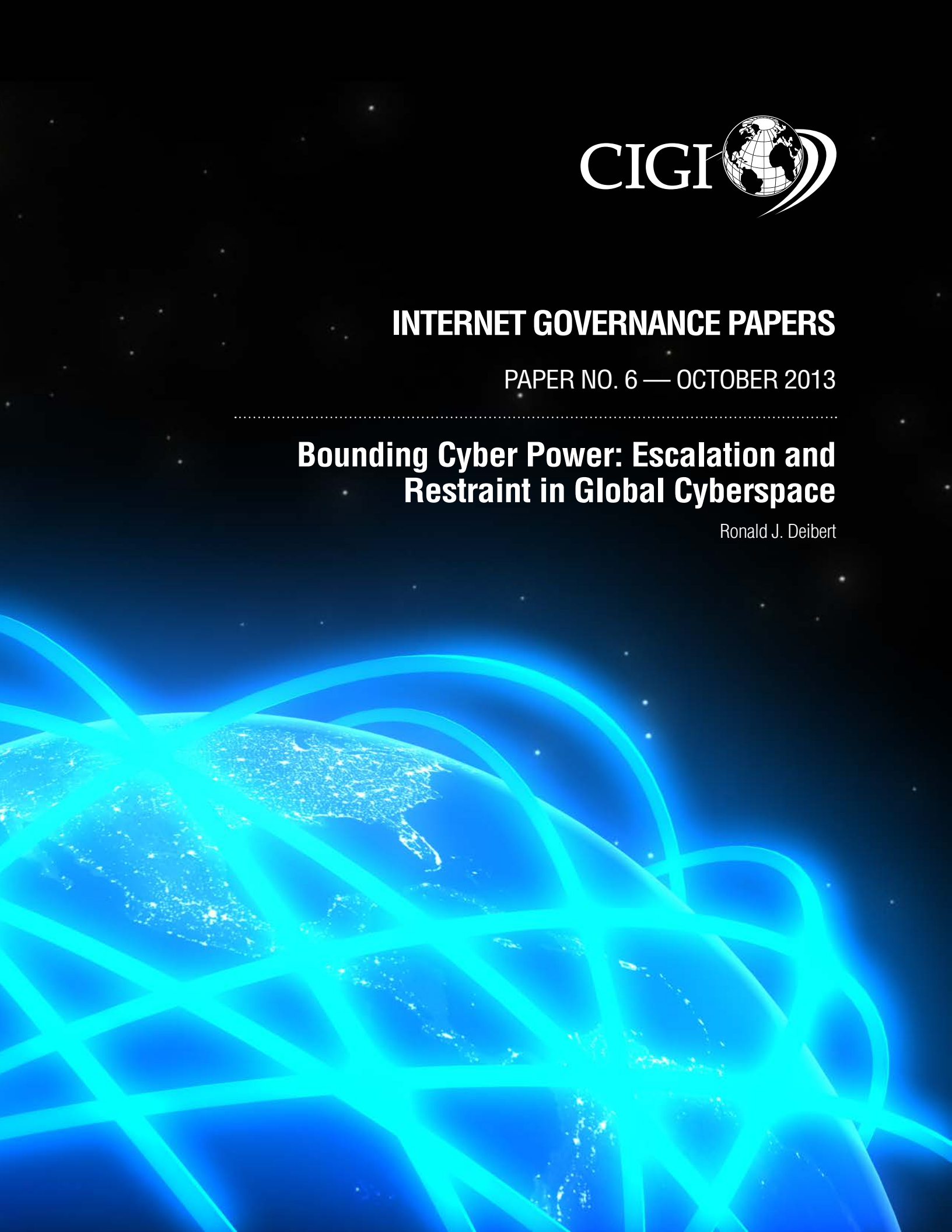

CIGI

INTERNET GOVERNANCE PAPERS

PAPER NO. 6 — OCTOBER 2013

Bounding Cyber Power: Escalation and Restraint in Global Cyberspace

Ronald J. Deibert

INTERNET GOVERNANCE PAPERS
PAPER NO. 6 — OCTOBER 2013

Bounding Cyber Power: Escalation and Restraint in Global Cyberspace

Ronald J. Deibert

Copyright © 2013 by The Centre for International Governance Innovation

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

This work was carried out with the support of The Centre for International Governance Innovation (CIGI), Waterloo, Ontario, Canada (www.cigionline.org). This work is licensed under a Creative Commons Attribution — Non-commercial — No Derivatives License. To view this license, visit (www.creativecommons.org/licenses/ by-nc-nd/3.0/). For re-use or distribution, please include this copyright notice.

ACKNOWLEDGEMENT

CIGI gratefully acknowledges the support of the Copyright Collective of Canada.

CIGI

CONTENTS

ABOUT ORGANIZED CHAOS: REIMAGINING THE INTERNET PROJECT

Historically, Internet governance has been accomplished *en passant*. It has emerged largely from the actions of computer scientists and engineers, in interaction with domestic legal and regulatory systems. Beginning at least with the 2003–2005 World Summit on the Information Society process, however, there has been an explicit rule-making agenda at the international level. This strategic agenda is increasingly driven by a coalition of states — including Russia, China and the Arab states — that is organized and has a clear, more state-controlled and monetary vision for the Internet. Advanced industrial democracies and other states committed to existing multi-stakeholder mechanisms have a different view — they regard Internet governance as important, but generally lack coherent strategies for Internet governance — especially at the international level. Given the Internet's constant evolution and its economic, political and social importance as a public good, this situation is clearly untenable.

A coherent strategy is needed to ensure that difficult trade-offs between competing interests, as well as between distinct public values, are managed in a consistent, transparent and accountable manner that accurately reflects public priorities. Guided by these considerations, CIGI researchers believe they can play a constructive role in creating a strategy for states committed to multi-stakeholder models of Internet governance.

In aiming to develop this strategy, the project members will consider what kind of Internet the world wants in 2020, and will lay the analytical groundwork for future Internet governance discussions, most notably the upcoming decennial review of the World Summit on the Information Society. This project was launched in 2012. The Internet Governance Paper series will result in the publication of a book in early 2014.

ABOUT THE AUTHOR

Ronald J. Deibert is professor of political science and director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto. His research interests include global security, human rights and the geopolitics of cyberspace and information controls.

He has published numerous articles, chapters and books on issues related to technology, media and world politics, including co-authoring the *Tracking Ghostnet* report, which documents an alleged cyber-espionage network affecting over 1,200 computers in more than 103 countries. He is also co-editor of three major volumes with MIT Press: *Access Denied: The Practice and Policy of Internet Filtering* (2008), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (2010) and *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (2011). He is the author of *Parchment, Printing, and Hypermedia: Communications in World Order Transformation* (New York: Columbia University Press, 1997) and *Black Code: Inside the Battle for Cyberspace* (McClelland & Stewart/ Random House, 2013).

Ronald is co-founder and principal investigator of the OpenNet Initiative and the Information Warfare Monitor, and he presently serves on the editorial board of the journals *International Political Sociology, Security Dialogue, Explorations in Media Ecology, Review of Policy Research* and *Astropolitics*. He is a consultant and adviser to governments, international organizations and civil society/non-governmental organizations on issues relating to cyber security, cybercrime, online free expression and access to information. He is a recipient of the Order of Ontario and Queen Elizabeth II Diamond Jubilee medal, and has a Ph.D. in political science from the University of British Columbia.

EXECUTIVE SUMMARY[1]

Cyberspace is the global communications and information ecosystem, and it is now deeply embedded in all aspects of society, economics and politics. As cyberspace has grown in size and significance, the security of the domain has become highly contested among states, the private sector and civil society. This paper is divided into two parts: The first half focusses on the forces that are contributing to escalating international tensions and conflicts in cyberspace, largely driven by state-based concerns around national security. From this perspective, the exercise of state power in cyberspace is growing (to borrow an old phrase) in "leaps and bounds." The second half employs a different meaning of "bounding power" — which refers to tying down, checking or restraining the exercise of power — and outlines steps that might be taken to lead us down an alternative path, whereby security and openness are both protected and preserved.

INTRODUCTION

At Georgetown University's April 2013 conference, International Engagement on Cyber, Eugene Kaspersky, CEO of Kaspersky Labs, delivered a keynote address about the prospects of a coming cyber disaster. His message was alarmist, meant to shock the gathered audience, but he also laid out a silver lining of sorts. After describing all of the enabling conditions that are leading us gradually, but invariably, toward catastrophe (and frankly admitting that even he really had no answers for these problems), he concluded on a cheery note: "we'll just get through it." If only it were so easy.

The previous evening, another set of keynote addresses was delivered with a complementary theme, this time by Republican State Representative Mike Rogers and the CEO of the cyber-security company Mandiant, Kevin Mandia. Rogers berated the Chinese government for their audacious acts of cyber theft, warned of the growing risks to critical infrastructure and then delivered his *coup de grace*: the United States needs to stop pussyfooting around, it's time to take the gloves off; now it's "game on."

For his part, Mandia talked about his company's widely publicized and discussed report, which presents evidence that the Chinese Peoples' Liberation Army was responsible for one of the most notorious China-based hacker groups, APT1.[2] Mandia freely admitted the report was coordinated with United States political leadership (including military, law enforcement and intelligence). The government had been briefed and, Mandia implied, even had a hand in the timing of the release. Said Mandia, "we're all ex-military, ex-intel guys" — suggesting comfortably close collaboration between his company and the government. For that reason, China and the rest of the world saw the report as a strategic escalation, a ratcheting up of the heated

1 The title of this paper is borrowed from John Hopkins University's Daniel H. Deudney's book, *Bounding Power: Republican Security Theory from the Polis to the Global Village*. In speaking with the author, Deudney explained that the title refers to a double entendre, which applies equally well to the theme of this paper: "bounding" in the sense of power growing in leaps in and bounds, and "bounding" in the sense of exploring ways to tie down and restrain that power. Parts of this paper are also drawn from points made in Ronald J. Deibert (2013), *Black Code: Inside the Battle for Cyberspace*, Toronto: Random House.

2 For the Mandiant report, see *APT1: Exposing One of China's Cyber Espionage Units*, available at: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

rhetoric between the United States and China around cyber-security issues.[3]

Rogers and Mandia are examples of a new, powerful logic emanating from inside "the Beltway," but rippling across the planet. Government and private sector officials are working increasingly in tandem, united around a *realpolitik* approach to the challenges of cyber security, buttressed by a burgeoning security-industrial complex reaping the economic windfall of the cyber-security market in an era of otherwise economic austerity.

The keynotes were also illustrative of something else: a sombre outlook on all things cyber. The Internet began with great hopes and expectations of liberation. Today, unfortunately, we live in a time of increasing cyber phobia. Cyber espionage and warfare, the growing menaces of cybercrime and data breaches, and the rise of new social movements such as WikiLeaks and Anonymous have vaulted cyber security to the top of the international political agenda.[4] Almost every day a new headline screams about a serious problem in cyberspace that demands immediate attention. There is a palpable urgency to act, defend against threats and build up capabilities to deter. But as ominous as the dark side of cyberspace may be, our collective reaction may become the darkest driving force of all. Where all this will lead is anyone's guess, but the constellation of factors contributing to a kind of perfect storm in cyberspace are strong and growing.

3 See Jack Goldsmith (2013), "The USG Strategy to Confront Chinese Cyber Exploitation, and the Chinese Perspective," *Lawfare*, February 21, available at: www.lawfareblog.com/2013/02/the-usg-strategy-to-confront-chinese-cyber-exploitation-and-the-chinese-perspective/.

4 For more on Anonymous, see Gabriella Coleman (2013), *Anonymous in Context: The Politics and Power Behind the Mask*, CIGI Internet Governance Papers Series No. 3.

This paper is divided into two parts, each reflecting a different meaning of a concept developed in Daniel Deudney's (1997) book *Bounding Power*. The first half focusses on the forces that are contributing to escalating international tensions and conflicts in cyberspace, largely driven by state-based concerns around national security. From this perspective, the exercise of state power in cyberspace is growing (to borrow an old phrase) in "leaps and bounds." The second half employs a different meaning of "bounding power," that which refers to tying down, checking or restraining the exercise of power, and outlines steps that might be taken to lead us down an alternative path, whereby security and openness are both protected and preserved. There is far more attention paid to conflict than to cooperation in cyber-security matters these days. Lessons of cooperation in other areas of international security that might be applied to the cyber domain are drawn upon in this section. Together, these steps are seen as a kind of "arms control" in cyberspace, in a very broad sense of the term. Arms control in cyberspace has been dismissed as irrelevant at best, or a political ruse at worst. There is not only merit in the concept, but at its heart is the recipe for a comprehensive approach to cyber security that secures a well-functioning global communications system without undermining political liberties. The principal argument is that the instinctive tendency to turn to *realpolitik* around cyber security is ultimately self-defeating, and that liberal democratic countries should pay more attention to bounding power in cyberspace, domestically and internationally, for both political and technical reasons.

BOUNDING CYBER POWER I: THE COMING "PERFECT STORM" IN CYBERSPACE

There are several trends happening simultaneously that are leading to a progressively more dangerous

and unstable environment in cyberspace. I have described these trends in detail elsewhere as a coming "perfect storm," and see them as largely contingent social and technological forces that are mutually reinforcing (Deibert, 2012). Summarized below are some of the most important trends, beginning with a broad transformation in the communications environment.

The rise of social media, mobile connectivity and cloud computing, while convenient and liberating, has fundamentally altered our communications ecosystem. In the space of a mere few short years, individuals have entrusted vast swaths of personal and private data to third parties, particularly the private sector. Some of this entrusting occurs consciously, when texts and emails are sent, documents are uploaded to cloud computing services or posts are made to social networking sites. But a great deal of it occurs unwittingly. For example, metadata is included in just about every digital transaction. In the case of mobile devices, metadata can include details about the make and model of the device, its geolocation, the destination of any communications (for example, calls, emails or SMS messages), and the length and time of the communication.[5] Metadata such as this can potentially be shared with and collected by cellphone tower operators, Internet service providers, Internet exchange points and even mobile device applications, among others. Regarding the latter, many applications give developers themselves permission to access users' contact lists, images captured by the mobile device's camera and text messages, in addition to whatever metadata is collected. Apple recently announced[6] that it crossed the 50 billion threshold for applications downloaded by users — a remarkable statistic underscoring the extent to which our digital lives have been turned inside out in recent years. The growing control by the private sector over so much data is happening simultaneously with another major shift: the growing assertion of government involvement in cyberspace. In the early days of the Internet, governments either lagged behind or consciously kept out of Internet governance issues. But over time, as the technology has matured and embedded itself into all aspects of society and economics, the stakes have grown, leading invariably to an increasingly larger presence of governments and cyberspace-related laws, regulations and policies (Mueller, 2010). Part of this involvement is meant to address risks relating to cybercrime. Individuals and organizations alike have adopted social media, cloud computing and mobile technologies too fast to develop appropriate security procedures, and there are frequently breaches of corporate and government databases. Many more are likely under-reported due to concerns about reputation. The risks around cybercrime, the possibility of crime blurring into espionage, and even warfare have vaulted cyber security to the top of the agenda. Nearly every government today ranks cyber-security issues highly, with many devoting proportionately greater resources to law enforcement and security agencies around cyberspace issues. For example, in the latest US Office of the Director of National Intelligence assessment, cyber threats are listed at the top, above terrorism.[7]

5 See *The Guardian*'s interactive guide to metadata, "A Guardian Guide to Your Metadata," available at: www.guardian.co.uk/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=0000000.

6 The announcement is available at: www.apple.com/ca/itunes/50-billion-app-countdown/.

7 For discussion of cyber threats, see Yousaf Butt (2013), "Rapid Response," *Foreign Policy*, March 22, available at: www.foreignpolicy.com/articles/2013/03/22/rabid_response?page=full.

Meanwhile, on a separate but related track, September 11 still casts a large shadow over the Western world and its approach to the cyber domain, with the long "war on terror" driving a major transformation in the security and exploitation of information and communications technology. The perceived failure to prevent that catastrophic event by not being able to "connect the dots" triggered a reshuffling in the law enforcement, defence and intelligence communities, and an exploding market for Big Data analytics.[8] This trend began as an urgent remedy to the existential threats of the September 11 terrorist attacks, and the need to prevent and contain future attacks by al-Qaeda and other terrorist groups. As we now know through documents leaked by Edward Snowden to *The Guardian* and *The Washington Post*, however, secret presidential authorizations, begun under the Bush administration and continued under Obama, led to vast expansions of surveillance programs undertaken with the cooperation of major telecommunications and Internet companies headquartered in the United States.[9] The perceived necessities of this new security regime — often described as "modernizing" lawful access regulations, but also undertaken under a shroud of secrecy — has effectively normalized wholesale collection of digital communications in the United States. This expansion has affected not only US citizens' communication rights, but also large portions of the world's Internet users whose communications are routed through US infrastructure and services.

Part and parcel of this normalization has been the growing prominence of signals intelligence agencies in cyberspace security. Three letter agencies that were born during the Cold War (such as NSA [National Security Agency], CSE [Communications Security Establishment], FSB ["Federal Security Service"]) have now assumed leadership roles, and have ballooned in size and scope as the perceived threats around cyberspace have grown larger. Canada's signals intelligence agency, Communications Security Establishment Canada, has seen its budget more than quadruple since 2001 and has a new headquarters being built in the Ottawa area, next to the headquarters of Canadian Security Intelligence Service.[10] Its US counterpart, the NSA, is building a massive data-processing complex in Utah —"Some published reports suggest it could hold 5 zettabytes of data. (Just one zettabyte is the equivalent of about 62 billion stacked iPhones 5's — that stretches past the moon.)."[11] The growth and prominent role of these agencies, largely operating in the shadows and closely linked to the military, shows the emphasis Western governments have placed on securitization of cyberspace.

Because most of what we call cyberspace is owned and operated by the private sector, and as a consequence of the vast amounts of data private sector communications companies control as part of their operations, governments have increasingly enrolled Internet and telecommunications companies in the policing of cyberspace. Revelations connected to the Edward Snowden leaks show that in the United States, in the wake of September 11,

8 For a discussion of this, see Shane Harris (2010), *The Watchers: The Rise of America's Surveillance State*, New York: Penguin.

9 See Glenn Greenwald and Spencer Ackerman (2013), "How the NSA is Still Harvesting Your Data," *The Guardian*, June 27, available at: www.guardian.co.uk/world/2013/jun/27/nsa-online-metadata-collection.

10 See: www.thestar.com/news/world/2013/06/07/canadians_not_safe_from_us_online_surveillance_expert_says.html

11 See James Bamford (2012),"The NSA is Building the Country's Biggest Spy Center (Watch What You Say)," *Wired*, March 15, available at: www.wired.com/threatlevel/2012/03/ff_nsadatacenter/.

companies with whom US security agencies had a long-standing working relationship were drawn more closely into surveillance programs.[12] Though no supporting documentation exists in the public domain, it is probably a safe assumption that similar sharing arrangements have been made in Canada, the United Kingdom, Australia, New Zealand and elsewhere. Even putting aside the cooperation that occurs under the umbrella of secrecy, widely available public evidence shows demands by governments on companies are increasing. Remarkably, Google, Twitter and Microsoft's transparency reports all reveal the highest volume of requests to companies for user data coming from liberal democratic countries.[13]

The surveillance and policing programs are complemented by the gradual emergence of a more offensive posture in cyberspace. Representative Rogers' incitement about "game on" may be striking but his view is not unique. General Keith Alexander, notably the head of both the NSA and United States Cyber Command, recently testified before Congress that the Pentagon "is conducting a coordinated, thorough review with the Joint Staff of existing standing rules of engagement on cyberspace. These revised standing rules of engagement should give us authorities we need to maximize pre-authorization of defense responses and empower activity at the lowest level" (cited in Maurer, 2012). This follows alongside proposals to reorient the rules of the engagement in cyberspace for the US Department of Defense to allow attacks on even private networks abroad as part of the "defence of the nation" (Nakashima, 2012). There has also been discussion about the use of kinetic, even nuclear attacks, as a way to deter against cyber assaults. The cyber-enabled sabotage of Iranian nuclear enrichment facilities, known as Operation Olympic Games, and the so-called Stuxnet weapon at the heart of it, may not have been the first recorded instance of a cyber attack resulting in physical damage (the Israeli disabling of radar installations in Syria prior to an air assault on a nuclear reactor would get that distinction), but Stuxnet definitely crossed a threshold. One remarkable difference with cyber weapons is that their design proliferates to the victims and others with each applied use. You can't get the blueprints for a ballistic missile after it blows up, but you can once a cyber weapon is deployed.[14]

States are not the only institutions ratcheting up offensive capabilities. The concept of "attacking back" — a euphemism for the private sector taking matters into their own hands, reaching across borders to disable networks that are causing them problems — adds another layer of complexity to the offensive environment.[15] It is now not uncommon to hear representatives of telecommunication companies speak of the legitimacy of using offensive computer network attacks, with the same rationale

12 For the top-secret draft report from 2009, see "NSA inspector General Report on Email and Internet Data Collection under Stellar Wind — Full Document" (2013), *The Guardian*, June 27, available at: www.guardian.co.uk/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection.

13 For Google, see www.google.com/transparencyreport/; for Twitter, see https://transparency.twitter.com/; and for Microsoft, see www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/.

14 For a thought provoking discussion of cyber war and cyber weapons, see Thomas Rid (2013), *Cyber War Will Not Take Place*, Hurst & Co. Rid disputes the use of the term "cyber weapon" in these and other examples on the basis of a strict definition of what constitutes a "weapon."

15 See Joseph Menn (2012), "Hacked Companies Fight Back with Controversial Steps," *Reuters*, June 17, available at: www.reuters.com/article/2012/06/17/us-media-tech-summit-cyber-strikeback-idUSBRE85G07S20120617.

now spreading to other market sectors. A recent survey undertaken of the private sector suggests that at least half of companies surveyed "thought their companies would be well served by the ability to 'strike back' against their attackers" (cited in Fallon, 2012). Meanwhile, some civil society activists and anti-authority collectives, such as Anonymous and LulzSec, have demonstrated an unpredictable but still relatively frequent tendency to engage in computer network attacks, particularly crowd-sourced denial of service.[16]

Looking at all of these factors from an international relations theory vantage point, it is clear that the structural conditions tend toward an arms race. Harvard's Joseph Nye is perhaps the first to articulate clearly how in the cyberspace domain, offence is dominant, deterrence is difficult to implement because of the problems associated with attributing attacks to their perpetrators and barriers to entry are low.[17] Attacks can be organized at lightning speed, from across the planet and can bury responsibility behind cleverly disguised methods and commandeered computers. While Mandiant may have made some progress overcoming the attribution problem, their progress may have had less to do with anything in particular it did than the fact that China-based attackers tend to be careless in hiding their tracks. Other countries and organizations are likely to be more careful.

The combination of these factors creates an increasingly unpredictable and potentially dangerous environment. The possibility of an accident, a misunderstanding or a targeted attack gone wrong, leading to reprisals or escalation, is very real. Considering that in an "Internet of Things" world, critical infrastructure is now increasingly connected to the Internet, such risks must be factored highly. For example, recent attacks emanating from North Korea disrupted the services of South Korean banks at a time of heightened tensions between the two countries. If those attacks affected South Korean critical infrastructure in a serious way, and were not merely a nuisance, they could have led to a South Korean reprisal, and possibly even US cyber or kinetic retaliation, which, in turn, could provoke a wider escalation involving China. In many ways, it feels as though we are in a situation similar to that which existed prior to World War I: no government desires war, but the structural conditions of the situation lead to it regardless.[18]

Among the factors contributing to the perfect storm in cyberspace is a political-economy dynamic. The growing needs of states and companies to go on the offence, to monitor communications networks, to infiltrate adversaries abroad, and to filter and analyze big data, have produced a massive explosion in the cyber-security industry. Cold War-era companies are now reorienting their business lines (for example, Raytheon, Northrup Grumman and Science Applications International Corporation) to sell a range of products and services to supply this need, from deep packet inspection to commercialized spyware. Other smaller, more specialized companies have also sprouted up. The size of this sector is difficult to gauge, given that it tends to operate in the shadows and under the veil of classification. Recently, *The Washington Post* put together a special exposé on "Top Secret America" that gives some indication of the market: hundreds

16 See Coleman (2013), "Anonymous in Context."

17 See Joseph Nye (2010), "Cyber Power," Belfer Center for Science and International Affairs, Harvard, May, available at: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

18 The seminal account of this is Barbara Tuchman (2004), *The Guns of August*, New York: Presidio Press.

of firms reaping billions of dollars in contracts.[19] It is important to note that although developed to service primarily US and allied needs, the market knows no boundaries. Products and services that are first developed and offered to Western law enforcement, defence and intelligence agencies are finding their ways into the hands of the world's autocratic and authoritarian regimes, which are using them to monitor and disable their own citizens' networks (for these regimes, the networks constitute the predominant security threat). Policy makers now have at their disposal a suite of tools that broaden their capabilities considerably: cellphone tracking, deep packet inspection, and even surreptitious computer and network penetration.

The Citizen Lab's research, based out of the University of Toronto's Munk School of Global Affairs, has been tracking this dark market, shedding light on its scope, scale and character. In 2011, it found that US-based Blue Coat Systems' network monitoring devices were deployed in Syria and Burma.[20] The Lab followed this up in 2013 with its Planet Blue Coat report, which used wide-scale Internet scans to reveal the presence of Blue Coat ProxySG devices (capable of censorship) and Blue Coat PacketShaper devices (capable of mass surveillance) in countries that rank among the world's most notorious abusers of human rights, including China, Russia, the United Arab Emirates and Vietnam.[21] In 2012, Citizen Lab researchers determined that the computers of Bahraini and Emirati activists were secretly monitored by their own governments using spyware products sold by a British (Gamma International) and an Italian (Hacking Team) company, respectively.[22] Notably, Blue Coat Systems, Gamma International and Hacking Team all made Reporters Without Borders' 2013 "Corporate Enemies of the Internet" list, ranking alongside "State Enemies of the Internet" Syria, China, Iran, Bahrain and Vietnam.[23] In *You Only Click Twice: FinFisher's Global Proliferation*, Citizen Lab's researchers document the results of a comprehensive global Internet scan for the command and control servers of Gamma International's FinFisher surveillance software.[24] The report details the discovery of a campaign in Ethiopia using FinSpy spyware against a political opposition group, and an examination of a FinSpy Mobile sample that appears to have been used in Vietnam. The researchers also found command and control servers for FinSpy backdoors, part of the FinFisher "remote monitoring solution," in 25 countries: Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, the United Arab Emirates, the United Kingdom, the United States and Vietnam.

Although a new and still largely obscure market, this trade in what some are calling "digital arms" is clearly spreading quickly. Innovation in this case comes from a variety of drivers: the nearly insatiable desire among autocratic regimes to infiltrate, subvert and disable networked opposition; the growing

19 This exposé is available at http://projects.washingtonpost.com/top-secret-america/.

20 See https://citizenlab.org/2011/11/behind-blue-coat/.

21 See https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/.

22 See https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/, and https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/, respectively.

23 See http://news.cnet.com/8301-13578_3-57573707-38/meet-the-corporate-enemies-of-the-internet-for-2013/.

24 See https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

desire among law enforcement, defence and intelligence agencies to exploit tools that allow them to undertake domestic surveillance and/or espionage abroad; and increasingly from large companies taking matters into their own hands, striking back at attackers they deem to be violating their private property.

Against the backdrop of these trends is a major demographic reality: today, most of the world's Internet population comes from the world's failing and fragile states, in countries where religion plays an important role and where authoritarian and autocratic regimes predominate. Political regimes of the Global South are coming into cyberspace in the context of the post-September 11 environment, with security at the top of the agenda. Many of these countries are placing more priority around controlling what content their citizens can access, and already have broad Internet filtering and surveillance regimes in place.[25] For these countries, many of which have governance challenges and face persistent domestic insecurities, greater state control of cyberspace is appealing on a number of levels. Moreover, the recent Snowden/NSA revelations will feed into this desire, as policy makers in these countries come to recognize the significant "home field" advantage enjoyed by the United States and its allies because of the routing of global telecommunications traffic through enterprises domiciled in, and thus subject to the laws of, the United States.[26] We can expect to see more international diplomatic efforts, such as those witnessed around the bungled 2012 ITU-WCIT (International Telecommunications Union-World Conference on International Telecommunications) meeting in Dubai, to lend international legitimacy to greater territorialized controls over cyberspace — a development that runs directly contrary to liberal democratic governments' foreign policy interests.

The global domain of telecommunications and Internet-enabled cyberspace is now feeling the stress of these combined pressures. What began as an accidental network that blossomed to become the infrastructure for planetary communications is now at a breaking point. Continuing the trajectory leads us down a path of much more tightly controlled national Internet spaces, a balkanization of the Internet, driven by security and political concerns, and possibly even a major catastrophe borne out of an increasingly ratcheted up arms race. For those who care about the value of an open system of information on a global scale, a strategy for remediation and long-term stability is critical.

BOUNDING CYBER POWER II: TOWARDS MIXTURE, DIVISION AND RESTRAINT

Faced with mounting problems and pressures to do something, policy makers may be tempted by extreme solutions. The Internet's de facto and distributed regime of governance — until recently, a mixture of informal and formal operating procedures, with decisions made by mostly like-minded engineers[27] — has come under increasing stress as a function of the Internet's continuing rapid growth and insecurity. There is an instinctive tendency in security-related discussions to default to the tradition of realism, with its accompanying state-centrism, top-down hierarchical controls and

25 For discussion and analysis of this, see Ronald J. Deibert et al. (eds.) (2010), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge: MIT Press.

26 See Ronald J. Deibert (2013), "Why NSA Spying Scares the World," *CNN Opinion*, June 12, available at: www.cnn.com/2013/06/12/opinion/deibert-nsa-surveillance.

27 For a description of this regime, see Laura De Nardis (2013), *Internet Points of Control as Global Governance*, CIGI Internet Governance Papers Series No. 2.

erection of defensive perimeters to outside threats. In the creation of cyber commands, in spiralling arms races among governments, in "kill switches" on national Internets and in the rising influence of the world's most secretive agencies into positions of authority over cyberspace, we see this tradition at play. As compelling as it may be, however, realism and its institutional manifestations fit awkwardly in a world where divisions between inside and outside are blurred, threats can emerge as easily from within as without and that which requires securing — namely cyberspace — is, ideally, a globally networked commons of information almost entirely in the hands of its users. Not only are the security policies and practices in predominance today antithetical to the principles of liberal democratic government and to the system of checks and balances and public accountability upon which it rests, they also legitimize the growing desire of autocratic and authoritarian regimes to subject cyberspace to territorialized controls, and the censorship and surveillance practices that go along with it.

There is an urgent need for the articulation of an alternative cyber-security strategy for civic networks and from the perspective of liberal democracy. For many who would characterize themselves as part of global civil society, "security" is seen as anathema. In today's world of exaggerated threats and self-serving hyperbole, it is easy to dismiss security as a myth to be demolished, rather than engaged.[28] Securitization is generally associated with the defence industry, Pentagon strategists, intelligence agencies and many others question whether employing the language of security only plays into this complex. But the vulnerabilities of cyberspace are very real, the underbelly of cybercrime is undeniably huge (and growing), an arms race in cyberspace is escalating and major governments are poised to set the rules of the road that may impose top-down solutions that subvert the domain as we know it. Dismissing these vulnerabilities as manufactured myths propagated by power elites will only marginalize civic networks from the conversations where policies are being forged.

There is an instructive parallel to be made between cyber-security discourse today and the global nuclear situation during the Cold War. At the dawn of the nuclear age, many theorists and intelligence community experts predicted nuclear weapons proliferation would proceed swiftly and inevitably. A recent study by Brookings has shown that these forecasts were, in fact, persistently inaccurate (Yusuf, 2009). Most expert projections erred on the pessimistic side. Also, the pacing and timing of nuclear proliferation has been consistently slower than most predicted. The reason for the inaccuracies are clear: security analysts were mostly informed by expectations and self-fulfilling prophecies that never fully materialized, and which did not take into account remediation efforts by arms control and counter nuclear proliferation advocacy and policy engagement that rose above that paradigm to strive for something more. Arms control efforts around nuclear (and other weapons of mass destruction) proliferation paid off in the long run, mitigating the worst of the pessimistic scenarios.

Arms control in cyberspace, on the other hand, has been ignored at best, ridiculed at worst. There are at least two reasons. One is the result of a widespread belief, articulated most prominently in an article by Georgetown University professor of computer science, Dorothy Denning, that information cannot be easily controlled in the same manner that classes

28 For an extended discussion, see Ronald J. Deibert (2011), "Towards a Cyber Security Strategy for Global Civil Society," *GISWatch*, November, available at: www.giswatch.org/en/freedom-expression/towards-cyber-security-strategy-global-civil-society.

of kinetic weapons can be.[29] While persuasive, the argument is directed at only one element of the broad set of practices associated with arms control: limiting or eliminating weapons. The second reason arms control in cyberspace is largely discredited has to do with a series of Russian-sponsored proposals made at the United Nations in favour of arms control around information weapons and operations.[30] Considering Russia's poor track record around computer crime, surveillance and computer network attacks in Estonia and Georgia, the proposals have been poorly received and seen by many as thinly veiled attempts to reign in US superiority in cyber capabilities.

Although both of these examples show us reasons to be cautious about arms control in cyberspace, neither of them are good reasons to abandon it entirely. Arms control refers not just to restrictions on certain classes of weapons, but to a wide variety of mutual restraint mechanisms, ranging from disarmament to cooperation around certain behaviours and practices, to agreements on the treatment of entire domains (sea, outer space, Antarctica and so on), to even something as broad as the framework of entire political structures. Deudney (1995) describes the liberal theoretical tradition in its entirety, and at its heart, as being a theory of arms control — what he calls "distributed security." The tradition of distributed security finds roots in liberal political orders reaching back to ancient Greece and the Roman Republic, and the late medieval, early Renaissance trade-based systems exemplified by the Venetians, the Dutch and the English. But the fullest expression of distributed security is found in the early United States and the writings of political philosophers associated with it, notably Montesquieu, Publius and others. Although multi-faceted and complex, distributed security starts with the aim of building structures that rein in and tie down political power, both domestically and internationally as a way to secure rights and freedoms. It's informed by "negarchy" as a structural alternative to the twin evils of "hierarchy" and "anarchy." In short, distributed security is the *negation* of unchecked and concentrated power.

At the core of this model are several key principles that can form the basis of a liberal democratic strategy for cyber security: mixture, division and restraint. Mixture refers to the intentional combination of multiple actors with governance roles and responsibilities in a shared space, while division refers to a design principle that no one of these actors is able to control the space in question without the cooperation and consent of others. As an approach to global cyberspace security and governance, each principle can provide a more robust foundation for the empty euphemism of "multi-stakeholderism," and a principle upon which to counter growing calls for a single global governing body for cyberspace. Citizens, the private sector and governments all have an important role to play in securing and governing cyberspace, but none to the exclusion or pre-eminence of the others.

Civic networks need to be players in the governance forums where cyberspace rules of the road are implemented. This is not an easy task, since there is no one single forum of cyberspace governance; instead, governance is diffuse and distributed across multiple forums, meetings and standard-setting bodies at local, national, regional and global levels.[31]

29 See http://faculty.nps.edu/dedennin/publications/Berlin.pdf.

30 See John Sheldon (2010), "The Case Against Cyber Arms Control," *World Politics Review*, December 9, available at: www.worldpoliticsreview.com/articles/7273/the-case-against-cyber-arms-control.

31 See DeNardis (2013), *Internet Points of Control as Global Governance.*

The idea of civil society participation in these rule-making forums varies widely, and is alien to some. Governments and the private sector have more resources at their disposal to attend meetings and influence their outcomes. Civic networks will need to collaborate to monitor all of these centres of governance, open the doors to participation in those venues that are now closed shops and make sure that "multi-stakeholder participation" is not just some paid lip service by politicians, but something meaningfully exercised as part of a deliberate process. Mixture and division are the principles upon which this justification can be made.

Consider the trajectory of the so-called London Cyber Process, which began in 2011 in London, followed by Budapest in 2012 and South Korea beginning later in 2013. (It is rumoured that Canada will make a pitch to host in 2014.) On the one hand, it is encouraging to see discussions about rules of the road in cyberspace among the great powers and, at the very least, such efforts could do well to build confidence and reduce uncertainty. But on the other hand, the meetings have been mostly state-driven exercises, with a private sector presence and civil society participating from the margins. Constituted this way, should the London Process ever conclude with an agreement, it would reflect partial concerns, at best, and potentially the lowest common denominator that unites China, Russia, the United States and the United Kingdom, at worst.

The principle of restraint is perhaps the most threatened by overreaction today. Securing cyberspace requires reinforcement of restraint on power, including checks and balances on governments, law enforcement and intelligence agencies. In an environment of big data, in which so much personal information is entrusted to third parties, oversight mechanisms on government agencies are essential. To be sure, security agencies are essential elements of government today; the world continues to be a dangerous place. But if they operate in an increasingly unrestrained environment, the potential for abuse of power is substantial. Part of a distributed security strategy must, therefore, also include a serious engagement with law enforcement. Many law enforcement agencies are overwhelmed with cybercrime and understaffed, lack proper equipment and training, and have no incentives or structures to cooperate across borders. Instead of dealing with these shortcomings head on, politicians are opting for Patriot Act powers that dilute civil liberties, place burdens on the private sector and conjure up fears of a surveillance society. What law enforcement needs is not new powers; it needs new resources, capabilities, proper training and equipment. Alongside these new resources should be the highest standards of judicial oversight and public accountability. Security and oversight are not incompatible; they are two sides of the same distributed security coin.

Although not often explicitly articulated as a philosophy, distributed security also captures the most efficient and widely respected approach to practical security in the computer science and engineering circles. Here it is important to remind ourselves that in spite of the threats, cyberspace runs well and largely without persistent disruption. On a technical level, this efficiency is founded on open and distributed networks of local engineers who share information as peers in a community of practice rooted in the university system (itself, a product of the liberal philosophy upon which distributed security rests). These communities need to be central during discussions about cyberspace governance, with government officials in supporting roles, rather than the other way around. The gradual securitization of the forums in which these communities interact, including more prominent participation of security agencies, threatens to erode the trust upon which the Internet functions.

What is remarkable is that the Internet functions precisely because of the absence of centralized control, because of the thousands of distributed, loosely coordinated monitoring mechanisms.[32] While these decentralized mechanisms are not perfect and can occasionally fail, they can also form the basis of a coherent distributed security strategy. Bottom-up, grassroots solutions to the Internet's security problems are consistent with principles of openness, avoid heavy-handedness and provide checks and balances against the concentration of power. Part of a distributed security strategy should enable ways to facilitate cooperation among the existing, largely scattered security networks while making their actions more transparent and accountable. These technical steering functions should be preserved as much as possible along the lines of reputation-based and independently distributed governance mechanisms in order to support an open yet secure communications space.

In other words, rather than abolish this system for another, more top-down approach, it should be buttressed and amplified. Loosely structured but deeply entrenched networks of engineers, working on the basis of credible knowledge and reputation, whose mission and *raison d'être* is to focus on cyberspace itself and its secure functioning to the exclusion of all else, are essential to its sustenance and security. We need to build out and give room and space for those networks to thrive internationally, rather than co-opt their talents for national security projects that create international divisions and rivalry.

One factor that would help facilitate such a development would be to conscientiously avoid the rhetoric of warfare and weapons in descriptions of threats and issues that are largely criminal in nature. Far too often, military and intelligence agencies are given deference in responses to areas from which they should more properly be excluded altogether. Lessons from the nuclear era could be drawn here as well. University of Toronto international relations theorist Emanuel Adler undertook a seminal study of the learning among Russian and US nuclear scientists during the Cold War, leading to the eventual development of a transnational epistemic community around nuclear arms control.[33] Critical to the success of this process was the engagement of scientists, engineers and civilian bodies with each other, unencumbered by the national defence agencies operating at higher levels. While Reagan-era mythology attributes the end of the Cold War to the United States outspending the Soviet Union, arguably just as important was the learning and trust among this epistemic community that contributed to the war's end. A page could be taken from this process and applied to supporting transnational networks of civilian engineers, scientists and practitioners in the cyber domain.[34]

---

32 Governance of the "root zone" is an exception — "the only point of centralized control in what is otherwise a distributed and voluntaristic network of networks." See Milton Mueller (2004), *Ruling the Root: Internet Governance and the Taming of Cyberspace*, Cambridge: MIT Press.

33 See Emanuel Adler (1992), "The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control," *International Organization* 46, no. 1: 101–145.

34 Unfortunately one critical difference between cyber and nuclear eras is that in the nuclear era, no one except the most extremist on either side really desired an outcome that would spell the end of civilization. With the cyber era, the consequences are almost certainly several orders of magnitude less destructive than a nuclear war, and far fewer people are motivated to rein in the cyber arms race. In fact, there are substantial constituencies that benefit from its continuation.

Arms control is almost always thought of as a set of practices that apply to states. But in light of the fact that the vast majority of cyberspace is owned privately, the same basic premise of oversight and accountability must also extend to the private sector. Civic networks like those that helped spawn the Arab Spring are inherently transnational and have a vital role to play in monitoring the globe-spanning corporations that own and operate cyberspace. Persistent public pressure, backed up by credible evidence-based research and campaigns (such as the Electronic Frontier Foundation's privacy scorecard), are the best means to ensure the private sector complies with human rights standards worldwide. Civic networks must also make the case that government pressures to police the Internet impose costly burdens on businesses that should be conceded only with the greatest reservations and proper oversight. Efforts to promote greater corporate social responsibility in the cyber domain, such as the Global Network Initiative, fit squarely into the distributed security model and should be encouraged. When complemented by government regulations that set standards around breach disclosures and respect for human rights abroad, a robust set of checks and balances can be developed, at least in the liberal democratic core, before gradually moving outward.

One area where such restraints should be explored is around the growing cyber-security market, particularly those technologies that clearly have offensive uses. The European Parliament has been debating end-use based restrictions on this trade.[35] Others think that's futile.[36] The US Department of State has issued guidance on the export of "sensitive technologies" to Iran and Syria pursuant to the applicable sanctions regimes.[37] Human rights organizations have filed complaints against Gamma International,[38] and Citizen Lab urged investor activism[39] when it discovered that Blue Coat Systems was owned, in part, by the Ontario Teachers' Pension Plan. To be sure, there are no easy or simple answers to this market and it's not clear that more government regulations or laws are the answer. But it is clear that greater vigilance and oversight are necessary, and that we cannot rely on market forces and corporate social responsibility to take care of negative uses on their own.

Universities have a special role to play as stewards of an open but secure cyberspace, since it was from "the university" that the Internet was born, and from which its guiding principles of peer review and transparency were founded. Protected by academic freedom, equipped with advanced research resources that span the social and natural sciences, and distributed across the world, university-based research networks are essential custodians and monitors of an open and secure cyberspace.

---

35 See the interview with Marietje Schaake, Dutch member of the European Parliament, available at: www.marietjeschaake.eu/2013/02/media-digital-freedom-strategy-vieuws/.

36 For a representative example, see James Lewis (2013), "Arms Trade as Analogy," *Cyberdialogue*, available at: www.cyberdialogue.ca/2013/03/arms-trade-as-analogy-by-james-lewis/.

37 See www.federalregister.gov/articles/2012/11/13/2012-27642/department-of-state-state-department-sanctions-information-and-guidance.

38 See www.privacyinternational.org/blog/our-oecd-complaint-against-gamma-international-and-trovicor.

39 See www.thestar.com/opinion/editorialopinion/2013/02/06/teachers_pension_plan_invests_in_internet_surveillance_firm.html.

A distributed approach to cyber security should amplify the role of inspector generals and privacy commissioner's offices. As more data is shared internationally and with third parties, the security of personal data is a critical public policy issue. Privacy commissioners and independent auditors are best poised to evaluate, monitor and raise awareness about these concerns. For example, Canadian privacy commissioners have a proven track record of leadership in cyberspace policy matters in Canada, and enjoy a strong reputation for this leadership abroad. It is a strength Canada should build upon and use as a model to export to countries just now beginning to grapple with cyberspace governance and security, rather than focussing primarily on the security agencies as the leads for engagement on best practices abroad.

Finally, bounding power in cyberspace will require a general attitude shift among users as to how they approach cyberspace. There is a paradox today: as never before we are surrounded by technology, and yet as never before do we, the users, know so little about how that technology functions. For most of us, it is indeed the "consensual hallucination" that novelist William Gibson once defined — always on, always working, 24/7, like running water. It is this obliviousness to what goes on beneath the surface that allows such untrammelled violations of privacy to occur. Shifting this attitude will not be easy. Cyberspace is an extraordinarily complex technological environment, and it gets more complex with each passing day. Furthermore, there are considerable disincentives to having average people "lifting the lid" on the technology, including secrecy laws and intellectual property protections. However, an essential check on the abuse of power in cyberspace must come from changing this social outlook from the ground up. Citizens must be encouraged to not accept the technological infrastructure of cyberspace and its services for granted. Lifting the lid on the Internet should be encouraged as a kind of civic virtue.

CONCLUSION

Looking toward the near term in cyberspace governance, there are many possible scenarios, with unforeseen contingencies taking us down any number of paths. At the same time, politics and society are not entirely chaotic: social order is shaped by underlying forces that set the tempo and framework within which life unfolds. Today, these forces appear to be driving securitization processes in cyberspace, processes that may end up subverting the domain entirely, possibly leading to system wide instability and perhaps even international violence.

It is imperative that we use our agency to check and constrain the least desirable elements of these trends and shape those structures that provide the framework for what is seen as legitimate or not. Doing so will require a clear vision and a strategy to implement it, which in turn will require coordinated work at multiple levels and involve a wide variety of stakeholders. The obstacles standing in the way of realizing this vision are certainly formidable, but the alternatives to doing nothing are dire.

The securitization of cyberspace may be inevitable, but what form that security takes is not. As the securing of cyberspace unfolds, ensuring basic principles of transparency, accountability and mutual restraint will be critical. To secure cyberspace in a way that does not sacrifice openness, liberal democracies do not need a new "cyber" theory, nor a reversion to old-school paradigms that reinforce international division; rather, we need to reinvest in and apply to the domain of cyberspace some timeless principles and practices.

WORKS CITED

Deibert, Ronald J. (2012). "The Growing Dark Side of Cyberspace (...and What To Do About it)." *Penn State Journal of Law & International Affairs* 1, no. 2.

Deudney, Daniel H. (1995). "The Philadelphian System: Sovereignty, Arms Control, and Balance of Power in the American States-Union, Circa 1787-1861." *International Organization* 49, no. 2: 191–228.

——— (1997). *Bounding Power: Republican Security from the Polis to the Global Village*. New Jersey: Princeton University Press.

Fallon, William J. (2012). "Willing Cyber Battles Without Fighting." *Time*, August 27. Available at: http://nation.time.com/2012/08/27/winning-cyber-battles-without-fighting/.

Maurer, Tim (2012). "Breaking Bad: How America's Biggest Corporations Became Cyber Vigilantes." *Foreign Policy*, September 10. Available at: www.foreignpolicy.com/articles/2012/09/10/breaking_bad?wp_login_redirect=0.

Mueller, Milton (2010). *Networks and States: The Global Politics of Internet Governance*. Cambridge: MIT Press.

Nakashima, Ellen (2012). "Pentagon Proposes More Robust Role for Its Cyber-Specialists." *The Washington Post*, August 9. Available at: http://articles.washingtonpost.com/2012-08-09/world/35491430_1_cyber-command-military-action-networks.

Yusuf, Moeed (2009). "Predicting Proliferation: The History of the Future of Nuclear Weapons."Brookings Foreign Policy Paper Series, January. Available at: www.brookings.edu/research/papers/2009/01/nuclear-proliferation-yusuf.

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on four themes: the global economy; global security; the environment and energy; and global development.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

CIGI MASTHEAD

Managing Editor, Publications
Carol Bonnett

Publications Editor
Jennifer Goyder

Publications Editor
Sonya Zikic

Assistant Publications Editor
Vivian Moser

Media Designer
Steve Cross

EXECUTIVE

President
Rohinton Medhora

Vice President of Programs
David Dewitt

Vice President of Public Affairs
Fred Kuntz

Vice President of Finance
Mark Menard

COMMUNICATIONS

Communications Specialist
Kevin Dias
kdias@cigionline.org
1 519 885 2444 x 7238

Public Affairs Coordinator
Erin Baxter
ebaxter@cigionline.org
1 519 885 2444 x 7265

57 Erb Street West
Waterloo, Ontario N2L 6C2, Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org