A Call to Cyber Norms

Discussions at the Harvard–MIT–University of Toronto Cyber Norms Workshops, 2011 and 2012

Belfer Center for Science and International Affairs
Kennedy School of Government
Harvard University

Computer Science and Artificial Intelligence Laboratory (CSAIL)
Massachusetts Institute of Technology

Canada Centre for Global Security Studies
Munk School of Global Affairs
University of Toronto

American Bar Association
Cybersecurity Legal Task Force

March 2015

The Cyber Norms Workshops were conducted under the Chatham House Rule, which bars quoting or attributing speakers' remarks.

The materials contained herein represent the opinion of the discussants and do not reflect the official policy of their respective agencies, private sector organizations, or governments. The materials should not be construed to be those of either the American Bar Association or the ABA Cybersecurity Legal Task Force unless adopted pursuant to the bylaws of the Association. These materials and any forms and agreements herein are intended for educational and informational purposes only.

A Call to Cyber Norms Acronyms

APEC –	Asia-Pacific Economic Cooperation
ARF –	ASEAN Regional Forum
ASEAN –	Association of Southeast Asian Nations
BGP –	Border Gateway Protocol
C&C –	Command and Control
CA –	Certificate Authorities
CBMs –	Confidence-building Measures
CERTs –	Computer Emergency Response Teams
CLOS –	Convention on the Law of the Sea
CSAIL –	Computer Science and Artificial Intelligence Laboratory
CTBT –	Comprehensive Nuclear Test Ban Treaty
DIME –	Diplomatic, Intelligence, Military, and Economic
DNS –	Domain Name System
DPI –	Deep Packet Inspection
ECIR –	Explorations in Cyber International Relations
GGE –	Group of Governmental Experts
GSSD –	Global Security Strategy and Diplomacy
IANA –	Internet Assigned Numbers Authority
ICANN –	Internet Corporation for Assigned Names and Numbers
ICT –	Information and Communication Technologies
IETF –	Internet Engineering Task Force
IoT –	Internet of Things
IPv6 –	Internet Protocol version 6
ISPs –	Internet Service Providers
ITU –	International Telecommunication Union
LOAC –	Law of Armed Conflict
NATO –	North Atlantic Treaty Organization
NSA –	National Security Agency
OSCE –	Organization for Security and Cooperation in Europe
PSI –	Proliferation Security Initiative
RIRs –	Regional Internet Registries
RoE –	Rules of Engagement
SCO –	Shanghai Cooperation Organization
SDN –	Software-defined Networking
VOIP –	Voice Over Internet Protocol
W3C –	World Wide Web Consortium
WCIT –	World Conference on International Telecommunications
WMD –	Weapons of Mass Destruction

Introduction

In little more than two decades, the Internet has evolved from a medium for scientific communication, embedded in academic culture, to a worldwide ecosystem that supports an enormous variety of interactions and transactions at both global and local levels. Its users have grown nearly a thousand-fold in number to over two billion, and their distribution has shifted from predominantly young, white, North Atlantic males to a globally dispersed, increasingly heterogeneous population with a majority in the global East and South. As wireless telephony and the Internet converge, and as clouds multiply, cyberspace has become increasingly ubiquitous, mobile, and geographically indeterminate.

These transformations have profoundly affected societies and states: government and military operations, medical and social services, economic production and distribution, power grids and financial markets all depend on digital networks, almost invariably connected through the Internet. Cyber applications such as social media have also reshaped political campaigns and protests, as seen first in the 2008 US presidential campaign and dramatically in the Arab Spring of 2011–2012.

These changes have a dark side. Besides supporting cooperation, cyberspace has become a platform for local and transborder irritation and conflict in forms like spam; disinformation campaigns; incitement of extremism; cybercrimes; political, military, and economic espionage; censorship and filtering of information flows; government surveillance and invasion of privacy; intentional disruptions of critical government and civilian services; and direct damage to digitally controlled infrastructure. As a result, Internet governance and norms vitally concern states, the private sector, civil society, and individual users, and they are increasingly matters of contention. Policy-makers in major and emerging cyber powers have realized that the Internet has outgrown earlier notions of acceptable behaviors in cyberspace and the rules for interactions among state actors and their citizens are unclear and inadequate. Such *anomie* threatens the beneficial use of cyberspace and even international security. In 2010, in a rare display of unity, a United Nations group of governmental experts (the GGE), which included representatives of the United States, several other liberal democracies, Russia, China, and several nonaligned countries, drew global attention to this situation in information and communication technologies (ICT).

> The global network of ICTs has become an arena for disruptive activity. The motives for disruption vary widely, from simply demonstrating technical prowess, to the theft of money or information, or as an extension of State conflict. The source of these threats includes non-State actors such as criminals and, potentially, terrorists, as well as States themselves. ICTs can be used to damage information resources and infrastructures. Because they are inherently dual-use in nature, the same ICTs that support robust e-commerce can also be used to threaten international peace and national security.[1]

The GGE then recommended "dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure."[2] Early in the following year, UK Foreign Minister William Hague announced that his country would hold an international conference in London to discuss cyber "rules of the road."

> We believe there is a need for a … structured dialogue to begin to build consensus among like-minded countries and to lay the basis for agreement on a set of standards on how countries should act in cyberspace… To this end, the UK is prepared to host an international conference later this year to discuss norms of acceptable behavior in cyber-space, bringing countries together to explore mechanisms for giving such standards real political and diplomatic weight.[3]

These calls for new rules of the road raised some key questions:

- What behaviors and activities should be subject to proposed norms?
- To whom should these apply? For example, states, their proxies, international organizations, ICT vendors and carriers, other multinational corporations?
- What goals and values should norms seek to realize?
- What are their sources and bases?

[1] "Group of Governmental Experts on Developments in the Field of Information Telecommunications in the Context of Security," United Nations General Assembly, A/65/201, 30 July 2010, http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf, 6.

[2] Ibid,8.

[3] William Hague, "Security and Freedom in the Cyber Age — Seeking the Rules of the Road," speech at Munich Security Conference, 4 February 2011, https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road.

- What norms might be broadly accepted and would their acceptance make a difference?
- How might such norms be enforced?

To address these questions and in the hope of providing input to the London conference, three researchers in cyber policies and politics, based respectively at Harvard, MIT, and the University of Toronto, convened a small workshop on cyber norms that was held at MIT in October 2011. The participants were academics, technologists, government policy-makers, and policy analysts — experts in issues of cybersecurity, or in the development of international norms for threat reduction and social welfare. They came from the United States, Canada, the United Kingdom, and several other liberal democracies. In line with the proposals by the GGE and Secretary Hague, their primary concern was to identify norms or constraints for diplomatic, intelligence, military, and economic (DIME) activities in cyberspace that threaten international stability and security. However, because many activities impinge on cybersecurity and its users' rights, the agenda broadened to include the consideration of norms for assuring the technological foundations of cyberspace, involving non-state actors in cyber defense, protecting online freedom, and reforming Internet governance.

This report summarizes the discussions at that workshop and at a second one that met in September 2012, in advance of the Budapest Cyberspace Conference, the successor to the London conference. It draws upon reports that were compiled immediately after the respective workshops. These were sent to selected policy-makers and delegates to the London and Budapest cyberspace conferences, and posted on the workshops' websites.[4] The discussions were not based on presented papers. Instead, to bridge the diversity of the participants' disciplines, interests, and views, they were organized in a series of ninety-minute sessions, each devoted to a specific issue or topic. In each session, a panel of four to six people first responded to a set of framing questions developed by the workshop-organizing committee and the panelists themselves. After forty-five minutes, the floor was open for other participants to comment and question.[5] To further encourage the exchange of ideas, the workshops were conducted under the Chatham House Rule, which bars quoting or attributing speakers' remarks, and participants were also informed that no report would suggest that the workshops produced a consensus view.

[4] See http://citizenlab.org/cybernorms/ for the 2011 conference and http://citizenlab.org/cybernorms2012/ for 2012. The participants at the workshops are listed on the respective websites.

[5] The framing questions for the sessions are available on the workshops' websites.

These constraints, the format of the workshops, and my reliance on the preliminary reports challenged me to choose between giving a running account of the discussions or condensing similar views on a topic, sometimes allowing the impression that each was expressed by a single speaker. Similar views on a topic are condensed and, when possible, merge discussions from the two workshops that dealt with the same topic. This choice reduces repetition and allows views, ideas, and proposals made at the first workshop to be enriched by thoughts expressed at the second. Consequently, rather than presenting a historical record of the workshops, this report represents their collective thinking on cyber norms. That said, the contexts for such thoughts changed in summer 2013, with the publication of documents that revealed the United States' National Security Agency's (NSA) extensive surveillance of global telecommunications, including the Internet. For some time to come, discussions of cyber norms will inevitably address protection of personal data, privacy, and espionage. Comments are marked off in "update" boxes, to indicate where views based on these revelations significantly qualify or support thoughts expressed at the workshops.

The sections of the report respectively cover:

- What international norms can accomplish, the evolution of western norms and governance for the Internet, and alternatives models for them;
- International law's applicability to cyberspace, with particular attention to the characterization of "cybered" military operations and the Law of Armed Conflict (LOAC);
- Economic espionage and cybercrime, and normative responses to them;
- Assuring the technological foundations and supply chains for cyberspace;
- Norms, principles, and processes for the involvement of non-state actors in cyber defense;
- Internet freedom; and
- Political processes and outlook for the development of cyber norms.

Each section begins with a description of the contexts or challenges that motivate the search for norms to guide or constrain behaviors. It then briefly summarizes discussions that elaborated these challenges, proposed norms, and analyzed whether they could make a difference or identified obstacles to them.

The workshops were possible because of the support and advice of my co-chairs Professors Ronald Deibert and Joseph Nye, the collaboration of the organizing committees, the work of the session chairs, the contributions of the panelists and participants, the help of the staff at the University of Toronto's Citizen Lab and at the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL), and the support of:

- The Belfer Center for Science and International Affairs at the Harvard Kennedy School of Government;
- The Canada Centre for Global Security Studies and Citizen Lab at the University of Toronto's Munk School of Global Affairs;
- Explorations in Cyber International Relations (ECIR), a joint Harvard-MIT research project;
- Microsoft Corporation's Office of Global Security Strategy and Diplomacy (GSSD);
- MIT CSAIL; and
- The John D. and Catherine T. MacArthur Foundation.

This report was particularly enabled by the rapporteurs at the second workshop: Ron Deibert, Nigel Inkster, Eneken Tikk-Ringas, Duncan Hollis, Chris Demchak, and John Mallery; and its note takers, Camino Kavanagh, Tim Maurer, Sarah McKune, and Eneken Tikk. Any mistakes or misrepresentations are mine alone.

Roger Hurwitz
Senior Rapporteur and Co-Chair

ABA Cybersecurity Legal Task Force

The ABA Cybersecurity Legal Task Force is pleased to participate in "A Call to Cyber Norms." The Task Force was created pursuant to the ABA Board of Governors mandate of June 2012 to examine ways to help lawyers protect their practices and their clients' confidential information and intellectual property during events involving cyber attacks as well as position the ABA to contribute to the national dialogue about cyber issues. The Task Force continues to examine where gaps in law and policy exist and what expertise the ABA can contribute to fill the gaps. Co-chaired by Judith Miller and Harvey Rishikof, the Task Force is comprised of representatives from 16 ABA entities having an interest in the cyber domain as well as leaders in the private sector responsible for cybersecurity.

The Task Force has three working groups. The first working group is focused on **Law Firms and Clients**, including internal law firm cyber issues, attorney/client relationships, and the protection of intellectual property. A Cybersecurity Handbook for Lawyers and Law Firms has been developed, which provides cyber threat information; outlines the implications facing lawyers and law firms; and details how best to prepare or respond in the event of a cyber breach.

The second working group is focused on the **Critical Infrastructure Private-Public Relationship**. The primary goal of this working group is to develop in advance potential scenarios and responses for a major cyber emergency. A number of workshops and meeting have been held and a book project on private-public information sharing will be forthcoming.

The third working group is focused on **International Law and Cyber**. The general issues that this subgroup is addressing includes how international law, in particular the *jus ad bellum* and *international humanitarian law*, apply to cyber conflicts and *cyber warfare*. The working group is also examining the law of armed conflict, international data conventions, and international criminal cyber conventions and treaties. We are pleased to participate in this report as part of our program.

Each of these subgroups has the additional objective of thinking about appropriate legislation in their respective areas, identification and dissemination of best practices, and the identification of critical gaps in legal frameworks that require legal expertise to resolve as well as the development of policy recommendations for the ABA House of Delegates. We know this report will constructively add to these conversations.

Judith Miller and Harvey Rishikof
ABA Cybersecurity Legal Task Force Co-Chairs
March 2015

Table of Contents

Chapter 1:
The Evolution of the West's Cyber Norms and Alternative Models

Context

1. The increasing use of cyberspace for military, intelligence, espionage, and criminal activities is a threat to international peace, national security, and societal well being.
2. Existing cyber norms seem inadequate or insufficiently clear and accepted to constrain these activities.
3. Also, the multi-stakeholder model of Internet governance and its institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN), which the West has sponsored, are now being challenged by many states on political, economic, and technological grounds.
4. There are consequently reasons and demands for new normative and institutional orders in cyberspace, but what they might be, how they will be established, and how broadly they will be accepted are open questions.

International norms are shared expectations among states about appropriate behavior. Even when they do not become laws or treaty provisions, norms generally bind states more strongly than do standards for voluntary compliance. When a state accepts a norm it puts its reputation at risk. If it fails to meet the norm, other states will typically demand an explanation or account, rather than ignoring the violation or attributing it to pure self-interest. Governments accept international norms, which may at times constrain their freedom of action, for several reasons: to induce other states to accept the constraints and so increase the predictability of interactions; and to assure support of values to which the state is committed, for example, protection of human rights. A group of states' acceptance of a norm also provides a basis for a state to mobilize sanctions against another state that is seen to violate the norm.

Because the commonly recognized norms for cyberspace were part of the American academic and engineering culture in which the Internet emerged, they are oriented toward technical concerns, particularly interoperability, openness, and information sharing. Similarly, the Internet's multi-stakeholder governance, which involves the private sector and civil society as well as states, reflects 1990s practices when the Internet was just beginning to expand commercially and internationally. There have been efforts since then to create frameworks for cooperation at the regional and even global levels that can deal with certain cyber threats, most notably cybercrime, malware, and disruption of networks. However, the growth in number of Internet users, the increased dependence of societies on it, and the proliferation of means to attack it have created a situation where the existing norms and frameworks seem inadequate to contain or remediate cyber threats. Arguably, new norms are needed to specify the rights, responsibilities, and prohibitions for states and other actors in cyberspace.

> Over the past decade, efforts to combat the threat of cybercrime have been conducted internationally, in particular, within the Shanghai Cooperation Organization, the Organization of American States, the Asia-Pacific Economic Cooperation Forum, the Association of Southeast Asian Nations (ASEAN) Regional Forum, the Economic Community of West African States, the African Union, the European Union, the Organization for Security and Cooperation in Europe and the Council of Europe, as well as through bilateral efforts between States. … Non-criminal areas of transnational concern should receive appropriate attention.
>
> — Group of Governmental Experts on Developments in the Field of Information Telecommunications in the Context of Security, United Nations General Assembly, A/65/201, 30 July 2010, http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf.

The workshop discussions highlighted several approaches to getting such norms:

1. States could *agree that cyberspace is an international commons*, like the sea, air, and space, and adopt laws pertaining to them, with some modifications to accommodate salient differences. For example, while the threshold for "use of force" at sea is intentional damage to property or injury to personnel, major disruptions, without physical damage, in digital networks might have effects that rise to that threshold. If so, causing such disruptions should be prohibited, although they might now be legal under international law. The idea of cyberspace as a commons with rights of passage conceptually fits the traditional view of a "free and open" Internet and the expectation that states and other actors will not interfere with packet flows in their intermediary "hops." Efforts to convince states to agree to this definition could culminate in a grand treaty like the Convention on the Law of the Sea (CLOS). However supporters

of this approach minimize the difficulties in reaching that outcome. They ignore that states are now more inclined to tighten control over their "national cyberspace" than to cede it to a commons, and that unlike other commons, the physical substrate in cyberspace has owners whose property rights also need to be considered.

2. *A piecemeal approach* follows from the recognition that states differ in their visions of cyberspace, especially regarding information access, sovereign authority, and sovereign responsibilities. Also states will differ about the threats they would like an agreement to constrain or proscribe — they do not similarly rank the threats or even have the same set of threats to rank. For example, China and Russia consider the flow of dissident political information as a threat, but don't feel threatened by industrial espionage. The United States supports the information rights of Russian and Chinese dissidents, but feels threatened by industrial espionage. Consequently, there might be very few "pieces" from which this approach can start, but its advocates expect that agreement on such "pieces" can increase trust among states and lead to their agreement on more points. Another aspect of the piecemeal approach involves agreements with different content at regional levels or in coalitions of like-minded states, with efforts to harmonize the differences coming later. A panelist at the second workshop emphasized that states' responses to changes in technologies are often lengthy processes. An important part of these processes is the adoption and defense of limited transnational norms by coalitions of like-minded states. These early actors may become models for other states.

3. Most states might *agree to a minimal set of expectations* for cyber-related behaviors, framed on the order of a "declaration of cyber principles." A panelist noted that this would be unlikely to touch on cyber warfare, cyber intelligence, controls over content, privacy rights, or any other matters related to national security interests. Nevertheless, a declaration could be a vehicle to establish some principles and a basis for having states that subscribe to it being held accountable for certain cyber behaviors, which fulfill or violate them. Aspirational values could be included to serve as a challenge to states for "better behavior." The norms or expectations most likely to be included in a minimal set would be in the area of information and resource sharing in response to humanitarian crises caused by severe disruptions or damage to a country's digital networks. These "lowest common denominator" norms can form the early basis for cooperation, and agreement to them could perhaps be worked through the United Nations Group of Government Experts. Nevertheless,

some participants at the first workshop believed even a minimalist declaration should be more ambitious and address the technology, practices, and purposes of the Internet.

A Minimal Set of Expectations Proposed at the First Workshop

1. Cyberspace should remain open, interoperable, and reliable.
2. All nations have an interest in a clean, healthy cyberspace, and therefore they have a duty to assist, inform, and educate one another.
3. All nations have an interest in a cyberspace that retains the trust of its users.
4. Fundamental freedoms of people for information and connectivity need be upheld.
5. Key international laws, norms, and rules should be extended to cyberspace.
6. Multi-stakeholder stewardship, involving governments, international organizations, and the private sector should shape the development and maintenance of the Internet.
7. Governments should refrain from political interference in technical development and standards for the Internet.

UPDATE: In response to the revelations of the National Security Agency's (NSA) surveillance of global telecommunications, some states have become more inclined to propose limits on state-sponsored political espionage. Brazil and Germany have called upon the UN General Assembly by way of a resolution to declare that "[the GA] is deeply concerned at human rights violations and abuses that may result from the conduct of any surveillance of communications." The resolution will note that these include "extraterritorial surveillance of communications, their interception, as well as the collection of personal data, in particular massive surveillance, interception and data collection." "Brazil and Germany Draft Anti-spy Resolution at UN," BBC News, 1 November 2013, http://www.bbc.co.uk/news/world-europe-24781417.

4. In the Chinese view, the Internet's current norms and its multi-stakeholder governance were developed by and serve the interests of a former hegemonic actor, the United States. China and Russia seek to replace this regime with one in which they and other states would have more authority and a greater role in administering the Internet. Accordingly, in September 2011 they tabled at the UN a "code of conduct" that emphasizes the rights of states in cyberspace, and they backed efforts to give the state-centric International Telecommunication Union (ITU) a role in administering the Internet.

Shaping International Norms to Benefit National Interests

Russia and China are motivated by more than national ego. Both states find the norm of openness inimical to their interest in controlling the information to which their populations are exposed. Besides recognizing the state's jurisdiction over activities on digital networks in its territory or "national cyberspace," the code of conduct would have states, on request, curb information flows from their territory that another government finds hostile. According to a workshop panelist, an expert in Russian cyber policies, Russia's concern for control arises in part from its immediate post-Soviet experience when foreign interests colonized Russian telecommunications. Since the mid-1990s, the Russian security services have led efforts, implemented through law, commerce, and technologies, for the state to retake control of Russia's "information space" in a sphere of influence that encompasses former Soviet states. Russia bolsters these efforts with activities at the international level, which seek acknowledgement of a right to filter content, the establishment of jurisdictional boundaries within cyberspace, and predictability in managing international security issues within the cyber domain.

An expert on Chinese cyber policy added that China shares Russian thinking on information sovereignty — China aims to exercise control of information within its own borders. China's thinking, however, goes further by including a claim that it has the right to attack hostile information sources outside its own borders because such sources can jeopardize China's internal stability. While the Chinese government promoted the Internet's rapid adoption, it also provided a sophisticated suite of techniques for monitoring and controlling Internet activities and content. These steps have created the impression of a lively and unconstrained cyber environment and ensure that China is connected to global cyberspace for purposes of its continued economic development, but they also minimize risk to the regime. China wishes to shape the international information environment through several long-term strategies. These include replacing ICANN with the International Telecommunications Union (ITU); increasing its influence in Internet standards bodies, such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C); and exploiting its dominant position in global mobile telephony manufacture. The Chinese thinking is ultimately grounded in the notion of "informatization," or the use of ICT to act as a force-multiplier across the full spectrum of state activities. The term has a wider strategic significance than is generally appreciated and represents a whole-of-state approach.

While the once-called "non-aligned" or "G77" states also seek a greater role for state officials in Internet governance, they are motivated more by frustration in having been shut out of policy and standard setting, by fears over the militarization of cyberspace, and by economic interests. Some states are primarily interested in restoring the revenue streams that their governments lost as a result of the move in telephony from circuit to packet switching (VOIP) with the Internet's globalization. Consequently, they may be swayed to support the current multi-stakeholder model by arguments that acknowledge these losses and offer some near-term compensation, rather than by appeals to Internet freedom and promises of far-off prosperity. For other states, like India and Brazil, a more important concern is ICANN's legitimacy, given its close ties to the US Department of Commerce. ICANN might successfully respond to that concern if it were to issue unilaterally a declaration of independence from all governments.

> UPDATE: At its meeting in Montevideo, Uruguay, in early October 2013, ICANN did seek to distance itself from the United States government. In its concluding statement, it "expressed strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance." The statement also called for "accelerating the globalization of ICANN and IANA functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing." In March 2014, the US Department of Commerce contributed to this distancing by announcing it did not intend to renew its contract with ICANN in 2015, but to transfer it to some authority constituted by the multi-stakeholder community.
>
> — ICANN, Montevideo Statement on the Future of Internet Cooperation, Oct. 7, 2013. https://www.icann.org/news/announcement-2013-10-07-en; National Telecommunications and Information Administration, United States Department of Commerce, NTIA Announces Intent to Transition Key Internet Domain Name Functions, March 14, 2014. http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

Other panelists noted that the multi-stakeholder model is additionally challenged by technological developments that shift Internet functionality to the local level and hence increase the state's ability to control it. The changes include:

1. The rollout of Internet Protocol version 6 (IPv6), which is energetically promoted by states such as Russia and China and attractive to any state wishing to register domain names in non-Roman scripts. Over time, this could result in the Regional Internet Registries (RIRs) that the Internet Assigned Numbers Authority (IANA) maintains (by agreement with ICANN/IANA), becoming progressively sidelined, while a *de facto* model of state-run domain-name governance takes hold.

> UPDATE: At the Montevideo meeting, ICANN also affirmed that the transition to IPv6 should remain a top priority globally. It added "in particular Internet content providers must serve content with both IPv4 and IPv6 services, in order to be fully reachable on the global Internet."
>
> — ICANN, Montevideo Statement on the Future of Internet Cooperation, Oct. 7, 2013. https://www.icann.org/news/announcement-2013-10-07-en.

2. The emergence of the Internet of Things (IoT) — machines communicating directly without human intervention — has sparked debates on privacy and other issues related to object naming. Who will assign the identifiers? How will information about the object be available? How will information be secured? What will be the ethical and legal framework for IoT control mechanisms? Government-sponsored working groups in the EU and China are already dealing with these issues in a top-down approach that runs counter to the traditional bottom-up practices of Internet governance.

Summary

1. Differences among states' visions for cyberspace and their concerns for national security will preclude any grand treaty similar to the CLOS or agreements for other global commons.
2. Globally accepted cyber norms are likely to be "lowest common denominators," for example, duty to assist in times of massive disruptions of digital networks, or noninterference in most flows.
3. The development of more restrictive norms at bilateral and regional levels and in coalitions of the like minded is possible and important for the long-term development of a new normative environment for cyberspace.
4. The global ICT landscape seems to be in a process of fragmentation. The Internet is becoming subject to greater levels of territorializing, whether it is called balkanization, border controls, or walled gardens.
5. Defenders of multi-stakeholder governance will have to seek support among G77 states, but to win over this constituency, they will have to acknowledge the shortcomings of the current model, take steps to redress its inherent economic and political inequalities, and be willing to take steps to mitigate threats arising out of the Internet's militarization.
6. Proponents of western cyber norms and multi-stakeholder governance have to look beyond challenges of single events, like WCIT, single organizations, like ITU, and single documents, like the code of conduct. They must recognize that the campaign for norms and governance is long term and needs to be pursued on all fronts at all times.

Chapter 2:
The Applicability of International Law to Cyberspace with Particular Regard for Military Operations and the Law of Armed Conflict (LOAC)[6]

Context

1. Existing laws specify neither the types of cyber operations that are grounds for war (*jus ad bellum*) nor constraints on cyber actions in war (*jus in bello*).
2. Governments have avoided setting red lines to avoid exploitation of declaratory policies (by acts below the threshold) or loss of reputation (from failure to retaliate).
3. There are questions whether criteria for "use of force" and "armed attack" in other domains can be applied to the cyber realm in the absence of other guides
4. Previous incidents such as Estonia 2007 and Stuxnet 2010 are not useful guides.
5. The apparent lack of legal clarity regarding military and other adversarial operations in cyberspace can lead to miscalculations, misunderstandings, and escalation.

The emergence of cyber threats and conflicts as major international security concerns has prompted questions about international law's applicability and adequacy in handling them. Some states have called for international organizations to create new legal instruments, while other states have argued that existing legal frameworks can be applied. Although there is no framework of laws specific to cyberspace in the way that maritime law is specific to the sea, a considerable number of legal principles and norms address various aspects and consequences of ICT use. Some deal with the protection of personal, corporate, national, or international interests in the use of ICTs; others take into account how these possibly competing interests can be balanced in providing security. In thinking about the application, extension, or replacement of these laws for cyberspace, it is important to distinguish international law from norms, which are shared expectations among states. International

[6] This section is based on Catherine Lotrionte and Eneken Tikk, rapporteurs, Summary for Panel 3: Applicability of International Law to Cyberspace and Characterization of Cyber Incidents, and Duncan Hollis, rapporteur, Summary for Panel 4: Law of Armed Conflict (LOAC) and Rules of Engagement (RoE) in Cyberspace. Cyber Norms Workshop 2.0, 12–14 September 2012, http://citizenlab.org/cybernorms2012/.

laws are binding rules made by states and derive from predefined sources such as:

- Treaties and conventions — binding, written documents signed by states;
- Customary international law — continuous practices, which are maintained by beliefs among states that they are legally obligated to such behaviors, for example, diplomatic immunity;
- General principles — rooted in the domestic laws of states. For example, the criminalization of murder by most states constitutes a general principle of civilization;
- The writings and teachings of scholars.

Recognized international laws are also subject to different interpretations by states. For example, while states accept that their citizens have freedom of speech, the United States and states in Europe and Asia vary considerably in how they interpret and limit that freedom. So codifying or applying international law for cybersecurity means working with a diversity of legal authorities, instruments, concepts, and practices. Some of these can be applied together and some cannot, but all their applications involve prerequisites. Consequently, the question is how international law will be applied in specific cases, not whether it can be.

Since current international law covers a wide array of issues, including privacy, cybercrime, and telecommunications, the challenge is to apply the laws and principles along the spectrum of cyber conflicts between states as well as non-state actors, like companies and individual users. Most of that spectrum is for incidents that do not approach the threshold of the "use of force" and "armed attack." It is therefore a mistake to focus heavily on questions regarding the legality of certain cyber activities under the UN Charter, whose core function is to deal with threats to international peace and security. By doing so, we may overlook other multilaterally accepted obligations that shape state behavior and whose violations can be a source of conflict, for example, when a state agency hacks a company's network in another country. There are generally accepted rules that can help mark out this spectrum such as rules that obligate everyone — including governments, corporation, and individuals — that processes personal data to protect them to a level corresponding to their sensitivity and rules that indicate the criminal categories and procedures that apply when such protection is broken. However, several large issues can affect the acceptance and use of international law in dealing with actual incidents in cyberspace: sovereignty, the interaction between law and policy/ practice, and the role of treaties.

According to the concept of sovereignty, which dates back to the founding of the modern international system in the Treaty of Westphalia (1648), all states are equal and should be free from external forces interfering in their internal affairs. In a legal perspective, a country has the right to control what it deems to be its own and to exercise such sovereignty to achieve its goals. In practice, the sovereignty it can exercise will depend on the sovereign interests of other states, and also, as international law recognizes, on the need to balance sovereignty against other international principles like human rights. States can consent to give up some exercises of sovereignty to realize systemic conditions or values, and generally such limitations do not happen without their consent. These limitations and other obligations deriving from international law create responsibilities for the state that includes responsibility for violations by entities under its jurisdiction. In the post 9/11 world this concept has been stretched to include a state's responsibility for non-state actors in its territory, which the state might be neither willing nor able to control.

However, most rules that could apply to cyber conflicts have not been tested in practice. A state may anticipate how it would interpret or use rules in a cyber incident, but how it acts in a particular situation might differ from its stated policy because of a perceived need to balance rules representing different interests against one another or to satisfy one interest at the expense of others. When Estonia's networks came under denial-of-service attacks in 2007, its government authorized its law-enforcement agencies to take control of the networks on grounds of national security. This move violated the general principle that privacy and personal data are protected from state infringement under international law, particularly since the attacks did not clearly warrant an exception. In 2010, the Dutch government breached users' privacy by taking over a large botnet's infrastructure and notifying victims around the world that their computers were infected.

These cases also highlight the need for historical perspective in applying international law in cyberspace. The UN Charter, written in1945, did not anticipate nonmilitary threats to international security. Since then many nonmilitary issues have been commonly called matters of security — "securitized" in the language of constructivist theories of international relations — but the circumstances in which international law would consider them as actual threats to a nation's security is a matter for careful review and debate. The prospects of such debates among international lawyers feed many countries' interest in a treaty that specifies what cyberspace behaviors threaten international security.

Yet a treaty can also prove a problem as some cases of international cooperation in dealing with cyber crimes suggest. Many countries have statutes dealing with computer crime and electronic evidence, and these basically agree in defining cybercrime as crime committed against or targeting computers, or committed through the use of computers or information communications technologies. To combat cybercrime, three basic components are required from a legal perspective: agreement about what constitutes substantive offences (hacking, fraud, IP, child porn, etc.); a set of investigative tools that permit obtaining evidence (content and transactional information); and the ability to have meaningful and rapid international cooperation, both formally and informally. The decade-old Budapest convention on cybercrime covers these essential elements, although it needs some updating. Nevertheless, the number ratifying that treaty is unlikely to grow much beyond those forty-two that had done so by March 2014, because of political tensions between North Atlantic countries, which support it, and Russia, China, and nonaligned countries, which consider it regional in character and infringing on sovereignty. This impasse may lead to a greater push for some kind of treaty at the UN level. Or quite possibly, because states recognize that cybercrime is a significant problem, they will put structures in place that reasonably resemble one another's. These could allow them to cooperate internationally, but not as a matter of routine. Similar problems of differing views or political obstacles may prevent widely accepted laws and frameworks for handling other concerns and for addressing conflicts below the "use of force" threshold but still not block cooperation on a case-by-case basis.

A panel on the Law of Armed Conflict (LOAC) made the same point about that law's applicability in cyberspace: it is a matter of *how* it applies, not whether. With the apparent exception of China, all states accept this point. The LOAC is based on the principle that military actions need to be constrained by a) distinction of military personnel and facilities from civilian ones, b) a response's proportionality to the provocation, and c) the action's necessity for the actor's own security. Since these constraints can apply to all means of attack, the LOAC, in principle, can accommodate new military technologies, including cyber ones. Why China is reluctant to affirm it for cyberspace is not clear. Perhaps because so much cyber conflict is below the threshold for LOAC, it believes a specific framework is warranted for cyberspace, or it might have a categorical objection to linking the LOAC to any cyber incident and operation.[7]

[7] The categorical position would be difficult to sustain given that the so-called "Martens Clause" emphasizes that the absence of a cyber-specific provision regarding information technology in an armed conflict does not mean that such technology is automatically permitted. Any use of information technology for military operations would therefore require the same levels of planning and analysis applicable in more conventional contexts.

UPDATE: In the UN GGE's June 2013 report, China agreed with the other fourteen members of the group that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment." Although the LOAC is not specifically mentioned, it is presumably covered by this recommendation.

— Report of the [United Nations] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations, 24 June 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98, 8.

The panel also agreed on the importance of legal thresholds for when LOAC rules apply and, similarly, for when a cyber operation constitutes a use of force. They may be triggered when cyber operations, regardless of methods or effects, are used in concert with conventional armed attacks, but they could also apply when a cyber operation in isolation rises to the level of the effects of an "armed attack" by other means. Military organizations and other actors, however, might adopt different assumptions about which cyber operations constitute armed attacks and which do not. A victim of a cyber operation might view the LOAC as clearly applying, while the perpetrator assumes that the operation was permissible or subject only to domestic criminal law(s).

The importance of the thresholds should spur work on the LOAC's applicability in two directions: developing a typology of cyber operations and technologies to inform analysis of the LOAC's applicability, and having lawyers with expertise in both cyber and the LOAC work out in more detail the LOAC's interpretation and application for cyberspace. Work in the second direction actually began within the NATO community several years ago and has produced the *Tallinn Manual on the International Law Applicable to Cyber Warfare* — a set of rules on the use of force and LOAC in cyberspace. Its express mission was to identify the existing LOAC cyberspace rules, rather than state what the rules should be. Yet the Tallinn Manual is meant only to start the discussion of the LOAC's application, not to end it, so representatives of other countries will need to enter the conversation and broader, non-NATO auspices will be needed. There may also be a need to move the discussion beyond a purely LOAC framework to ensure that the impact of military cyber operations on civilian populations gets considered, even if such operations clearly do not qualify as attacks in the LOAC sense. Of course, one should recognize that legal reasoning alone will not constrain cyber powers: they are unlikely to agree to constraints that they do not find in their interests.

The *Tallinn Manual*, by addressing five critical topics, tries to clarify how the LOAC will work in cyberspace:

1. What constitutes direct participation in hostilities, thereby delineating what civilians can (and cannot do) with respect to military cyber operations;
2. What types of cyber events can constitute “attacks,” including those affecting computer functionality;
3. How the principle of neutrality applies to cyber operations;
4. Whether and how entities deserving special protections under the LOAC, e.g., the Red Cross, must identify themselves in cyberspace;
5. How to treat non-state actor cyber operations and incidents.

Several distinctive features of current cyber technologies have an impact on how the LOAC applies to cyber operations. The most notable is the problem of attribution since much of the application depends on being able to identify the attacker. When the attacker’s identity is unclear, it becomes difficult to know if the LOAC or some other legal regime, for example, domestic criminal law, applies. The second feature is the unpredictability of cyber operations. Since even the most carefully planned operation, Stuxnet, for example, may have unanticipated cascading effects, research is warranted into whether the LOAC’s existing prohibition on a state’s use of indiscriminate weapons can apply to cyber incidents and operations. These considerations prompted several suggestions for making LOAC more practicable and likely to reduce cruelty in cyber space.

Suggested Extensions of the LOAC for Cyberspace

1. States should protect (and not attack) information technology infrastructure itself.
2. Military cyber operations must meet specific functional requirements, for example, any attack must be reversible, if the technology exists to allow reversibility.
3. States need to agree upon and develop means to electronically mark computer systems, networks, and packets deserving special protections, such as hospitals and the International Committee for the Red Cross, that are essential to civilian information flows.
4. Rules of engagement need to ensure that cyber attacks are attributable in some way, for example, digitally signed malware. This would be equivalent to uniforms in cyberspace.
5. States should develop a concept of "cyber peace" (in the sense of geo-strategic stability where actors refrain from disruptive activities) that could be part of future discourse alongside the existing rubrics of cyberwar and cybercrime.

The discussion also raised additional questions on the characterization of cyber operations and the LOAC. Specifically:

- Did Stuxnet constitute a use of force or "armed attack," as the term is used in LOAC? Some workshop participants believed it was neither, while others insisted it crossed both thresholds, but differed on its legality. Some noted that the Stuxnet incident itself might set a precedent, and, in particular, Iran's lack of response might limit future victims' ability to invoke the UN and LOAC frameworks.

- Does a *counterforce* versus *countervalue* distinction apply in cyber operations' targeting? Individuals, corporations, and other nongovernmental groups are frequently victims of cyber operations, but the effects have so far fallen short of those to whom the counterforce/countervalue distinction has been applied historically. In any case, the LOAC does not make such a distinction, but instead uses the principle of proportionality — weighing civilian collateral damage in the context of the military objective achieved. Workshop participants nevertheless thought some "effects test" could be used to assess individual cyber operations and their legality, especially if critical civilian infrastructure was impaired.

- Does its owning or funding networks used by another state for military purposes affect a state's liability or neutrality? If the other state's activity were simply intelligence gathering, it would not trigger the LOAC in contrast to a scenario where the technology was a component of an attack itself. The level of involvement by the owning or funding state does make a difference. Funding activities alone do not make it liable for any damage caused nor can actions of corporations in the state pull it out of neutrality. However, a state is responsible for its own actions and for those of proxies under its effective control.

- Does a state have responsibility for private actors whose technology might raise LOAC questions? Although sales by corporations within a state of technologies that foreign militaries use do not expose that state to LOAC, the issue did provoke discussion on export-control laws and what technology should be openly available in commercial contexts. Participants discussed the implications of corporations themselves playing a military-like role in responding directly to cyber attacks with their own counterattacks.

Summary

1. International laws can be applied to the full spectrum of cyber conflicts — to those below and those rising beyond the threshold of armed conflict.
2. Though providing procedures and remedies, international law is neither the only nor a whole answer for handling a cyber conflict.
3. Foreign policy-makers are likely to be skeptical about the role of international law in addressing a cyber conflict because international law scholars are focused on finding solutions to systemic problems, while the policy-makers focus on advancing their states' objectives in specific situations.
4. On some issues, like cyber espionage or state responsibility for non-state actors, policy-makers will reject frameworks that lawyers propose because they want flexibility over cases.
5. Because law can constrain a state's rivals as well as itself, law can be used to advance a state's national security interests and also win a case, whether in a court or in public opinion.

Chapter 3:
Norms in Response to Cyber Espionage and Cybercrime

Context

1. The proliferation of cyber technologies has enabled espionage and financial crimes on an unprecedented scale. Because these activities can be conducted across national borders, investigating crimes or espionage, identifying perpetrators, and apprehending them require international cooperation.
2. However, frameworks and norms for such cooperation are largely missing. The major existing instrument — the European Convention on Cybercrime — is frequently criticized as ineffective, outdated, or infringing on national sovereignty.
3. Since espionage is not prohibited under international law (although it is illegal under the domestic laws of every state), there is also little existing basis for international cooperation against it.
4. The use of cyber systems in espionage and other intelligence, surveillance, and reconnaissance can easily cross the line between exploit and attack, causing disruption, damage, or loss, and resulting in unintended or unwanted escalation.

Given the traditional understanding that political and military espionage are needed for national security planning and preparation, proposals to restrict espionage, without distinction for industrial espionage, seem to have little chance of gaining traction. There are nevertheless several options for victims of industrial espionage to get other states, especially its alleged sponsors, to consider espionage unacceptable behavior. First, the United States and other victimized states might seek a UN declaration that industrial espionage is illegal under international law because it violates the sovereignty of another state and cannot be justified as anticipatory self-defense. Second, the victims may point out to China and other alleged sponsors that they consider persistent industrial espionage "economic warfare," with repercussions for international security and suggest instead bilateral understandings that would limit its level. A third option, tending in the opposite direction, is for victims to consider incidents of industrial espionage as unfair trade practices and to demand that the World Trade Organization level economic penalties on the sponsors. This approach may require a complaining state to decompose blanket charges of espionage into individual cases, with the result of dissipating some of the grievance, while creating the challenge of providing sufficient, compelling evidence.

Another alternative would be for a coalition of like-minded states to internationalize the investigation, pursuit, and apprehension of perpetrators of industrial espionage. The initiative could be modeled on the “proliferation security initiative” (PSI), whose members undertake to intercept shipments or arrest traffickers of materials contributing to nuclear proliferation. Although some states regard the PSI to be illegal, it has gained the endorsements of nearly one hundred states so that the interception or arrest of proliferators by any one of them is not seen as a unilateral action. A comparable effort for industrial espionage would require the US and other interested countries to have laws enabling them to try foreign nationals and companies in their own courts for economic espionage originating outside their national boundaries. Prosecution of the same suspects by a number of states might suppress espionage and force the World Trade Organization to develop specific rules and remedies for industrial espionage that states could enact, for example, damage awards against offending companies and tariffs against existing states. Such an initiative, however, will have less success in attracting support than the PSI, which addressed the fears of many nations over Weapons of Mass Destruction (WMD), since only the United States and a few other states with major intellectual property stores feel victimized by industrial espionage. Many states will therefore see little gain in antagonizing China, the would-be initiative’s main target, by joining it. The difficulties at this initiative’s operational levels would also be greater than those for the PSI. Attribution problems plague the identification of cyber spies and thieves, and, even when incriminating evidence is available, companies might not press charges for fear of damaging their reputations. In addition, intelligence agencies that may have evidence helpful for prosecuting a case will likely not disclose it in order to conceal their sources or their own espionage activities.

Because of these obstacles, the US and other victim states might gain more from hardening their defenses against espionage, rather than trying to prosecute it. They can encourage or even mandate organizations in their private and public sectors to adopt end-to-end encryption, information sharing, and capacity building to detect espionage. These practices would also reduce other cybercrimes by lessening users’ vulnerability and the expected gains for criminals. Information sharing and a duty to warn (or inform) others of attacks and discovered malware become increasingly relevant with the growth of situations where individuals, organizations, or governments are unaware that a) their information systems are at risk, b) their data have been stolen, or c) new organizational routines can introduce new vulnerabilities. A "duty to warn" is already partly formalized at domestic levels by laws mandating notification of security breaches. Internationally, the duty to warn is being institutionalized through data-sharing procedures among CERTs, and regional organizations of states like NATO. Cloud vendors and tier-1 ISPs, whose operations are not confined to any one state, should also be subject to such norms and laws, although an appropriate supervisory authority is lacking at this time. Because of their alignment with several UN resolutions on building a culture of cybersecurity,[8] information sharing and a "duty to warn" can gain widespread nominal acceptance. However, not all states and organizations will meet these expectations because of their costs, reputational risks, and disclosures of possible improprieties in data collection.

Export Control on Surveillance Technologies

Governments of less developed countries, which conduct surveillance of their own citizens' online activities, usually acquire the needed technologies from more developed countries. On the view that such surveillance threatens people's rights for information, expression, and political association, there have been proposals that technologically advanced states, which are committed to a human rights agenda, impose or broaden existing export controls on these technologies. Such an initiative might prove effective quickly because the technology suppliers are mainly found in a small number of liberal democracies where public opinion in support of such controls can be grown. In some cases, public reports that a company has supplied an obnoxious regime with such technology have already caused the company to claim it has stopped or will stop the supply. At the operational level, however, there needs to be some distinction between "lawful" and "unlawful" use of the technologies so that vendors will cooperate in enforcing the norms rather than evade them in fear of a significant loss of sales.

[8] E.g., UN General Assembly Resolution, "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures," A/Res/58/199, 30 January 2004, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.

UPDATE: In 2013 and 2014, the United States' claims of Chinese espionage against American companies became increasingly prominent in the US-China relationship.

- In February 2013 the American cybersecurity company Mandiant reported, with approval from the White House, a persistent pattern of espionage of over one hundred American companies by a group in Shanghai that is apparently a unit of the Chinese military. Several months of mutual recriminations followed this report, until the US and China moved to ease tensions by establishing a high-level working group to discuss cybersecurity problems and practices.

  — Mandiant, APT1: Exposing one of China's Cyber Espionage Units, Feb. 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

- In its report to the US Congress, the US-China Security and Economic Review Commission (November 2013) noted complaints by various American government organizations, including the Department of Defense, its Defense Science Board, the Justice Department and the House Intelligence committee of Chinese cyber espionage against American defense contractors, penetration of critical infrastructure, and deliberate compromise of Chinese-manufactured cyber equipment.

- The commission also noted that because the Chinese legal system has become more protective of intellectual property rights, a possible US government option is to encourage American companies and individuals to bring cases of cyber theft before intellectual property courts in China.

  — 2013 Annual Report to Congress, 243-248, 255-256. http://www.uscc.gov/Annual_Reports/2013-annual-report-congress.

- On May 20, 2014, the U.S. Attorney General announced the indictments of five Chinese military officers, part of the hacking unit identified in the Mandiant report, for thefts of intellectual property from several American firms. The Chinese government denounced the indictments, denied its involvement in cyber espionage, banned or threatened to ban the government's use of certain American firms' software and Internet services, and suspended its participation in the high-level working group on cybersecurity.

— Summary of the indictment: Dept. of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage. May 19, 2014. http://www.justice.gov/ opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor; for indictment text: http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.

Awareness and encryption — deterrence by denial — are not sufficient to stop cybercrime, and there are several arguments why more activist strategies should be pursued by states acting together. A primary one is that cybercrime organizations breed new attack techniques, which could be unilaterally acquired by a state to the detriment of international security. A second argument is that these organizations' capabilities, when augmented with outsourced specialized skills, can often exceed those of most states to defend themselves. In a more *realpolitik* view, suppressing cybercrime organization — a "draining of the swamps" — might reduce the major cyber-threat actors to a manageable number of state actors, which could impose a regime on the use of cyber weapons.

States whose strategies emphasize international cooperation for the apprehension and prosecution of cybercriminals face the choice of promoting the expansion of the Budapest Convention on Cybercrime or advocating a new treaty. As already noted, the US and other supporters of the convention argue that the convention sets a standard for international cooperation in investigating and prosecuting cybercrime, but only forty-two have ratified the treaty. Its critics find it regional in character, deficient in provisions for handling data, and outdated by the new types of cybercrime. Also many states in the East and South will not join the convention because of its North Atlantic origins. The impasse over a global treaty on cybercrime does not, however, preclude arrangements for cooperation in criminal investigations being developed in the context of bilateral relations and formalized, for example, in extensions of mutual assistance treaties, or practiced on a more informal, *ad hoc basis*. The US and other states, which are zealous in the pursuit of cybercrime, will therefore need to convince states like Russia and China that cooperation is also in their interest, possibly by first seeking cooperation only in cases of major criminality, such as terrorism, or for online activities that are unambiguously criminal (like child pornography) in the respective jurisdictions. Successful instances of cooperation in such cases can provide reusable routines and encourage more cooperation.

Summary

- State-sponsored, cyber enabled economic espionage, a.k.a., intellectual property theft, is a growing concern, but several factors will prevent the emergence of an international norm proscribing its practice.
  - Relatively few nations suffer from it, so most will be reluctant to offend China, at which the norm would be primarily intended.
  - The United States, the primary beneficiary of such a norm, lacks the moral authority to win support for it, when given the Snowden revelations; it is known to practice other types of espionage on a global scale.
  - A state might be reluctant to support such a norm for fear that were it to seek its enforcement by bringing a complaint against another state, before some authority, e.g., the World Trade Organization, it would need to disclose the basis of its attribution.
- It is in most states' interests to cooperate in suppressing cybercrime, because a) cyber criminals in developing techniques that might later be adopted by states contribute to international insecurity and, b) some organizations have the cyber capabilities of threatening vital interests of many states and undermining their domestic security.
- However due to the regional differences and concerns for sovereignty, many states in the global South and East will not sign on to the European Council Convention on Cybercrime (Budapest), which could provide a framework for such cooperation.

Chapter 4: Assuring Technological Foundations of Cyberspace: Security, Resilience, and Integrity in Telecommunications Infrastructure

Context

1. The vulnerabilities of cyber systems are increasing as a consequence of greater system complexity, larger attack surfaces, and mobility of devices.
2. While the cloud has spurred efforts to enhance cybersecurity, it will also lead users to put more of their information assets under the same protective arrangement and so increase their risk to a single (or common) point of failure.
3. The globalization of the cyber supply chain has weakened oversight of the production of hardware and software components. Some consumers consequently fear that certain producers might intentionally introduce vulnerabilities into products for later exploitation.
4. As part of the move to establish their "national cyberspaces," some states may make unilateral decisions on technical standards or network protocols that would affect their networks' interoperability with those in other states, thus putting global interoperability at risk.

At the first workshop, participants from the research community and the private sector emphasized that states, ICT vendors, and carriers have roles in protecting the Internet and need to:

- Recognize the international implications of technical decisions and act with respect for one another's networks and the broader Internet.
- Act to help ensure the end-to-end interoperability of an Internet accessible to all.
- Respect the free flow of information in national network configurations and refrain from arbitrary interference with internationally interconnected infrastructure.
- Act to protect information infrastructures and secure national systems from damage or misuse.

These expectations imply that design decisions should support the soundest technical standards; be transparent with regard to rationales and metrics; introduce no hidden vulnerabilities or Trojans; and have minimal complexity, that is, no unnecessary features that might introduce vulnerabilities. The expectations are also consistent with openness and security for the Internet, which the United States and some other state actors have specified as primary goals for their respective cyberspace strategies."[9]

However, even if the US champions these points, getting them broadly accepted and observed among states will be difficult. Some states will seek standards, network protocols, or computational frameworks that will support their network defenses or control — for example, information filtering — regardless of their impact on openness and transparency. Also, as buyers of ICT equipment, many states and service providers are likely to prove more cost sensitive than security conscious. This assumption is supported by noting that many companies and governments have purchased Huawei products rather than higher-priced competitors' products, despite allegations by the United States that Huawei designs in vulnerabilities that will enable Chinese espionage. (China dismisses these allegations as groundless and intended to create an informal barrier to trade.) The United States and like-minded allies therefore face an uphill battle and considerable expenditure of political capital to gain acceptance of their standards. These costs might, however, be rationalized on grounds that in addition to contributing to online freedom, good ICT standards reduce the opportunities for bad cyber behaviors and thereby contribute to international security.

Possible norms and practices that would contribute to assuring the integrity of the cyber supply chain include:

- Third-party certification of production centers' hardware and software;
- A certification architecture enabling trusted chains of custody for components;
- "Naming and shaming" of insecure producers; and
- Barring their sales to government and defense sectors.

These practices would need to be broadly accepted by consumers to create enough pressure on producers to satisfy them. Since many consumers are more price than security sensitive, governments might need to provide

[9] President of the United States, "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World," May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

incentives to private sector companies to purchase certified products or put taxes on uncertified ones. Once past these start-up costs, the acceptance, sustainability, and effectiveness of such operational norms will depend on educated consumers and a market for quality goods that actually delivers them. Perceptions of better quality, on one hand, and suspicions of possibly compromised ICT, on the other, might then maintain market segmentation for hardware and software. The alternative is for states to have components for military and critical infrastructure systems manufactured under their direct control, as the United States sometimes does and China and Germany plan to do. But many states would be unable to pay the costs or provide the trusted oversight for that option.

The Telecommunications Core

Because telecommunications are an especially critical component of modern societies' infrastructures, the second workshop devoted a panel to cyber threats to infrastructure and norms to protect them. The panel noted that states and non-state actors that seek to project power globally through cyber weapons will likely target the telecommunications core, which includes:

- Terrestrial fiber optic networks;
- Undersea fiber optic cables;
- Network standards enabling their operation;
- Hardware and software supply chains producing the equipment over which the networks run, including monitoring and control systems;
- Key dependency structures such as the Domain Name System (DNS), edge gateways, and Border Gateway Protocol (BGP);
- Carriers, operators, and associated processes, including managed services, personnel, vendors, and partners.

Building on previously proposed norms, the panel argued that the state has a role and responsibility to assure the trustworthiness (their availability, integrity, and confidentiality) of these systems. Due diligence on the part of the state and the private sector companies, which the state regulates, would pertain in part to:

- Defending citizens from malicious actors and violations of privacy;
- Protecting the country's national and economic security; and
- Isolating and mitigating risks to prevent propagation of adverse consequences for allies, friends, partners, and neighbors.

The panel emphasized the importance of security architecture for the telecommunications core, specified its requirements, and reviewed the layers and associated security controls in technical security architectures from the physical communications level through electronic equipment, network operations, cryptographic support, and networking protocols.[10] Part of that review examined how secure DNS can improve the security of core operations, enable broader, more reliable use of cryptography, and enable trust in many new applications. A certificate industry expert noted that in response to recent attacks on certificate authorities (CA), the industry has moved toward a norm of transparency whereby some CA functions are open for audit.

Requirements of Security Architectures for the Telecommunications Core

1. Capability to manage risk through resilience and recovery.
2. A resilience infrastructure that can withstand natural or man-made hazards with minimal interruption or failure.
3. Diverse primary and backup communications capabilities that do not share common points of failure.
4. Redundancy must provide multiple communications capabilities to sustain business operations and eliminate single points of failure.
5. Recovery plans and processes able to restore operations in the event of interruption.

The panelists agreed that strategies to implement a robust security architecture would benefit greatly from research to improve the level of assurance in equipment as well as in operational and maintenance processes of carriers or external service providers. For the carriers, such research would include developing reference security architectures, which integrate risk management across the telecom core ecosystem by identifying interdependencies in their systems and providing strong traceability. Initiatives with significant payoff on this agenda include clean pipes to filter malware at the carrier level, strategies for securing cloud computing connected directly to the telecom core, and enabling trusted Internet connectivity. These would align with the current interests of the sophisticated carriers. To better calculate return on their investments, they are already engaged in modeling the complexities of their systems, understanding socio-technical interactions, developing indices

[10] Based on John Mallery, rapporteur, Summary for Panel 5: Norms for Security, Resilience and Integrity in Telecommunications Critical Infrastructure. Cyber Norms Workshop 2.0, September 2012. http://citizenlab.org/cybernorms2012/.

of cyber protection, and creating quantitative evidence-based measures for the effectiveness of security.

The panel noted that successful implementation of a security strategy needs seamless coordination between public and private actors. Each has different functional roles in the infrastructure — from the supply chain to the operators and service providers and ultimately to the authorities that set standards and provide product certification and attestation. All the while, incentives for industries must remain cognizant of and harmonized with national or supranational regulatory environments. Incentives for implementation might include tax incentives and industry participation in overseeing national infrastructures and decisions about public spending for critical infrastructure protection. As a condition of licensing their operation, governments should also require carriers to produce evidence that they meet national cybersecurity standards for the telecom core. The panel also recommended more specific norms that states should accept to protect their telecommunications cores.

Summary

States’ Due Diligence for Protecting Their Telecommunications Core

1. Assure development and execution of a strategy to security maturity to include
   - threat models — national and international
   - security architecture
   - security strategy

2. Maintain a current security architecture by
   - separating production and operation from certification and attestation
   - assuring independent evaluation, certification, and accreditation
   - continuously monitoring and rapidly mitigating threats, and
   - planning for recovery and continuity

3. Take policy steps to assure
   - manageable complexity in the telecom core
   - alignment of response capability with risk
   - alignment of equipment cost and total cost of ownership with risk reduction

4. Join international efforts for security, e.g., International Cable Protection Committee

5. Encourage development of international best practices such as
   - national telecom cores
   - data sharing and threat mitigation
   - transparency and certification of equipment

6. Develop norms to reduce high-consequence risk
   - Protect against disruption of undersea cables during peace and war.
   - Clarify conditions where international law permits denial of network access and network shaping.

Chapter 5: Norm Development and Practical Issues for Engaging Critical Private Actors[11]

Context

1. Private sector ICT companies and semi-independent agencies, particularly CERTs, have the capabilities to play vital roles in coordinated cyber defense, mitigation, and remediation for cyber attacks. However, regional and global norms are needed to institutionalize such work.
2. In many places, the legal frameworks that facilitate public-private partnerships are rudimentary.
3. Private sector companies' interests may differ from those of governments. As a general rule, companies that operate in multiple states/jurisdictions would like a harmonization of the laws/rules across these locales, whereas governments prefer to make laws/rules as they see fit.
4. Carriers and ISPs activities, such as inspection and clean-up of users' computers, may approximate surveillance or invasion of privacy.

The UN resolution for cybersecurity,[12] various national strategy papers,[13] and even Russia's draft of a Convention for International Information Security[14] expect the private sector to play a significant role in protecting cyberspace. It follows from this that states should be expected to develop organizational frameworks, or at least working relations, with local and international private companies to accommodate their participation in cybersecurity and defense. States accepting this practice as normative can create a "win-win" situation. The companies often have more capabilities and practice in dealing with

[11] Based in part on Chris Demchak, rapporteur, Summary for Panel 6: Cyber Security Awareness and Norm Development: Practical Issues for Engaging Critical Private Actors. Cyber Norms Workshop 2.0, September 2012, http://citizenlab.org/cybernorms2012/.

[12] UN General Assembly Resolution, "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures," A/Res/58/199, 30 January 2004, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.

[13] See the European Union Network and Information Security Agency's (ENISA) collection of national cybersecurity strategies; http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

[14] Foreign Ministry of the Russian Federation website. http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument.

threats in cyberspace; but to be effectively involved in cybersecurity and defense, they will need authorization from states.

The collaborations among ISPs, ICT vendors, some governments, and researchers against Conficker and other recent malware pandemics revealed some respective needs and capabilities. Because of Conficker's extent, the collaboration grew to over one hundred top-level domain operators and Microsoft, in daily touch with ICANN and, less frequently, with governments. These partners implemented an extensive strategy of prevention through blocking botnet command and control (C&C) sites, and remediation measures through disinfecting host computers. However, the collaborations exposed the difficulties of cooperation at the legal and policy levels compared to the relative ease of cooperation at technical levels. In some countries, there was a need to work around legal hurdles, such as contractual barriers to take down, anti-trust laws, and protection of privacy. Similar legal difficulties at the international level were avoided by resorting to coordinated local actions that blocked access to the C&C sites at the name resolution level and did not require any trans-border activity. These were ad hoc and work-around efforts, which do not lend themselves to government-sanctioned institutionalization. Governments in democratic countries may also be reluctant to participate in these efforts because inspection and disinfection of users' computers can create the impression of surveillance, and if the government role in such actions is not transparent, an adverse public reaction can follow.

The organizational form of public-private partnerships that could institutionalize and empower effective cybersecurity collaborations will vary across states. In some European countries, these partnerships are well developed for many sectors and supported by domestic laws. In other countries, ICT trade groups have been set up to share information, but governments have sometimes lagged in connecting to them. Less-developed countries typically lack such partnerships. National and international organizations, with experience in public- and private-sector partnering on economic matters, for example, Asian-Pacific Economic Cooperation (APEC), could improve that situation by guiding and nurturing the growth of partnerships in such places. However, governments and companies might have different visions and timetables for implementing the partnerships. Companies like Goldman Sachs or Lockheed Martin, which operate globally, will want to harmonize the rules across countries, while a government, even if it views itself as an enabler, will face local and legacy issues that might keep it from accepting such norms. Moreover, as some companies that have called for international public-private partnerships recognize, the development of nationally bounded partnerships does not address the problems of international coordination among governments and companies.

Governments face several challenges in making public-private partnerships for cybersecurity the norm rather than the exception: recruiting private-sector participation, stimulating the development of effective metrics, and nurturing information sharing. There are three main groups of private enterprises for recruitment: critical infrastructure industries, IT capital goods providers, and likely victims — the targets of attacks. While the critical infrastructure industries have business models in which the costs of compliance with regulations are part of baseline expenses, the two other types tend to view regulation costs as impairing profits. Consequently, such companies will initially resist the idea of government-mandated security measures. Motivating their acceptance might therefore require them to redefine their profit assessments to explicitly include cybersecurity investments and the return on such investments.

One approach would be to get firms to think systemically rather than individualistically and consequently see cybersecurity as an unavoidable burden that cannot be relieved by passing it along to other parties or ignoring it. A stimulus for that would be publication of data that show how the neglect of cybersecurity by individual firms cumulatively contributes to negative systemic consequences, such as reduced profit, weakened national markets, and constrained options for all firms in meeting foreign competition. Presumably a firm would not want to be later identified as contributing to such results. Other possible stimuli include 1) encouraging firms to include in standard profit-and-loss statements consideration for losses over time due to cyber insecurities inside the firm, across its community, or across its ecosystems; and 2) third parties' apportioning upstream and downstream liability and credits to firms as key nodes and contributors to the cyber (in)security profile of the overall system.

The main goals of these partnerships should include the development of metrics, data, and knowledge-sharing structures that can provide adequate descriptions at the enterprise, sector, and systemic levels. Appropriate metrics can help expose hidden dependencies in a firm's network and information flows, while also supporting multi-stakeholder and collective national strategic assessments. The metrics can also improve the collaborating agents' foresight and situational awareness, increase the transparency of their actions, and assess their respective contributions to security at collective levels. Governments will probably have to take leadership roles in nurturing the development of the metrics because they will likely have a broader, more comprehensive view than individual firms. Similarly, governments will be needed to develop and maintain trusted data-sharing structures. Although private, voluntary associations have developed in some key sectors (e.g., financial services), they have limited views of the security situation or the consequences of their actions outside their sector, and they lack access to government intelligence and other data, which could broaden their views. Since the enterprises will be providing much of the data for aggregation and interpretation, the institutional structures will need to include both private and public actors across a broad catchment.

One model for such structures is the privately managed CERT or computer emergency response team. Although originally limited in mission to knowledge sharing on incidents after their occurrence, CERTs have taken on broader roles in responding to alerts and mitigating cyber attacks and incidents. They will likely evolve toward less-voluntary and more regulatory bodies. Another model proposed at the workshop is a "cyber bridge" or center with personnel seconded from government and the private sector. Knowledge critical for cybersecurity can be exchanged through such a center without revealing sources, methods, or proprietary data. The center could also integrate and forward the data to all parties to alert them of trends and threats. It could also enable sharing knowledge and successful experiences in managing cyber crises.

Summary

- Many private sector companies, particularly critical infrastructure operators, ICT capital goods providers and prime victims of cybercrime, such as banks, can effectively partner with states in providing cybersecurity. For that to become the norm, the states will need to authorize the activities and many companies will need to overcome their regard of security as pure costs.

- The goals of the partnerships should include the development of metrics, data and knowledge-sharing structures. These can
  - expose dependencies in information flows at the firm, sector and national levels;
  - support collective strategic assessments, and
  - assess contributions of respective participants to security at various levels.

- One model for such partnerships are privately managed CERTs, many of which are evolving toward semi-regulatory bodies. Another model is a "cyber bridge" or center with personnel from government and the private sector where knowledge can be exchanged without revealing sources and collection methods.

Chapter 6: The Roles of Non-State Actors in the Development of Norms and Governance

Context

The interests and potential influence of non-state actors in promoting international cyber norms derive from

- The private sector's ownership of the physical substrate of the Internet;
- The governments' dependence on ICT carriers and vendors for maintenance and development of cyber-based operations;
- The vital role of cyber in the economic and social development of societies;
- The interdependence of networks increasing the importance of actors whose capabilities or interests transcend those of national actors.

States, private-sector companies, and civil society organizations as groups differ in their cyber visions, interests, and concerns.

- These differences can lead to proposals and support for competing norms for the same cyber behaviors;
- These differences may also be obstacles to developing coordinated defenses against cyber threats.

Non-state actors have played significant roles in the Internet's technological development and governance, and some have had considerable influence on the cyber policies of democratic states. Currently, many non-state actors, including carriers and ICT vendors, political and social activists, civil society advocates of Internet freedom and privacy, cybersecurity practitioners, and even ethical hackers have existential motives to propose or promote norms for securing cyberspace and maintaining its openness. These conditions can either help assure the actor's existence, help realize its mission or, at the very least, facilitate its online activities. An actor in this position can constitute what media scholar Chris Kelty calls a "recursive public" — a group that is

> vitally concerned with the material and practical maintenance and modification of the technical, legal, practical and conceptual means of its own existence as a public. It is a collective independent of other

> forms of constituted power and is capable of speaking to existing forms of power through the production of actual alternatives.[15]

Because of their involvement with the Internet, which gives them the potential to act online globally, some of these actors have the skill sets as well as the interest to produce alternatives to the current situation in cyberspace — think, for example, of Microsoft's leadership in the fight against Conficker and botnets.

Nevertheless the discussion about non-state actors' roles revealed skepticism that any would become leading proposers or promoters of new cyber norms at a global or regional level. Many non-state actors, most notably private-sector companies but also civil society groups, operate under conditions set by states, and they will likely fear that certain demands, like non-interference in information flows, if made too vigorously, could lead the states to tighten these conditions. Moreover, such actors may have little success in influencing states' cyber policy-makers. Despite cyber interdependence, which has accompanied globalization, on one hand, and the emergence of a global civil society supported by the Internet on the other hand, cyber policy-makers seem much more concerned with pursuing the objectives of their respective states than with improving the general conditions in cyberspace. Their attitude is consistent with the movement, noted elsewhere, toward extending a Westphalian system of states into cyberspace, but it does not bode well for robust norms for international cooperation on cybersecurity or maintaining an open Internet.

The discussion reviewed several other reasons why non-state actors will more likely follow than lead efforts for new norms, namely:

- ***The lack of a common agenda.*** Since national CERTs in various regions of the world have created frameworks and norms for successful collaboration, a global alliance of CERTs might be expected to help shape future behaviors in cyberspace, particularly with regard to information sharing and response to crises. However, a meaningful global alliance is unlikely because the regional frameworks differ in their primary focus. The African CERTs focus on the problem of operating under constraints in funding and capacity, while collaboration among CERTs in Muslim countries primarily concerns handling controversial content. Cybersecurity is a low priority. The Latin American CERT alliance is focused on information sharing to combat cybercrime. Cooperation among Asian Pacific CERTs has been motivated by a shared vision of a clean Internet and focuses on cleaning up botnets.

[15] Chris Kelty, *Two Bits: The Cultural Significance of Free Software* (Durham, NC: Duke, 2008), 3. http://twobits.net/pub/Kelty-TwoBits.pdf.

- ***The fragility of trust among the actors.*** Collaborations in cyberspace are typically built on trust, and trust can suffer when an actor is perceived as acting for the interests of another party rather than for the collaboration. Trust among CERTs, for example, is sometimes threatened by tensions among the states that sponsor them, especially when a national CERT is closely tied to its government. The disclosures about the US's Olympic Games program – the framework for the development of Stuxnet – have raised fears in some CERTs that technical information shared for cybersecurity might be used by a state for military intelligence or economic competition. One response to these disclosures has been discussions among CERTs about a norm of clearly separating "security operations" from the "intelligence and competitive domains" in order to protect the trust basis of collaboration.

UPDATE: The continuing revelations since 2013 of mass surveillance by American, British, Russian and many other state security services emphasizes the importance of this proposed norm and similar ones mentioned elsewhere to protect the integrity of cyber networks and the privacy of individuals. However, the extent of the practices and the respective governments' justifications or implausible denials of them suggest that states will be unlikely to accept or observe such norms.

- ***The inability of most alliances and regional organizations to develop cyber norms because of member states' reluctance to be bound by policies on cyber adopted at that level.*** Intergovernmental organizations, like NATO, will have difficulty in developing an overall vision of cybersecurity and specifying norms or shared expectations according to it. In the case of NATO, one consequence of this lack of vision is the refusal to state what cyber attacks, if any, against a member would invoke a collective security response. The preference is instead to see cyber attacks as matters for consultation on a case-by-case basis, and for member states to support the targeted state at their choosing. In contrast, members of the Shanghai Cooperation Organization (SCO) have been able to agree to norms for collaboration on cybersecurity because of that organization's heavy focus on security cooperation on behalf of national sovereignty and territorial integrity and against the "three evils" of terrorism, separatism, and extremism. While the motive for cooperation is no higher than state interest or regime preservation, the member states' clear, common understanding that each faces similar threats enables them to cooperate. As noted in other discussions, states and non-state actors, which are committed to a free and open Internet, have resisted Russian and

Chinese efforts with the "Code of Conduct" to promote these norms as universal ones.

- ***The lack of incentives for private sector companies to propose, promote or adopt new norms.*** Many organizations, especially those in the private sector, are in a collective action dilemma with regard to leading-by-example efforts to establish new security norms. Although they may recognize that these norms will benefit the general community and themselves as part of it, they know that their actions risk considerable costs. For example, in notifying the public of a security breach it suffered, a company risks damage to its reputation. While this dilemma might be resolved through incentives for taking action (or threat of penalties for not doing so), that solution indicates that companies will likely act only after the norms have been proposed and imposed either by governments or aroused publics. The history of environmentalism suggests a possible trajectory for ICT companies with respect to cyber norms. Many industrial companies, which originally resisted environmental regulations, accepted them and even innovated environmentally friendly practices once public opinion, leverage from investors, or legal action created incentives or pressure to do so. Nevertheless, the involvement of these companies is important even at a later stage because they can use their technical expertise to persuade the undecided and resisters to accept the new norms. Company executives and technical experts who have access to government officials at various levels can also influence change in government policies and their effective implementations.

- ***Organizations in civil society (NGOs), particularly those working for human rights, would like cyber norms and cybersecurity strategies to also protect their online activities, but they lack the credibility and expertise to lead campaigns for such norms.*** NGOs are frequently the target of cyber attacks, and many are now trying to develop cyber hygienic practices that will reduce their vulnerability to them. Broadly speaking, NGOs want liberal governments to include protection of civil society in their cybersecurity strategies, to advocate freedom of information and association online, and to restrain their cyber espionage and surveillance. NGOs might be interested and appropriate members in RAND-like cybersecurity information-sharing and strategy-development centers or in similar public-private partnerships for cybersecurity. They will, however, need invitations from governments to participate. Typically they have not received such invitations, despite third parties, such as Citizen Lab, having highlighted in case studies the relevance of NGOs' experiences for cyber defense and planning.

- ***While there are many "recursive publics" with an interest in establishing norms for behavior and technologies in cyberspace, the great variety in their interests, influence, and means of advocacy precludes their coalescing around a common set of norms.*** Many online communities of interest have stakes in the preservation of cyberspace. Some are criminal in character, while others are grey or white groups that often provide services and innovations benefiting more institutionalized cyber players. These might have some marginal influence in discussions of cyber policies. All the recursive publics are built on in-group trust, whose most basic form online is trust that packets will be delivered to their destinations without interference. This principle is increasingly threatened by state behaviors. Consequently, these groups are likely to become more forceful in advocating for noninterference and also for the survival of the Internet in non-fragmented form, since that is also vital for their own survival. However, to be effective, such advocacy will need to align with the position of some states and major players in the private sector.

- ***Some "recursive publics" can, like certain ICT companies, play important roles in shaping and implementing cyber norms.*** The model of recursive publics is good for thinking about informal groups of highly skilled cyber innovators, and the contribution of their groups' sociality to the technical work they do. As is evident in open-source communities, the members' knowledge of the technical issues, not their institutional positions, generates their trust and respect for one another. Some governments like the United States and the Netherlands have recognized the innovative potential of such groups and have begun funding open-source development of security software and practices. Yet these groups will need to maintain and be seen to maintain independence to be effective and influential on others. An analogy to the Comprehensive Nuclear Test Ban Treaty (CTBT) is useful. For many years, states raised problems of verification to stall progress toward a treaty, but in the meantime scientists were working together to develop a monitoring capability. Once states found a will for a treaty, there was a solution at hand for the verification problem. The application of this practice to cyber might be in a network of groups, including CERTs and some recursive publics, which would monitor the Internet's health. Universities, which enjoy a reputation for academic freedom, could have a critical role in supporting the independence of such a network by hosting some of its member groups.[16]

[16] Per R. Deibert, *Black Code* (Toronto: Signal, 2013), 244: "Universities have a special role to play as stewards of an open and secure cyberspace as 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 planet, university-based research networks could be the ultimate custodians of cyberspace."

UPDATE: Initiatives by two service providers, Google and Microsoft, can be characterized as norm enterprises.

- Google's "Transparency Report," first published in 2010, and appearing regularly since at half year intervals, discloses demands made by governments or other authorities for user data, records, etc., and the company's response (for current reports, see http://www.google.com/transparencyreport/). Other companies, starting with Twitter in 2012, and including Microsoft, Verizon, Apple, Facebook, Yahoo and other major providers, by 2014, have adopted the practice, to the point of such disclosures now being publicly expected.

- Microsoft, in December 2013 published "International Cybersecurity Norms: Reducing conflict in an Internet-dependent world," (http://www.microsoft.com/en-us/download/details.aspx?id=45031) which proposed that states observe six norms to limit conflict in cyberspace:
    - States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.
    - States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.
    - States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.
    - States should commit to nonproliferation activities related to cyber weapons.
    - States should limit their engagement in cyber offensive operations to avoid creating a mass event.
    - States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.

Summary

- Many non-state actors depend on conditions in cyberspace to enable or enhance their activities and some have the capabilities to assure to some extent these conditions. Nevertheless, non-state actors, notably private sector companies but also civil society organizations, are not likely to become cyber norm entrepreneurs.
- Most operate under conditions set by states and can reasonably fear that certain demands, such as non-interference in information flows, could lead the states to set additional constraints.
- The companies and organizations lack a common agenda. Even the agendas of CERTs differ across global regions, and while ICT vendors and carriers might have similar interests they are often in competition with one another. Trust and mutuality are consequentially fragile.
- Regional alliances and organizations are often unable to develop cyber norms because members are reluctant to be bound by policies adopted at the more collective level.
- Very few private sector companies have sufficient incentives to propose, promote or adopt new norms, i.e., the expected value of creating new conditions does not exceed the anticipated costs of the endeavor.
- Organizations in civil society lack the credibility and expertise to lead campaigns for cyber norms that would protect their online activities.
- Nonetheless, some organizations, like universities, and certain ICT companies can play important roles in shaping, promoting and implementing new cyber norms.

Chapter 7:
Internet Freedom and a Global Information Society

Context

1. Since the early 1990s, the United States and its allies have considered freedom of expression and association online the default norms. Those states have only rarely curtailed flows and transactions, for example, online sales of Nazi memorabilia in France and child pornography everywhere.
2. Governments in some democratic states with diverse populations, for example, India, have outlawed or encouraged removal of online information that they consider to incite or contribute to social unrest (e.g., racist speech).
3. Authoritarian, autocratic, conservative, and fragile states have viewed the spread of the Internet and social media as threats because they can support dissent and opposition.
4. Because the Internet has contributed to social and economic development in these states, such regimes have responded by filtering and blocking access to information they consider objectionable, rather than banning the Internet.
5. Regimes have sought to justify their responses by proposing norms that make states the final authority for Internet flows in their territories. They have sought to ground these claims in norms of national sovereignty.
6. The resulting state-centric model for Internet governance now competes for support from states with the multi-stakeholder model that underlies the existing institutions of Internet governance, that is, ICANN and IETF.

In many authoritarian, autocratic, conservative, or fragile states, the penetration of the Internet and social media are considered beneficial for economic and social development, but also as threats to the regimes because they are effective means for dissent and opposition. Rather than totally blocking cyber operations in their territories, many regimes have resorted to filtering information flows, blocking access to hostile sites, or interfering with the use of social media. Such practices, now found in over forty states, are arguably more pernicious than censorship of mass media in cyberspace since they can involve surveillance of interpersonal communications. States have justified these practices on the grounds of sovereignty and national security, with perhaps the most notable of such justifications found in the Code of Conduct, a set of global cyber norms that Russia and China along with two fellow members of the Shanghai Cooperation Organization (SCO) proposed to the UN in 2011. It called for the acknowledgement of states as the final arbiter for networks in their territories. This proposal ignores that citizens have a right to information (i.e., as the Universal Declaration of Human Rights recognizes), so at the very least states need to find some balance between their claims of sovereignty and this right of their citizens. As part of their effort to make sovereignty the controlling value in cyberspace, Russia and China also campaigned to have states give the state-centered International Telecommunications Union (ITU) a role in administering the Internet. They have denigrated ICANN, the Internet's current administrator, as an instrument of American hegemony, rather than an independent agent. Their campaign achieved some success at the World Conference on International Telecommunications (WCIT) in December 2012, when eighty-nine states signed a new international telecommunications treaty that empowers the ITU to play a role in developing the Internet, and sixty other states, led by the US and its allies, walked out in protest of that.

The US and other liberal democracies continue to champion the idea of cyberspace as a domain or ecosystem where freedoms of expression and access to information are norms and where technical and administrative decisions should be free of political interference. Accordingly, they continue to uphold a multi-stakeholder model for Internet governance, which gives the private sector, civil society, and technical experts a voice in making policy and setting standards. Yet the Western democracies have not provided a narrative that will convince states which do not share their values of free speech and association that online freedom and an open Internet architecture are in their best interests. The Chinese model of Internet control, which minimizes the number of international gateways and massively employs firewalls, apparently belies an argument that openness and noninterference are indispensable for cyber development and innovation in a country. The liberal democracies have also not adequately recognized that governments in some states that are ethnically divided and lack traditions of tolerance may fear the Internet more for its potential to destabilize their societies than to overthrow them. Many such states can also dismiss the West's criticisms of Internet filtering and persecution of online activists as selective and hypocritical: such practices by allies, like Saudi Arabia and Bahrain, are ignored, and western governments are known to conduct online surveillance, block sites, and filter for security reasons. Finally, these governments have not proposed a new architecture for cyberspace to counter models being developed by

China and Russia that will facilitate control of cyberspace in their territories, for example, assignment of IP numbers by country- or software-defined networking (SDN). While the current Internet architecture and its institutions have fostered technological development as well as democratic ideals, they are now at the end of their life cycle.

A discussion on governance at the second workshop also noted that states in the global South and East, which support more state-centric institutions, are not necessarily seeking to legitimate online censorship. Instead they may feel that the present administrators do not sufficiently accommodate users in their regions, although the bulk of users are now located there. ICANN and the IETF (Internet Engineering Task Force – the standards-setting body) were not adding members from these regions and were also slow to support the growth in cloud and mobile computing, which is particularly rapid in these regions. Some of these states also view ICANN suspiciously because of its association with the US and their suspicions of US intentions for the development of cyberspace, given its creations of a cyber command and Stuxnet. From this perspective, a governing institution in which each state is theoretically equal would be more likely to resist further militarization of cyberspace.

Summary

1. Finding the appropriate international institutions that states will find legitimate to regulate Internet freedom and dissent has proven elusive.
2. The issue of freedom of expression lies at the heart of democracies; despite different traditions of restraint, the core agreement is that legal processes are required to resolve the debate.
3. The divide between democracies and authoritarian regimes based on what constitutes legitimate dissent reflects core political values.
4. The state-centric model v. the multi-stakeholder model will continue to struggle for primacy.

Chapter 8:
The Outlook for International Cyber Norms

Context

1. The increasing strategic competition among states in and about cyberspace raises questions and doubts about its future development. Will there be generally uniform policies and practices across cyberspace or will the trend toward fragmentation increase with possible effects on interoperability as well as access to information?
2. States and other groups operating at the international level have proposed norms to manage this competition among states. These would define unacceptable cyber behaviors, seek to suppress the creation of cyber vulnerabilities, provide bases for collective cyber defense, and assure individual users' rights. The number of proposals and conflicts among them raise questions about which should have priority for states and other international actors seeking security and cyberspace's beneficial development.
3. There has been little progress at international and regional forums, such as the GGE, the OSCE, and the ARF, toward defining the needed cyber norms, let alone implementing confidence-building measures. Quite possibly the large number of players at these venues prevents significant agreements from being reached. Bilateral and minilateral negotiations might be better ways for major players to define acceptable cyber behaviors toward one another.

Current processes at the UN Group of Governmental Experts (GGE), ASEAN Regional Forum (ARF), and the Organization for Security and Cooperation in Europe (OSCE) have highlighted several possible futures for the Internet and cyberspace in general. It appears that many countries, besides Russia, China, and other SCO members, have thought about establishing their sovereignty in cyberspace and have begun moving beyond asserting this goal at a policy level to implementing at an engineering level, through access controls, filtering, etc. A more "balkanized" Internet can therefore be expected. The state-level fragmentation may be compounded by certain IT vendors and carriers pursuing walled-garden strategies, that is, the creation of mini cyber ecosystems in which users' experience of cyberspace is supported entirely by a vendor's applications and services. In both cases, interoperability is no longer as highly valued a norm. These strategies respond to insecurities, bred by the political and commercial competitions, that an open Internet fosters.

However the somewhat pejorative term *balkanization* to indicate a future of varying standards of acceptable cyber behaviors is probably not helpful in describing positions in the debate over norms. Only Western officials and commentators use the term, while elsewhere the setting of local standards is called "extending national borders into cyberspace," without a sense that doing so betrays some ideal or norm. States that are trying to create these borders are not planning to delink from the Internet, but to remove from the networks whatever they find objectionable, without having to answer to anyone. The associated demand for more state-centric governance of the Internet does not seek an entire break with the past by totally displacing the multi-stakeholder model. Even the statist ITU is multi-stakeholder after a fashion, since it's working and advisory groups include representatives of the private sector as well as government officials. Thus a more realistic challenge for the Western allies is to redefine their expectations of an open Internet and multi-stakeholder governance to provide a broadly acceptable alternative that acknowledges but limits national governments' control of cyberspace.

Moreover, fragmentation does not necessarily mean deterioration in international cybersecurity, although it does suggest that cooperation at the regional or global level would be more difficult. Improvements in cybersecurity technologies will arguably raise the costs and capabilities needed for effective exploits and attacks, and the major cyber powers will have an interest in keeping the barrier to entry high to assure greater predictability and control of their environment. To do so, they will need to create a consensus on the following:

- The Law of Armed Conflict (LOAC) applies to cyberspace, so there will be limits on these states' aggressive cyber behaviors.
- Offensive capabilities that would undermine the technological foundations of the cyber ecosystem should not be developed or, if developed, not used.
- Certain design principles should be basic and common to offensive capabilities, possibly including watermarking or digital signatures, reversibility, and kill-switches so that attacks by the major powers can be unambiguously attributed and stopped when they go beyond their intended goals.

UPDATE: Since the 2012 workshop, some progress was made in meeting the above conditions.

- **LOAC:** The GGE agreed in its signed June 2013, report that international law, including by implication the law of armed conflict, does apply to cyberspace. China was party to this agreement, although it had previously been vague on this matter and, since then, it has been rumored to be reconsidering this view.

  — Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations, 24 June 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

- **Building Trust:** Members of the OSCE, including the Russian Federation, agreed in December 2013, to confidence building measures centered on the sharing information on cyber threats, voluntary disclosures of member states' measures "to ensure an open, interoperable, secure, and reliable Internet," consultations to avoid misperceptions of certain national cyber programs as threats, and the establishment of contact points.

  — Organization for Security and Co-operation in Europe, Organization for Security and Co-operation in Europe. Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies. Decision no. 1106, Dec. 3, 2013. http://www.osce.org/pc/109168

- **Proliferation:** Also in December 2013, members of the Wassenaar Arrangement agreed to voluntary export controls on deep packet inspection (DPI) and network surveillance equipment that "under certain conditions, may be detrimental to international and regional security and stability."

  — Public Statement of the of the 2013 Plenary Meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Technologies. http://www.wassenaar.org/publicdocuments/2013/WA%20Plenary%20Public%20Statement%202013.pdf.

With respect to acceptance of a norm to **preserve the integrity of the technological foundations of cyberspace** there may have been a retreat. The Snowden revelations have included allegations that the NSA influenced the adoption several years earlier of a cryptologic standard that can be cracked. To the extent this is believed, some states might insist that entities, that operate in their territories use "national" encryption standards, which could also similarly exploited.

- The major actors should enforce nonproliferation of significant offensive capabilities to other actors, but can delegate the regulation of lesser capabilities to a broader group of actors.
- The major actors need to develop, most probably through bilateral and small group meetings, a robust set of confidence-building measures that will help preserve trust among them.

However, some commenters expressed doubt that cyber defense would match offence in the way this view foresees. Several thought that clouds would be large, vulnerable targets; they could be easily captured and used in attacks on other cyber facilities. One discussant conceded that research and better organization practices would raise the threshold for exploitation, but did not think this would change the offence-defense balance because the "Internet of Things" and other new ICT developments would introduce new vulnerabilities. Another agreed that the "big players" could be expected to act rationally, but was less certain about how smaller states would behave if they acquired high-end offensive capabilities. An effective nonproliferation regime would therefore be key for realizing international cybersecurity. It would need to be based on studies of how cyber knowledge proliferates and would have to include means of keeping high-end hacker knowledge secret.

In another view, fragmentation could be an obstacle to the broad international cooperation that is needed to deal with three persistent and significant cyber-based threats to states:

- The lack of clarity regarding what rules of international conduct apply in cyberspace, particularly with regard to conflicts, and a lack of consensus on where clarity is lacking;
- The exposure of critical infrastructures to cyber attacks which might cause more disruption and collateral damage than physical attacks;
- The cyber-enabled theft of intellectual property from technologically developed states and its economic consequences for these states. Some states, most notably Germany, have proposed that states should affirm that systematic economic espionage can constitute a violation of a target state's sovereignty and that states can be held responsible for such espionage originating in their territories.

The GGE can be an appropriate and possibly productive forum for the first threat — for clarifying *how* international rules, including the laws of war, apply to cyberspace. There is also now a good chance that governments, represented by the GGE experts, can agree on a number of confidence-building measures (CBMs). To some extent, Russia and China have accepted the Western democracies' agenda on these points, and Russia has agreed to use the term *cybersecurity* as distinct from *information assurance*. However the GGE is not the place to discuss protection of critical infrastructures through technological and policy measures, and it is probably not useful for the discussion of economic espionage.

Some comments faulted the view that states alone will determine the norms, governance, and development of cyberspace as too narrow. Since the development and adoption of international norms has many influences and agents, there is a need for broad participation in the conversations on cyber norms and for them to move beyond their current legalistic character. Those who are trying to preserve the current institutions and practices of cyberspace should consequently focus their arguments on the private sector and civil society as well as on emerging powers like India, Brazil, and South Africa and other states that have not yet decided on these issues. The arguments should describe the model's benefits for security and economic development, rather than refight Cold War ideological battles. The democratic and bottom-up character of the western norms could be emphasized in conversations with nongovernmental actors who might be more ready than the governments to push for the acceptance of such norms (because of the protection they offer against possible government efforts to limit their use of cyberspace). Thus, it is important to understand the subnational as well as national audiences that can influence the conversations about norms and to recall that people now active in these subnational networks may be their states' future decision makers.

A more pessimistic outlook highlighted the significance of the Internet demographics' major shift from users in the North Atlantic community to the majority now in the global East and South. The countries in these regions have different cultural and religious traditions that are less tolerant of difference than that in which the Internet took shape, and in some countries the diversity of populations is also a source of social tension. So Internet freedom, which is the norm in the West, is often a challenge or threat to governments and societies in the East and South. In addition, many countries there are also beset by organized crime, which uses digital media to organize its activities and may also engage in cybercrime. There is consequently considerable pressure on states to control activities and information in cyberspace, and they may be understandably reluctant to relinquish whatever actual control they have to satisfy norms that support users' privacy and access to information. According to one discussant who is familiar with the discussions in the GGE, none of the experts from nonaligned states engaged in debate about security norms or information rights, and international cybersecurity does not seem to be their leading concern. They are more concerned about issues that affect them on a daily basis, such as cybercrime.

From this perspective, one needs to think about the domestic implications of decisions and norms that are made at the international level. The present calls for greater cybersecurity will likely prompt realist approaches in many states, especially those where regimes regard cybercrime and online political dissent with equal suspicion. That is, there will be more selective control, filtering, surveillance, and suppression of cyber activities behind a wall of secrecy. There can, of course, be a more liberal response to cybersecurity, based on core principles such as the separation of government powers and respect for human rights. The multi-stakeholder institutions in principle support this liberal approach but their survival is uncertain in the face of states' efforts to create and control national cyberspace.

UPDATE: In its Statement on behalf of multi-stakeholder governance, the Netmundial Conference, which met in Sao Paolo, Brazil, April 22-24, identified five stakeholder groups: governments, the private sector, civil society, academia and the technical community. It asserted that online rights include freedoms of expression, association, information and access to information, privacy, accessibility and development. "Security, stability and resilience of the Internet should be a key objective of all stakeholders in Internet governance." The governance process should ensure the participation of all stakeholders, be open, transparent, collaborative, consensus driven, and equitable. Matters of cybersecurity, such as jurisdiction, law enforcement, cybercrime prevention and digital threats need to be addressed in a multi-stakeholder manner, involving "appropriate collaboration among governments, private sector, civil society, academia and technical community."

Although the conference originated as part of Brazil president's angry response to the Snowden revelations regarding the NSA's online surveillance, its final statement indicated that this practice and other controversial issues such as net neutrality required more discussions at the international level to reach common understandings among stakeholders on appropriate norms.

— NETmundial Multi-stakeholder Statement, April 24, 2014. http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

Epilogue

The June 2013 report by the UN GGE begins by reviewing the response to its call in 2010 for states to enter a dialogue on cyber norms in order to reduce collective risk and protect critical national and international infrastructure. It found that:

- States have undertaken numerous initiatives in bilateral and multilateral contexts and at international forums to enhance cybersecurity in order to improve their security and global stability.
- States recognize that they have an interest in promoting the use of ICTs for peaceful purposes and in preventing conflicts arising from their use.
- States recognize that common understandings on norms, rules, and principles applicable to cyberspace can play an important part in advancing peace and security.

The report provides recommendations on the development and content of norms, rules, and principles of responsible behavior in using ICTs. These are significant because they reflect a consensus among states with diverse ideologies and cyber capabilities – one that the UN General Assembly could later endorse.[17] The recommendations read like a pastiche, saying, in effect, “this but also that,” rather than definitely siding with one or another view on matters of controversy. Nevertheless, there were many and some surprising points of agreement.

With regard to process, the report affirms that states must lead in developing a common understanding, but adds that the participation of the private sector and civil society would benefit the undertaking. The United Nations should play a leading role in facilitating the dialogue needed among member states, and can be assisted by work at regional forums and international organizations, such as the African Union, ASEAN, APEC, EU, and SCO.

With regard to the content of the norms, the report:

- Recommends the application of norms derived from relevant existing international law to cyberspace but adds that further study is required to determine how the norms should apply, and that given the attributes of cyber technologies, more norms could be developed over time. The main statement reflects the Western position, while the qualifications accommodate the Chinese view of cyberspace as such a different domain that it requires laws of its own.

[17] The members of the GGE issuing the report were Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, the UK, and USA.

- Finds that the UN Charter applies to cyberspace and is essential to maintaining peace and an open, secure, and accessible online environment. This implies that certain behaviors can violate the peace and constitute use of force, but they are not specified.

- Takes note of the "Code of Conduct," without endorsing it.

- Affirms a state's sovereignty and jurisdiction with regard to the conduct of ICT activities within its territory, but adds that a state's efforts at cybersecurity must "go hand in hand" with respect for human rights and freedoms as stated in the Universal Declaration of Human Rights and other international instruments. These provisions attempt to balance the liberal democracies' emphasis on information rights in cyberspace with authoritarian states' use of sovereignty and security as the basis for surveillance and interference in information flows.

- Recommends that states increase their cooperation against criminal and terrorist use of ICTs, with harmonization of legal approaches and collaborations among law-enforcement and prosecutorial agencies.

- Declares in effect sovereign responsibility for cyber acts attributed to a state or originating in its territory. A state should cooperate in the investigation of wrongful cyber behaviors attributed to it, should not use proxies for such behavior, and should seek to prevent non-state actors from using its territory for such behaviors. This somewhat surprising agreement on the extent of a state's responsibility will raise the bar on "plausible deniability" of cyber exploits and attacks.

- Recommends that states encourage the private sector and civil society to participate in improving cybersecurity, including supply-chain security. This provision acknowledges roles for public-private partnerships but seems to anticipate that they'll be state led.

The report also has recommendations on confidence-building, information-sharing, and capacity-building measures. It concludes with the recognition that international cybersecurity is a work in progress and each step will have to build on what has already been achieved. According to the GGE, a technological environment in which new users and applications are continually added requires this "iterative approach." So no set of rules or norms instituted all at once could possibly be adequate. Perhaps this view also foresees how the differences among states that suggest different norms or priorities for them will not be resolved soon.