such awareness in others. This single digital security failure had historic consequences for national and international security. This episode, it is to be hoped, will serve as a catalyst for a society-wide paradigm shift on digital security.

2 See Appspicket.com (2017); Waddell (2016).

Works Cited

Adams, Michael. 2016. "Why the OPM Hack Is Far Worse Than You Imagine." *Lawfare* (blog), March 11. www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.

Appspicket.com. 2017. "Two Factor Authentication and US Presidential Elections." *Appspicket* (blog), February 17. https://appspicket.com/two-factor-authentication-and-us-presidential-elections/.

Harris, John F. and Bryan Bender. 2017. "Bill Perry Is Terrified. Why Aren't You?" *Politico*, January 6. www.politico.com/magazine/story/2017/01/william-perry-nuclear-weapons-proliferation-214604.

Perlroth, Nicole. 2016. "Hackers Used New Weapons to Disrupt Major Websites Across U.S." *The New York Times*, October 22. www.nytimes.com/2016/10/22/business/internet-problems-attack.html.

Waddell, Kaveh. 2016. "Why Some People Think a Typo Cost Clinton the Election." *The Atlantic*, December 13. www.theatlantic.com/technology/archive/2016/12/why-some-people-think-a-typo-cost-clinton-the-election/510572/.

Zakaria, Fareed. 2017. "Deterrence Strategy Unfit for Cyber Weapons Proliferation." *Newsmax*, March 10. www.newsmax.com/FareedZakaria/wikileaks-cyber-warfare-trump/2017/03/10/id/778026/.

Eileen Donahoe is a distinguished fellow at CIGI, where she focuses on internet governance, global digital policy, international human rights and cyber security. She is executive director of the Global Digital Policy Incubator and adjunct professor at the Center for Democracy, Development, and the Rule of Law at Stanford University.

Previously, she served as the first US Ambassador to the United Nations Human Rights Council in Geneva, and as director of global affairs at Human Rights Watch, where she represented the organization worldwide on human rights foreign policy. In her earlier career, Eileen was a technology litigator at Fenwick & West in Silicon Valley.

She holds a B.A. from Dartmouth, an M.T.S. from Harvard, an M.A. in East Asian studies from Stanford, a J.D. from Stanford Law School and a Ph.D. in ethics and social theory from the Graduate Theological Union at the University of California, Berkeley. She is a member of the Council on Foreign Relations.

Acknowledgements

The “Getting beyond Norms” workshop in March 2017 in Cambridge and this publication owe a great deal to the support of CIGI Research Associate Stephanie MacLellan, who provided administrative and editorial assistance to the project from its beginning through to final publication.

Centre for International
Governance Innovation

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