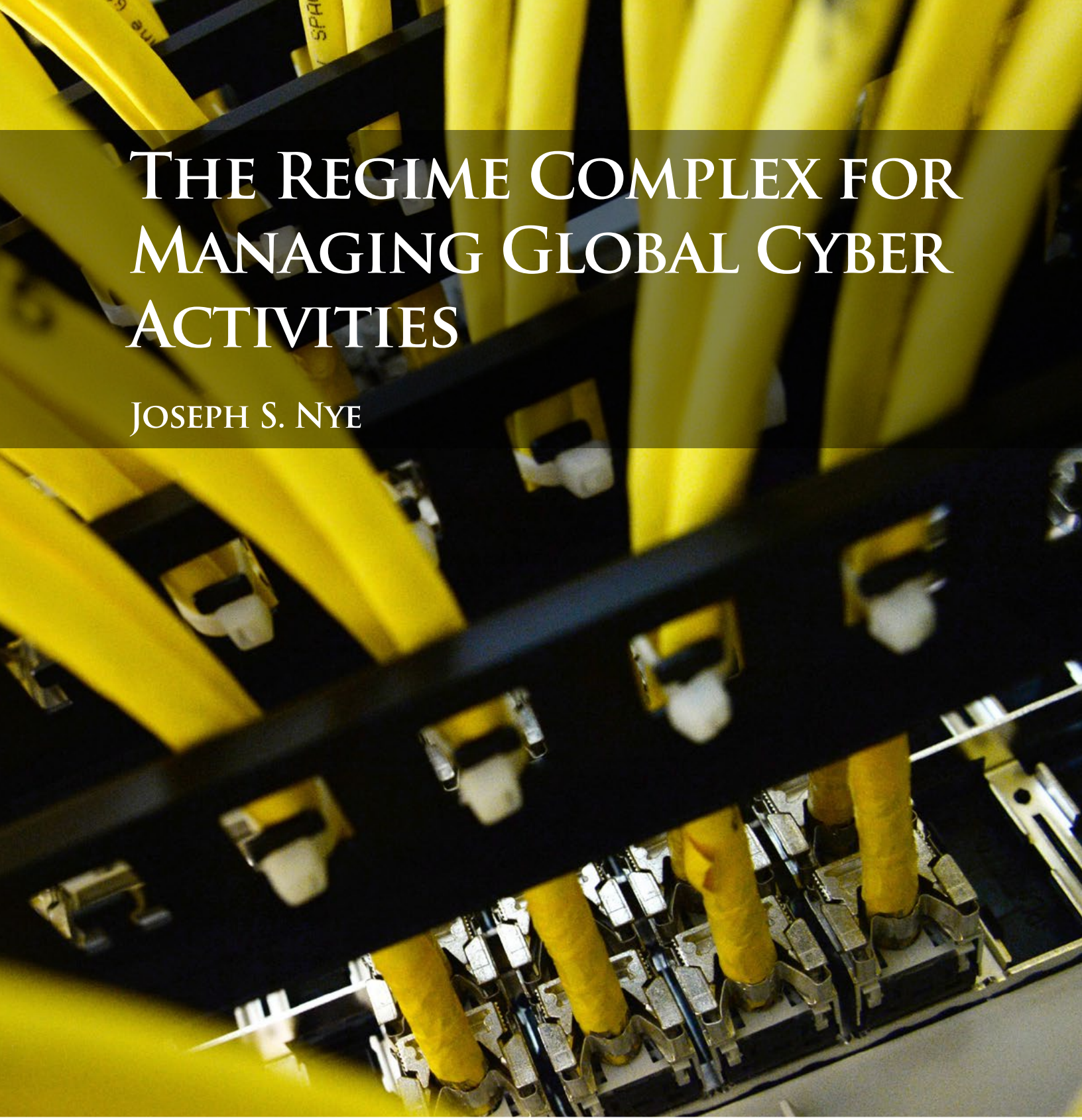


The Regime Complex for Managing Global Cyber Activities

Joseph S. Nye

HARVARD Kennedy School
Belfer Center for Science and International Affairs

November 2014

Belfer Center for Science and International Affairs

John F. Kennedy School of Government
Harvard University
79 JFK Street
Cambridge, MA 02138
Fax: (617) 495-8963
Email: belfer_center@hks.harvard.edu
Website: http://belfercenter.org

This paper was originally published by the Centre for International Governance Innovation and the Royal Institute for International Affairs as Paper No. 1 in the Global Commission on Internet Governance series.

Cover photo: An illustration dated July 2013 shows ethernet cables inside a server room in Berlin, Germany. (Matthias Balk/AP)

The Regime Complex for Managing Global Cyber Activities

Joseph S. Nye

HARVARD Kennedy School
Belfer Center for Science and International Affairs

November 2014

About the Global Comission on Internet Governance

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- Enhancing governance legitimacy —including regulatory approaches and standards
- Stimulating economic innovation and growth —including critical Internet resources, infrastructure and competition policy
- Ensuring human rights online —including establishing the principle of technological neutrality for human rights, privacy and free expression
- Avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy- oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

About the Author

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

Acknowledgements

I am indebted to Amelia Mitchell for research assistance, and to Laura DeNardis, Fen Hampson, Melissa Hathaway, Roger Hurwitz, Robert O. Keohane, Alexander Klimberg, John Mallery, Bruce Schneier and Jonathan Zittrain for comments.

Acronyms

CERTs	Computer emergency response teams
CSIS	Center for Strategic International Studies
DDoS	Distributed denial-of-service
DNS	Domain name addresses
GATT	General Agreement on Tariffs and Trade
GGE	Group of Governmental Experts (UN)
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ICANN	Internet Corporation for Assigned Names and Numbers
ISOC	Internet Society
ISP	Internet service provider
ITU	International Telecommunication Union
LOAC	Laws of Armed Conflict
NSA	National Security Agency (US)
W3C	World Wide Web Consortium
WCIT	World Conference on International Telecommunications
WGIG	Working Group on Internet Governance
WIPO	World Intellectual Property Organization
WTO	World Trade Organization

Table of Contents

Introduction

When we try to understand cyber governance, it is important to remember how new cyberspace is. "Cyberspace is an operational domain framed by use of electronics to...exploit information via interconnected systems and their associated infra structure" (Kuehl 2009). While the US Defense Department sponsored a modest connection of a few computers called ARPANET (Advanced Research Projects Agency Network) in 1969, and the World Wide Web was conceived in 1989, it has only been in the last decade and a half that the number of websites burgeoned, and businesses begin to use this new technology to shift production and procurement in complex global supply chains. In 1992, there were only a million users on the Internet (Starr 2009, 52); today, there are nearly three billion, and the Internet has become a substrate of modern economic, social and political life. And the volatility continues. Analysts are now trying to understand the implications of ubiquitous mobility, the "Internet of everything" and analysis of "big data." Over the past 15 years, the advances in technology have far outstripped the ability of institutions of governance to respond, as well as our thinking about governance.

Since the 1970s, political scientists have looked at the international governance processes of various global affairs issues through the perspective of regime theory (Keohane and Nye 1977; Ruggie 1982). This paper is a mapping exercise of cyber governance using regime theory. Regimes are the "principles, norms, rules and procedures that govern issue areas in international affairs," but these concepts have rarely been applied to the new cyber domain (Krasner 1983). In its early days, thinking about cyber governance was relatively primitive.

Ideological libertarians proclaimed that "information wants to be free," portraying the Internet as the end of government controls. In practice, however, governments and geographical jurisdictions have been playing a major role in cyber governance right from the start (see Goldsmith and Wu 2006).

Cyberspace is a unique combination of physical and virtual properties.[1] The physical infrastructure layer largely follows the economic laws of rival resources and increasing marginal costs, and the political laws of sovereign governmental jurisdiction and control. The virtual or informational layers have economic network characteristics of increasing returns to scale, and political practices that make government jurisdictional control difficult.[2]

Attacks from the informational realm, where costs are low, can be launched against the physical domain, where resources are scarce and expensive. Conversely, control of the physical layer can have both territorial and extraterritorial effects on the informational layers.

Governments and non-state actors cooperate and compete for power in this complex arena. Cyber power can be defined in terms of a set of resources that relate to the creation, control

[1] Martin Libicki (2009, 12) distinguishes three layers of cyberspace: physical, syntactic and semantic. However, with applications added upon applications, the Internet can be conceived in multiple layers. See Blumenthal and Clark (2009, 206ff) for a four-layer model. Nazli Choucri (2012) has also proposed multiple layers.

[2] Jonathan Zittrain points out that may change as unowned apps, such as email, give way to proprietary apps, such as Facebook or Twitter direct messaging (pers. comm.).

and communication of electronic and computer-based information — infrastructure, networks, software and human skills. This includes the Internet of networked computers, but also intranets, mesh nets, cellular technologies, cables and space-based communications. Cyber power can be used to produce preferred outcomes within cyberspace, or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace. The Internet, which is a network of thousands of independently owned networks, is only part of cyberspace. Cyber attacks can come through several vectors, such as humans and hardware supply chains, as well as malware delivered over the network. Internet governance is the application by governments, the private sector and civil society of principles, norms, rules, procedures and programs that shape the evolution and use of the Internet (Working Group on Internet Governance [WGIG] 2005). Naming and numbering is only a small part of Internet governance, and while Internet governance is at the heart of cyberspace, it is only a subset of cyber governance.

Aspects of Cyber Governance

There is considerable insecurity in cyberspace because the barriers to entry are low and offence is often cheaper than defence, which is why it is sometimes depicted as analogous to the ungoverned and lawless Wild West. In practice, however, there are many areas of private and public governance. Certain technical standards related to Internet protocols are set (or not) by consensus among engineers involved in the non-governmental Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C) and others. Their informal procedures eschew voting and are sometimes summarized as "rough consensus and running code."

The determination as to which of these standards is broadly applied often depends upon private corporate decisions about their inclusion in commercial products. Private contracts among different tiers of Internet service providers (ISPs) use BGP (border gateway protocols) and undersea cables to connect the many networks that make up the Internet. The Internet Corporation for Assigned Names and Numbers (ICANN) has had the legal status of a non-profit corporation under US law, although its procedures have evolved to include government voices (but not votes). In any event, its mandate is limited to domain names and assignment of top-level numeric addresses, not the full panoply of cyberspace governance. National governments control copyright and intellectual property laws, although they are subject to negotiation and litigation, sometimes within the frameworks of the World Intellectual Property Organization (WIPO) and the World Trade Organization (WTO). Governments also determine national spectrum allocation within an international framework negotiated at the International Telecommunication Union (ITU).

The United Nations Charter, the Laws of Armed Conflict (LOAC) and various regional organizations provide a general overarching framework as national governments try to manage problems of security and espionage. The Council of Europe's Convention on Cybercrime in Budapest provides a legal framework that has been ratified by 42 states. Incident response teams (computer emergency response teams [CERTs] and CSIRTs [Computer Security Incident Response Teams]) cooperate regionally and globally to share information about disruptions. Bilateral negotiations, track two dialogues, regular forums and independent commissions strive to develop norms and confidence-building measures. Much of the governance efforts occur within national legal frameworks, although the technological volatility of the cyber domain means that laws and regulations are always chasing a moving target.

The cyberspace domain is often described as a public good or a global commons, but these terms are an imperfect fit. A public good is one from which all can benefit and none can be excluded, and while this may describe some of the information protocols of the Internet, it does not describe the physical infrastructure, which is a scarce proprietary resource located within the boundaries of sovereign states and more like a "club good" available to some, but not all. And cyberspace is not a commons like the high seas, because parts of it are under sovereign control. At best, it is an "imperfect commons" or a condominium of joint ownership without well-developed rules (pers. comm. with James A. Lewis; see Center for Strategic International Studies [CSIS] 2008). It has also been termed a club good where a shared resource is subject to various degrees of exclusion according the rules and agreements of different institutions (Raymond 2013).

Cyberspace can also be categorized as what Elinor Ostrom termed a "common pool resource," from which exclusion is difficult and exploitation by one party can subtract value for other parties.[3] Government is not the sole solution to such common pool resource problems. Ostrom showed that community self-organization is possible under certain conditions. However, the conditions that she associated with successful self-governance are weak in many parts of the cyber domain because of the large size of the resource, the large number of users and the poor understanding of how the system will evolve (among others).

In its earliest days, the Internet was like a small village of known users — an authentication layer of code was not necessary and development of norms was simple in a climate of trust. All of that changed with burgeoning growth and commercial use. While the openness and accessibility of cyberspace as a medium of communication provide valuable benefits to all, free riding behaviour in the form of crime, attacks and threats creates insecurity. The result is a demand for protection that can lead to fragmentation, "walled gardens," private networks and cyber equivalents to the 17th-century enclosures that were used to solve that era's "tragedy of the commons" (Ostram 2009, 421; Hurwitz 2009). Internet experts worry about "balkanization" or fragmentation. To some extent that has already occurred, yet most states do not want fragmentation into a "splinternet" that would curtail economic benefits.

Providing security is a classic function of government, and some observers believe that growing insecurity will lead to an increased role for governments in cyberspace. Many states desire to extend their sovereignty in cyberspace, seeking the technological means to do so. As Diebert and Rphozinski (2010) put it, "securing cyberspace has definitely entailed a 'return of the state' but not in ways that suggest a return to the traditional Westphalian paradigm of state sovereignty." Moreover, while accounts of cyberwar have been exaggerated, cyber espionage is rampant and more than 30 governments are reputed to have developed offensive capabilities and doctrines for the use of cyber weapons (Rid 2013). US Cyber Command has announced plans to employ 6,000 professionals by 2016 (Garamone 2014). Ever since the Stuxnet virus was used to disrupt Iran's nuclear centrifuge program in 2009 and 2010, the hypothetical use of cyber weapons has become very real to governments (Demchak and Dombrowski 2011, 32).

[3] See Ostram et al. (1999, 278), for a challenge to the Garrett Hardin's (1968, 1243) formulation of "the tragedy of the commons."

Efforts to attack or secure a government network also involve the use of cyber weapons by non-state actors. The number of criminal attacks has increased with estimates of global costs ranging from US$80-400 billion annually (Lewis and Baker 2013, 5). Corporations and private actors, however, can also help to protect the Internet, and this often entails devolution of responsibilities and authority (Deibert and Rohozinski 2010, 30; see Demchak and Dombrowski 2011). For example, banking and financial firms have developed their own elaborate systems of security and punishment through networks of connectedness, such as depriving repeat offenders of their trading rights, and by slowing speeds and raising transactions costs for addresses that are associated with suspect behaviour. Informal consortia, such as the Conficker Working Group, have arisen to deal with particular problems, and hacker groups like Anonymous have acted to punish corporate and government behaviour of which they disapprove.

Governments want to protect the Internet so their societies can continue to benefit from it, but at the same time, they also want to protect their societies from what might come through the Internet. China, for example, has developed a firewall and pressures Chinese companies to self-censor behind it, and the country could reduce its connections to the Internet if it is attacked (Clarke and Knake 2012, 146). Nonetheless, China — and other governments — still seeks the economic benefits of connectivity. The tension between protection of the Internet and protecting society leads to imperfect compromises (see Zittrain 2008). Reaching an agreement on norms to govern security is complicated by the fact that while Western countries speak of "cyber security," authoritarian countries such as Russia and China refer to "information security," which includes censorship of content that would be constitutionally protected in democratic states.

These differences were dramatized at the December 2012 World Conference on International Telecommunications (WCIT) convened by the ITU in Dubai. Although the meeting was ostensibly about updating communications regulations, the underlying issue was the extent to which the ITU would play a role in the governance of the Internet. Authoritarian countries, and many developing countries, feel that their approach to security and development would benefit from the UN bloc politics that characterizes the ITU. Moreover, they dislike the fact that ICANN is a non-profit incorporated in the United States and at least partially accountable to the US Commerce Department. Western governments, on the other hand, fear that the state-centric features of the ITU would undercut the flexibility of the "multi-stakeholder" process that stresses the role of the private and non-profit sectors as well as governments. While there are different interpretations of multi-stakeholderism, which can be traced back to the Geneva and Tunis meetings of the UN's World Summit on the Information Society in 2003 and 2005 (Maurer 2011), respectively, the vote in Dubai was 89 to 55 (Klimburg 2013, 3) against the "Western" governments. In the aftermath of the WCIT conference, there were articles about the crisis in Internet governance and worries about a new Cold War (see Klimburg 2013; Mueller 2012). Many of these fears were overstated, however, if one looks at cyber governance through the lens of regime theory.

Regimes and Regime Complexes

Regimes are a subset of norms, which are shared expectations about appropriate behaviour. Norms can be descriptive, prescriptive or both. They can also be institutionalized (or not) to varying degrees. A regime has a degree of hierarchical coherence among norms. A regime complex is a loosely coupled set of regimes. On a spectrum of formal institutionalization, a regime complex is intermediate between a single legal instrument at one end and fragmented arrangements at the other. While there is no single regime for the governance of cyberspace, there is a set of loosely coupled norms and institutions that ranks somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages.

The oval map of cyber governance activities in Figure 1 mixes norms, institutions and procedures, some of which are large in scale, while others are relatively small; some are quite formal and some very informal. The labels are often arbitrary.[4] The oval is not designed to map all governance activities in cyberspace (which is a massive undertaking) and, thus, is deliberately incomplete. Like all heuristics, it distorts reality as it simplifies. Nonetheless, it is a useful corrective to the usual UN versus multi-stakeholder dichotomy as an approach to cyber governance, and it locates Internet governance within the larger context of cyber governance. First, it indicates the extent and wide range of actors and activities related to governance that exist in the space. Second, it separates issues related to the technical function of connectivity, such as domain name addresses (DNS) and technical standards where a relatively coherent and hierarchical regime exists, from the much broader range of issues that constitute the larger regime complex. Third, it encourages us to think of layers and domains of cyber governance that are much broader than just the issues of DNS and ICANN, which have limited functions and little to do directly with larger issues such as security, human rights or development. As Laura DeNardis (2014, 226) writes, "a question such as 'Who should control the Internet, the United Nations or some other organization?' makes no sense whatsoever. The appropriate question involves determining what is the most effective form of governance in each specific context."

When we look at the whole range of cyber governance issues, some of the bipolarity in alignments that characterized the WCIT begins to erode. Liberalism is not the only divide. For example, some of the countries that voted against the West were not authoritarian, but were post-colonial or developing countries concerned about issues of sovereignty, which can be swayed by programs to develop their cyber capabilities or to protect the interests of their telecom companies. Also, within the liberal democratic bloc, there are important differences between the United States and Europe over issues of privacy, which have been increased by Edward Snowden's revelations regarding surveillance. Such issues may wind up having strong effects and being resolved within trade agreements like the proposed Trans-Atlantic Trade and Investment Partnership. It oversimplifies the politics of cyber governance to compress all of these dimensions into a bipolar dispute over liberal versus authoritarian approaches to content control.

This mapping of a regime complex also indicates the importance of linkages of cyber to normative and regime structures outside the issue area. The various actors that are located at the edge of the oval have independent structures of power and institutions outside the cyber issue area,

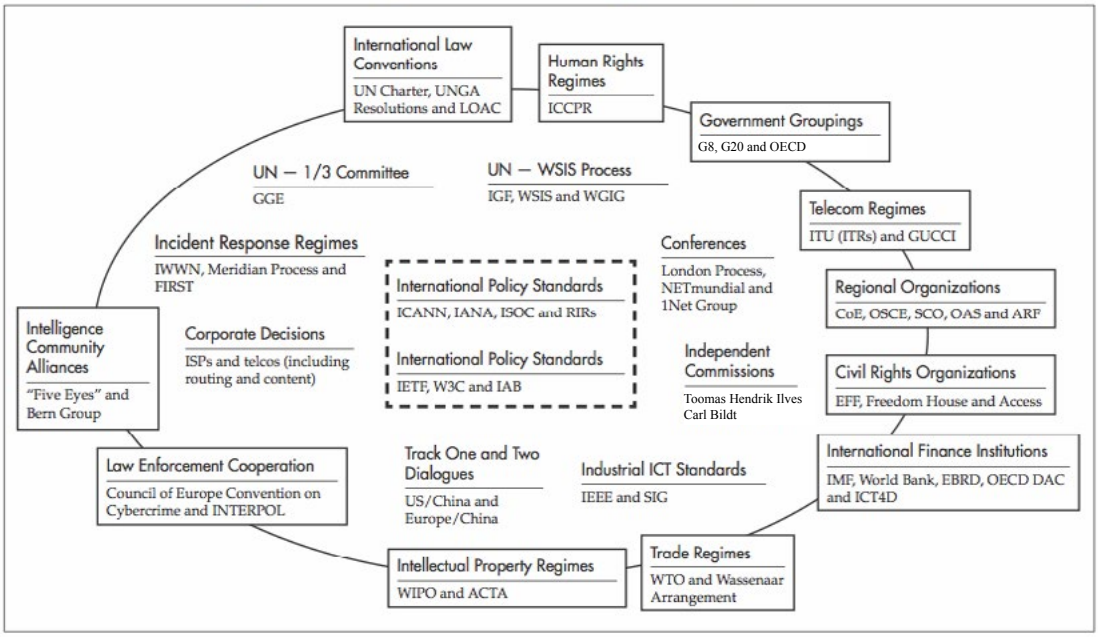
[4] I am indebted to Alexander Klimburg for help with the labels.

but still play a significant role in issues of cyber governance. In other words, much of cyber governance comes from actors and institutions that are not focused purely on cyber. Moreover, these institutions compete and are used in a process of "contested multilateralism," whereby state and non-state actors seek to shape the norms that govern activities within the oval (Morse and Keohane, forthcoming).

Finally, this approach helps to relieve some of the fears of extreme balkanization. Interference with the central regime of domain names and standards could fragment the functioning of the Internet, and it might make sense to consider a special treaty limited to that area (Sofaer, Clark and Diffie 2010). However, trying to develop a treaty for the broad range of cyberspace as a whole could be counterproductive. The loose coupling among issues that now exists permits cooperation among actors in some areas at the same time that they have disagreements in others. For example, China and the United States can use the Internet for economic cooperation even as they differ on human right and content control. Countries could cooperate on cybercrime, even while they differ on laws of war or espionage.

What regime complexes lack in coherence, they make up in flexibility and adaptability. Particularly in a domain with extremely volatile technological change, these characteristics help both states and non-state actors to adjust to uncertainty. Moreover, they permit the formation of clubs or smaller groupings of like-minded states than can pioneer the development of norms that may be extended to larger groups at a later time. As Keohane and Victor (2011, 7) note of the regime complex for climate change, "adaptability and flexibility are particularly important in a setting...in which the most demanding international commitments are interdependent yet governments vary widely in their interest and ability to implement them."

Figure 1: The Regime Complex for Managing Global Cyber Activities



Source: Author.

Acronyms for Figure 1

3G	Global Governance Group	GUCCI	Global Undersea Communications Cable Infrastructure	ITRs	International Telecommunication Regulations
ACTA	Anti-Counterfeiting Trade Agreement	IAB	Internet Architecture Board	IWWN	International Watch and Warning Network
ARF	Association of Southeast Asian Nations Regional Forum	IANA	Internet Assigned Numbers Authority	OAS	Organization of American States
DAC	Development Assistance Committee (OECD)	ICCPR	International Covenant on Civil and Political Rights	OECD	Organisation for Economic Co-operation and Development
EBRD	European Bank for Reconstruction and Development	ICT	information and communications technology	OSCE	Organization for Security and Co-operation in Europe
EFF	Electronic Frontier Foundation	ICT4D	Information and Communication Technologies for Development	RIRs	regional Internet registries
FIRST	Forum for Incident Response and Security Teams	IEEE	Institute of Electrical and Electronics Engineers	SCO	Shanghai Cooperation Organisation
"Five Eyes"	Alliance of Australia, Canada, New Zealand, the United Kingdom and the United States	IETF	Internet Engineering Task Force	telcos	telecommunications company
G8	Group of Eight	IGF	Internet Governance Forum	UNGA	United Nations General Assembly
G20	Group of Twenty	IMF	International Monetary Fund	WSIS	World Summit on the Information Society
GGE	Group of Governmental Experts (UN)	IISOC	Internet Society		

Norms and Cyber Sub-Issues

The norms that affect the various sub-issues of regime complexes can be compared along a variety of dimensions such as effectiveness, resilience, autonomy and others (Hasenclever, Mayer and Rittberger 1997). It is more useful to compare cyber issues in terms of four dimensions: depth, breadth, fabric and compliance. Depth refers to the hierarchical coherence of a set of rules or norms. Is there an overarching set of rules, which are compatible and mutually reinforcing (even if they are not adhered to or complied with by all actors)? For example, on the issue of domain names and standards, the norms, rules and procedures have coherence and depth; however, on the issue of espionage, there are few. Breadth refers to the scope of the numbers of state and non-state actors that have accepted a set of norms (whether they fully comply or not). For instance, on the issue of crime, 42 states have ratified the Budapest convention.

"Fabric" refers to the mix of state and non-state actors in an issue area. This is particularly interesting in cyber because the low barriers to entry mean many of the resources and much of the action is controlled by non-state actors. Issues with a high degree of state control have a "tight fabric"; those where non-state actors are pre-eminent have a loosely woven fabric. Security issues such as the laws of war in cyber have a tight fabric of sovereign control, while the DNS has a loose fabric in which non-state actors play a major role. As suggested above, a loosely woven fabric is not synonymous with shallowness or incoherence. A fourth dimension for comparison is compliance: how widespread is the behavioural adherence to a set of norms? For instance, on the sub-issue of domain names and standards, compliance is high; on issues of privacy it is mixed; and on human rights it is low. Some of the major sub-issues of the cyber regime complex are compared along these dimensions below. (The list is not designed to be complete and other rows for trade, intellectual property or development can easily be added to the table.)

Table 1: Some Issues in the Cyber Regime Complex

	Depth	Breadth	Fabric	Compliance
DNS/standards	High	High	Loose	High
Crime	High	Medium	Mixed	Mixed
War/Sabotage	Medium	Low	Tight	Mixed
Espionage	Low	Low	Mixed	Low
Privacy	Medium	Low	Mixed	Mixed
Content control	Low	Low	Loose	Low
Human Rights	Medium	Medium	Loose	Low

Source: Author.

The variation in the characteristics of these sub-issues suggests why cyberspace is likely to remain a regime complex rather than a single, strong regime for some time. As Keohane and Victor (2011, 8) argue in regard to climate change, it is "actually many different cooperation problems, implying different tasks and structures. Three forces — the distribution of interests, the gains from linkages, and the management of uncertainty — help to account for the variation in the institutional outcomes, from integration to fragmentation." This is clearly true of cyberspace as well, though it is important to notice the difference. There is in one area of the cyber domain where interests and gains from linkage are strong enough that a coherent regime exists.

Partly because of strong common interests in connectivity, and partly because of path dependency and the way the basic standards of the Internet were established in the United States, there is a core regime related to standards and assigned names and numbers including management of the DNS root zone servers. While there has been controversy about the status of ICANN, and the US government has indicated it plans to devolve the IANA function to ICANN in the future, no state has thus far found it would benefit from ceasing to comply. The development of standards is advanced primarily by non-state actors, such as the IETF, the W3C, the IEEE and others, where states and voting have minimal effect. This is the area of cyber where the concept of multi-stakeholderism is most apparent.

Crime might seem to be the next likely sub-issue to be susceptible to regime formation. The issue has a loose fabric in which spammers, criminals and other free riders impose large costs on both states and private actors. The Budapest convention provides a coherent structure with depth, but its breadth has been limited by its origins in Europe. Many post-colonial countries and authoritarian countries such as Russia and China object to obligations that they see as intrusions on their sovereignty as well as the European origin of the norms. Some developing countries also see little to gain by joining, as few of their national companies would benefit, while they fear the potentially high costs of enforcement, should they to become signatories. Moreover, some private companies find it is in their economic interest to hide the extent to which they have been victimized and simply absorb it as a business cost, rather than suffer reputational and regulatory costs. States may also think that the costs are not high enough to merit action — even if cybercrime costs US$400 billion, it is still only 0.05 percent of global GDP. Thus, insurance markets are difficult to develop and compliance is far from satisfactory. This may change in the future if the costs of cybercrime increase, given its sophistication and scope. Despite differences over what information activities constitute a crime in authoritarian and democratic countries, cooperation could be modelled after extradition laws that relate to actions that are "doubly criminal" — that is, illegal in both countries.

War has an overarching normative structure that is derived from the UN Charter and the LOAC. The issue has a tight structure growing out of the nature of war as a sovereign action of states. The third meeting of the UN's GGE, which concluded in July 2013, agreed in principle that such laws applied in the cyber domain. What this means in practice, when there is great technological uncertainty, is more challenging. While a group of NATO legal scholars has produced the Tallinn Manual on International Law Applicable to Cyber Warfare — which attempts to translate general principles regarding proportion, discrimination and collateral damage into the cyber domain — the scope of the acceptance of these principles has been limited by its origins (Schmitt 2013). While there has been no cyberwar in a strict sense, there has been cyber sabotage, such as Stuxnet, and cyber instruments, such as distributed denial-of-service (DDoS) attacks, which were used in the Russian invasion of Georgia. On the other hand, there have been press accounts that the United States decided not to use cyber adjuncts in Iraq, Libya and elsewhere, because of uncertainties about civilians and collateral damage (Schmitt and Shanker 2011; Markoff and Shanker 2009). Thus, compliance is judged with these norms as mixed.

According to press accounts, there is extensive use of cyber espionage by a wide variety of states and non-state actors. While espionage is an ancient practice that is not against international law, it often violates the domestic laws of sovereign states. Traditionally (for example, in the

US-Soviet competition during the Cold War), rough "rules of the road" led to reciprocal expulsions and reductions in diplomatic missions as a means of regulating the friction created by espionage. Thus far, cyber espionage is so easy and relatively safe that no such rules of the road have been developed. The United States has complained about Chinese cyber espionage that steals intellectual property, and raised the issue at the summit between US President Barack Obama and President of the People's Republic of China Xi Jinping in June 2013. However, the US effort to create a norm that differentiates spying for commercial gain from all other spying has been lost in the noise created by the revelations of extensive National Security Agency (NSA) surveillance released by Snowden (Goldsmith 2013). Moreover, normative efforts have been plagued by the loose fabric of the issue. Although the exposure of Chinese spying in 2013 by Mandiant suggested a clear government connection, many other instances are more ambiguous about whether they are by government or non-state actors (Sanger, Barboza and Perlroth 2013).

Privacy is a sub-issue of growing importance given the increases in computing power and storage that are often summarized as the "era of big data." There are widespread concerns about companies, criminals and governments storing and misusing personal data. At the same time, in the age of social media, there are changing generational attitudes in many societies about where to draw the appropriate lines between public and private. Private terms-of-service agreements are often cumbersome and opaque to consumers. Additionally, personal identification information, once on the Internet, can end up in numerous places, rendering futile most efforts to have the initial posting site remove it. At the same time, European efforts to enforce a "right to be forgotten" with legal excisions of history have raised concerns among some civil libertarians. The concept of privacy is poorly defined and understood, and has very different legal structures in Europe and the United States, not to mention authoritarian states (see Brenner 2014). Thus, it is not surprising that while there are conflicting norms, the normative structure for the sub-issue lacks depth, breadth or compliance.

Content control is another sub-issue with conflicting norms with little depth or breadth. For authoritarian states, information that crosses borders by any means and jeopardizes the stability of a regime is a threat. The SCO has, therefore, expressed a concern about information security, and Russia and China have proposed UN resolutions to that effect. In practice, authoritarian countries filter such threatening messages and would like to have a normative structure that would encourage other states to comply. But the United States could not stop a Falun Gang email to China without violating the free speech clauses of the US Constitution. This is why democratic countries refer to cyber security and argue against the control of the content of Internet packets.

At the same time, democratic countries do control some content. Most try to stop child pornography but are divided on issues such as hate speech, and many Internet corporations have been caught between conflicting national legal systems. Moreover, this sub-issue has a loosely woven fabric and various private groups create black and gray lists of what they regard as violators of various norms. In some cases, these vigilantes have been able to borrow the authority of government (Mueller 2010, chapter 9). Copyright is another important area related to content control. For example, the proposed Stop Online Piracy Act in the US Congress would have required Web hosting companies, search engines and ISPs to sever relations with websites and users found in violation of copyright. While such measures have met with strong resistance, it is likely they will remain contentious both in domestic and transnational politics. Thus, there is no

depth, breadth or widespread compliance with a normative structure for content control.

Human rights is a cyber sub-issue that has many of the same problems of conflicting values that plague content control, but there is an overriding legal structure in the form of the Universal Declaration of Human Rights. Moreover, in June 2012, the UN Human Rights Council affirmed that the same rights that people have off-line must also be protected online. Within the declaration, however, there is a potential tension between Article 19 (freedom of opinion and expression) and Article 29 (public order and general welfare). On the other hand, different states interpret the declaration in different ways, and authoritarian states that feel threatened by freedom of speech or assembly make no exceptions for the Internet. The US government has proclaimed an Internet freedom agenda, but has not explained whether this includes a right of privacy for foreigners. This agenda has also been complicated in the wake of the Snowden revelations. In 2011, the Netherlands held a conference that launched a Freedom Online Coalition, which now includes 22 states committed to human rights online, but the disparities in behaviour lead to the conclusion that the normative structure in this sub-issue lacks depth, breadth or compliance. Nonetheless, the loose fabric of the issue allows ample opportunity for non-state actors to press for human rights in cyberspace. For instance, the civil society organization, Global Network Initiative, has been pressing private companies to sign up to principles that advance transparency and respect human rights (MacKinnon 2012, chapter 14).

The Future Dynamics of the Cyber Regime Complex

Given the youth of the issue and the volatility of the technology, there are many potential paths along which cyber norms may evolve. Regime theorists have developed three quite different causal models that tend to complement each other. Realists argue that regimes are created and sustained by the most powerful state. Such hegemons have the incentive to provide public goods and discipline free riders because they will benefit disproportionately. But, as their power ebbs, the maintenance of regimes becomes more difficult (Gilpin 1987). From this point of view, the declining US control of the Internet suggests future fragmentation.

A second approach, liberal institutionalism, emphasizes the rational self-interest of states seeking the benefits of cooperative solutions to collective action problems. Regimes and their institutions help states achieve benefits by providing information and reducing transactions costs. They cut contracting costs, provide focal points, enhance transparency and credibility, monitor compliance and provide a basis for sanctioning deviant behaviour (Keohane 1984). This approach helps to explain why a regime exists for the DNS where perceived interests in cooperation are high, while a regime does not exist in the sub-issue of espionage where interests diverge significantly.

A constructivist set of theories emphasizes cognitive factors, such as how constituencies, groups and social movements change the perception and organization of their interests over time (Ruggie 1998). It is a cliché that states act in their national interest. The important question is how those interests are perceived and implemented. This is particularly important in the cyber domain, where the technology is new, and states are still struggling to understand and define their interests. In a chronological analogy, state learning of interests in the cyber domain is equivalent

to about the year 1960, in what was then a new technology of nuclear weapons and nuclear energy (Nye 2011a). It was not until 1963 that the first arms control treaty was ratified — the atmospheric test ban — and 1968 that the Non-Proliferation Treaty was signed. The situation in cyber is made more complex by the much greater roles of a diverse set of private and non-profit actors responding to rapid social and economic change. Transnational epistemic communities of people and groups that share ideas and outlooks — such as ISOC and the IETF — play important roles (Adler and Haas 1992). Over time, the extent and interests of these cyber epistemic communities has grown. Cognitive theories help to explain the evolution of norms, but also why there is considerable fragmentation in the normative structures of sub-issues like privacy, content control and human rights.

Optimists about the development of norms in the cyber regime complex can point to some recent evidence of progress. For example, the disagreement between the sovereigntist and multi-stakeholder philosophies seemed somewhat less stark at the NETmundial conference in Sao Paolo, Brazil in 2014, than at the WCIT conference in Dubai in 2012. Moreover, while early meetings of the GGE were unable to reach consensus, the latest meeting reached agreement on a number of points, including the principle that international laws of war applied to cyberspace. In addition, the number of states acceding to the Council of Europe's Convention on Cybercrime has gradually increased, and INTERPOL has established a cybercrime centre in Singapore. Forty-one states have agreed to use the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies to stop sales of spyware to authoritarian countries. There has been an increase in international and transnational cooperation among CERTs. Before the recent dispute over Ukraine, the United States and Russia agreed that their hotline arrangements would be extended to cyber events. The United States and China established an official working group on cyber in 2013. Numerous track two groups and various private conferences and commissions continued to work on the development of norms. Industry groups continued to work on standards regarding everything from undersea cable protection to financial services. And non-profit groups pressed companies and governments to protect privacy and human rights.

Conversely, pessimists about normative change in the cyber regime complex point to the overall decline of the trust that is so important in the issue area. Some observers date this loss to what they see as the militarization of cyberspace symbolized by: the DDOS attacks that accompanied the Russian disruption of Estonia in 2007 and invasion of Georgia in 2008; the establishment of the American Cyber Command in 2009; and the discovery of Stuxnet in 2010. Others point to the 2013 Snowden revelations that the NSA not only carried out espionage (which is not new or unique), but also subverted encryption standards and open-source software. Some technologists believe that trust can be rebuilt from the bottom up with new software technologies, as well as procedures for inspection of hardware supply chains. Others argue that low trust will be a persistent condition and it will exacerbate a fragmenting trend toward greater control by sovereign states (see Schneier 2013).

Some analysts reinforce their pessimistic projections by pointing to realist theories about the decline of US hegemony over the Internet. In its early days, the Internet was largely American, but today, China has twice as many users as the United States. Where once only roman characters were used on the Internet and HTML tags were based on abbreviated English words, now there are generic top-level domain names in Chinese, Arabic and Cyrillic scripts, with more alphabets

expected to come online shortly (ICANN 2013). And in 2014, the United States announced that it would relax its Department of Commerce's supervision of ICANN and the IANA function. Some experts worried that this would open the way for authoritarian states to try to exert control over the system of root zone servers, and use that to censor the addresses of opponents.

Such fears seem exaggerated both on technical grounds and in their underlying premises. Not only would such censorship be difficult, but, as liberal institutionalist theories point out, there are self-interested grounds for states to avoid such fragmentation of the Internet. In addition, the descriptions in the decline in US power in the cyber regime are overstated. Not only does the United States remain the second-largest user of the Internet, but it is also the home of eight of the 10 largest global information companies (Statista 2013).[5] Moreover, when one looks at the composition of voluntary multi-stakeholder communities such as the IETF, one sees a disproportionate number of Americans participating for path dependent and technical expertise reasons. From an institutionalist or constructivist viewpoint, the loosening of US influence over ICANN could be seen as a strategy for strengthening the institution and reinforcing the American multi-stakeholder philosophy rather than as a sign of defeat (Zittrain 2014).

It is interesting to look at the experience of other regimes when US pre-eminence diminished in an issue area. In trade, for example, the United States was by far the largest trading nation when the General Agreement on Tariffs and Trade (GATT) was created in 1947, and the United States deliberately accepted trade discrimination by Europe and Japan as part of its Cold War strategy. After those countries recovered, they joined the United States in a club of like-minded nations within the GATT (Keohane and Nye 2001). In the 1990s, as other states' shares of global trade increased, the United States supported the expansion of GATT into the WTO, and the club model became obsolete. The United States supported Chinese accession to the WTO and China surpassed it as the world's largest trading nation. While global rounds of trade negotiations became more difficult to accomplish and various free trade agreements proliferated, the rules of the WTO continued to provide a general framework where the norm of most favoured nation status and reciprocity created a structure where particular club deals could be generalized to a larger number of countries. Moreover, new entrants, such as China, found it in their interests to observe even adverse judgments of the WTO dispute settlement process.

Similar to the non-proliferation regime, when the United States had a nuclear monopoly in the 1940s, it proposed the Baruch Plan for UN control, which the Soviet Union rejected in order to pursue it own nuclear weapons. In the 1950s as nuclear technology spread, the United States used the Atoms for Peace program, coupled with inspections by the new International Atomic Energy Agency, to try to separate the peaceful from weapons purposes. During the 1960s, the five nuclear weapon states negotiated the Non-Proliferation Treaty, which promised peaceful assistance to states that accepted a legal status of non-nuclear weapon states. In the 1970s, after India's explosion of a nuclear device and the further spread of technology for the enrichment and reprocessing of fissile materials, the United States and like-minded states created a Nuclear Suppliers Group that agreed "to exercise restraint" in the export of sensitive technologies, as well as an International Nuclear Fuel Cycle Evaluation, which called into question the optimistic projections about the use of plutonium fuels. While none of these regime adaptations were

[5] Note that Yahoo and Yahoo-Japan have been treated as one entity for the purposes of company rankings.

perfect, and problems persist with North Korea and Iran today, the net effect of the normative structure was to slow the growth in the number of nuclear weapon states from the 25 expected in the 1960s to the nine that exist today (see Nye 1981). In 2003, the United States launched the Proliferation Security Initiative, a loosely structured grouping of countries that shares information and coordinates efforts to stop trafficking in nuclear proliferation-related materials.

In short, projections based on realist theories of hegemony are based on poorly specified indicators of change (see Nye 2011b, chapter 6). Even after monopolies over a new technology erode, it is possible to develop normative frameworks for governance of an issue area.

Conclusions

Predicting the future of the normative structures that will govern the various issues of cyberspace is impossible because of the newness and volatility of the technology, the rapid changes in economic and political interests, and the social and generational cognitive evolution that is affecting how state and non-state actors understand and define their interests. While the explanations are complementary, it seems likely that liberal institutionalist and cognitive regime theories will provide better tools for understanding those changes than oversimplified theories of hegemonic transition.

One projection does seem clear. It is unlikely that there will be a single overarching regime for cyberspace any time soon. A good deal of fragmentation exists now and is likely to persist. The evolution of the present regime complex, which lies halfway between a single coherent legal structure and complete fragmentation of normative structures, is more likely. Different sub-issues are likely to develop at different rates, with some progressing and some regressing in the dimensions of depth, breadth and compliance. Some areas, such as crime, in which states have common interests against third-party free riders, seem ripe for interstate agreement, even if only an agreement to assist in legal and forensic efforts (Tikk 2011). Other issues, such as privacy, may see compromises in the context of trade negotiations, which formally have no direct connection with the cyber area. And some areas, such as war, may not be susceptible to formal arms control agreements, but may see the evolution of declaratory policy, confidence-building measures and rough rules of the road. Rather than global agreements, like-minded states may act together to avoid destabilizing behaviour, and later try to generalize such behaviour to a broader group of actors through means ranging from formal negotiation to development assistance. Whatever the outcomes, analysts interested in the development of normative structures for the governance of cyberspace should avoid the over-simplified popular dichotomies of a "war" between the ITU and ICANN. Instead, they would do better to view the problems in the full complexity offered by regime theories and the concept of regime complexes.

Works Cited

Adler, Emmannuel and Peter M. Haas. 1992. "Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program." International Organization 46 (1): 367–90.

Blumenthal, Marjory and David D. Clark. 2009. "The Future of the Internet and Cyberpower." In Cyberpower and National Security, edited by Franklin D. Kramer, Stuart Starr and Larry K. Wentz.

Washington, DC: National Defense University Press.

Brenner, Joel. 2013. " Mr. Wemmick's Condition: or Privacy as a Disposition, Complete with Skeptical Observations Regarding Various Regulatory Enthusiasms." Lawfare Research Paper Series 2 (1): 1–43.

Choucri, Nazli. 2012. Cyberpolitics in International Relations. Cambridge: MIT Press.

Clarke, Richard A. and Robert K. Knake. 2012. Cyber War: The Next Threat to National Security and What to Do About It. New York: Ecco.

Council of Europe Convention on Cybercrime. 2014. "Convention on Cybercrime CETS No.: 185." http://conventions.coe.int/Treaty/Commun/ ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

CSIS. 2008. Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Washington, DC: CSIS.

Deibert, Ronald J. and Rafal Rohozinski. 2010. "Risking Security: Policies and Paradoxes of Cyberspace Security." International Political Sociology 4 (1).

Demchak, Chris C. and Peter Dombrowski. 2011. "Rise of a Cybered Westphalian Age." Strategic Studies Quarterly (Spring).

DeNardis, Laura. 2014. The Global War for Internet Governance. New Haven: Yale University Press,

Garamone, Jim. 2014. "Hagel Thanks Alexander, Cyber Community for Defense Efforts." American Forces Press Service, March 28. www.defense.gov/news/ newsarticle.aspx?id=121928.

Gilpin, Robert. 1987. "The Theory of Hegemonic Stability." Understanding International Relations: 477–84.

Goldsmith, Jack. 2013. "Reflections on U.S. Economic Espionage, Post-Snowden." Lawfare, December 10. www.lawfareblog.com/2013/12/reflections-on-u-s-economic-espionage-post-snowden/.

Goldsmith, Jack and Tim Wu. 2006. Who Controls the Internet? Illusions of a Borderless World. Oxford: Oxford University Press.

Hardin, Garrett. 1968. "The Tragedy of the Commons." Science 162 (3859).

Hasenclever, Andrea, Peter Mayer and Volker Rittberger. 1997. Theories of International Regimes. Cambridge: Cambridge University Press.

Hurwitz, Roger. 2009. "The Prospects for Regulating Cyberspace." Unpublished paper. November.

ICANN. 2013. "Internet Domain Name Expansion Now Underway." News release, October 23. www.icann. org/en/news/press/releases/release-23oct13-en.

Keohane, Robert O. 1984. After Hegemony: Cooperation and Discord in the World Political Economy. Princeton, NJ: Princeton University Press.

Keohane, Robert O. and Joseph S. Nye. 1977. Power and Interdependence. Boston: Little, Brown.

———. 2001. "Between Centralization and Fragmentation: The Club Model of Multilateral Cooperation and Problems of Democratic Legitimacy." John F. Kennedy School of Government, Harvard University Faculty Research Working Paper Series, RWP01-004.

Keohane, Robert O. and David G. Victor. 2011. "The Regime Complex for Climate Change." Perspectives on Politics 9.

Klimburg, Alexander. 2013. "The Internet Yalta." Center for a New American Security Commentary. www. cnas.org/sites/default/files/publications-pdf/CNAS_ WCIT_commentary%20 corrected%20%2803.27.13%29. pdf.

Krasner, Stephen, ed. 1983. International Regimes. Ithaca, NY: Cornell University Press.

Kuehl, Daniel T. 2009. "From Cyberspace to Cyberpower: Defining the Problem." In Cyberpower and National Security, edited by Franklin D. Kramer, Stuart Starr and Larry K. Wentz, 26–28. Washington, DC: National Defense University Press.

Lewis, James. A. and Stewart Baker. 2013. The Economic Impact of Cybercrime and Cyberespionage. CSIS report. http://csis.org/files/publication/60396rpt_ cybercrime-cost_0713_ ph4_0.pdf.

Libicki, Martin. 2009. Cyberdeterrence and Cyberwar. Santa Monica: RAND.

MacKinnon, Rebecca. 2012. Consent of the Networked: The Worldwide Struggle for Internet Freedom. New York: Basic Books.

Markoff, John and Thom Shanker. 2009. "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk." The New York Times, August 1. www.nytimes.com/2009/08/02/ us/ politics/02cyber.html.

Maurer, Tim. 2011. "Cyber Norm Emergence at the United Nations — An Analysis of the UN's Activities Regarding Cyber-security?" Belfer Center for Science and International Affairs, Harvard Kennedy School Discussion Paper 2011-11.

Morse, Julia and Robert O. Keohane. Forthcoming. "Contested Multilateralism." The Review of International Organizations.

Mueller, Milton. 2010. Networks and States. Cambridge, MA: MIT Press.

———. 2012. “ITU Phobia: Why WCIT Was Derailed.” Internet Governance Project. www.internetgovernance. org/2012/12/18/itu-phobia-why-wcit-was-derailed/.

Nye, Joseph S. 1981. “Maintaining the Non-Proliferation Regime.” International Organization: 15–38.

———. 2011a. “Nuclear Lessons for Cyber Security.” Strategic Studies Quarterly: 18–38.

———. 2011b. The Future of Power. New York: PublicAffairs.

Ostrom, Elinor. 2009. “A General Framework for Analyzing Sustainability of Social-Ecological Systems.” Science 325.

Ostrom, Elinor, Joanna Burger, Christopher Field, Richard Norgaard and David Policansky. 1999.

“Revisiting the Commons: Local Lessons, Global Challenges.” Science 284 (5412).

Raymond, Mark. 2013. “Puncturing the Myth of the Internet as a Commons.” Georgetown Journal of International Affairs Special Issue: 5–15.

Rid, Thomas. 2013. Cyber War Will Not Take Place. New York: Oxford University Press.

Ruggie, John Gerard. 1982. “International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order.” International Organization 36 (2).

———. 1998. “What Makes the World Hang Together? Neo-utilitarianism and the Social Constructivist Challenge.” International Organization 42 (4): 855–85.

Sanger, David E., David Barboza and Nicole Perlroth. 2013. “Chinese Army Unit Is Seen as Tied to Hacking Against U.S.” The New York Times, February 18. www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all.

Schmitt, Eric and Thom Shanker. 2011. “U.S. Debated Cyberwarfare in Attack Plan on Libya.” The New York Times, October 17. www.nytimes.com/2011/10/18/ world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

Schmitt, Miachael N., ed. 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press.

Schneier, Bruce. 2013. “The Battle for Power on the Internet.” The Atlantic, October 24. www.theatlantic. com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/.

Sofaer, Abraham D., David Clark and Whitfield Diffie. 2010. “Cyber Security and International Agreements.” In Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, edited by Committee on Deterring Cyberattacks: Informing Strategies and Developing Options and National Research Council. Washington, DC: National Academies Press.

Starr, Stuart H. 2009. “Toward a Preliminary Theory of Cyberpower.” In Cyberpower and National Security, edited by Franklin D. Kramer, Stuart Starr and Larry K. Wentz. Washington, DC: National Defense UP.

Statista. 2013. “Market Value of the Largest Internet Companies Worldwide as of May 2013 (In Billion U.S. Dollars).” Statista. www.statista.com/ statistics/277483/ market-value-of-the-largest-internet-companies-worldwide/.

Tikk, Eneken. 2011. “Ten Rules for Cyber Security.” Survival 53 (3): 119–32.

WGIG. 2005. Report of the Working Group on Internet Governance. Château de Bossey: WGIG. www.wgig. org/docs/WGIGREPORT.pdf.

Zittrain, Jonathan. 2008. The Future of the Internet and How to Stop It. New Haven: Yale University Press.

———. 2014. “No Barack Obama Isn’t Handing Control of the Internet Over to China.” The New Republic (224).

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
Fax: (617) 495-8963
Email: belfer_center@hks.harvard.edu
Website: http://belfercenter.org