Global Governance 18 (2012), 339–361

Global Governance and the Spread of Cyberspace Controls

Ronald J. Deibert and Masashi Crete-Nishihata

States are moving to assert their interests more forcefully in cyberspace and associated governance regimes. Traditionally, transnational networks of engineers, based primarily in the United States and Europe, have been the primary architects of cyberspace governance, with the users and private sector shaping cyberspace itself. However, governments are becoming increasingly influential across a number of governance forums and are deliberating on how to exercise power in and through cyberspace. Particularly noteworthy are how nondemocratic states outside of Europe, North America, and parts of Asia have begun to forcefully assert their interests in cyberspace governance regimes, including some, like the International Telecommunications Union, that were previously marginalized in the Internet space. Western liberal democracies are also moving away from laissez-faire and market-oriented approaches to more state-directed controls and regulations. Drawing from international relations theory literature, and in particular constructivist approaches, this article examines international and global mechanisms and dynamics that explain the growth and spread of cyberspace controls. It also provides a study of "norm regression" in global governance: the growth and spread of practices that undercut cyberspace as an open commons of information and communication. **Keywords:** *cyberspace, global governance, norm regression, International Telecommunication Union.*

Cyberspace encompasses the global digital communications environment that is embedded in political, economic, and social activity.[1] One of the burgeoning areas of cyberspace research is the study of information controls: actions conducted in and through cyberspace that seek to deny, disrupt, manipulate, and shape information and communications for strategic and political ends. Whereas once it was popularly assumed that cyberspace was immune to government regulation because of its dynamic nature and distributed architecture, a growing body of scholarship has shown convincingly how governments can shape and constrain access to information, freedom of speech, and other elements of cyberspace within their jurisdictions.

Today, more than thirty countries engage in Internet filtering, not all of them authoritarian regimes.[2] Internet surveillance policies are now widespread and bearing down on the private sector companies that own and operate the infrastructure of cyberspace, including Internet service providers

(ISPs). Likewise, a new generation of second- and third-order controls complement filtering and surveillance, creating a climate of self-censorship.[3] There is a very real arms race in cyberspace that threatens to subvert the Internet's core characteristics and positive network effects.

The study of cyberspace controls has tended to focus on the nation-state as the primary unit of analysis and has examined the deepening and widening of these controls within domestic contexts.[4] But largely unexamined so far are the *international* and *global* dynamics by which such controls grow and spread. The dynamics and mechanisms at these levels are important to consider because states do not operate in a vacuum; they are part of a global social order that has important implications for how they are constituted (constitutive norms), and what they do and how they behave (regulative norms).[5] This can have both "positive" and "negative" dynamic characteristics.[6] In a positive sense, states learn from and imitate each other. They borrow and share best practices, skills, and technologies. They take a cue from what like-minded states are doing and implement policies accordingly.

There are also negative international dynamics that shape the character of global relations. States compete against each other. Their perceptions of adversarial intentions and threats can impact the decisions they make. This dynamic has been characterized in the international relations literature as the logic of the "security dilemma."[7] One can see this logic playing itself out clearly today in cyberspace with the development of national armed forces capabilities to fight and win wars in that domain.

Government policies and behavior are also impacted by the activities of transnational actors—namely, civil society networks and the private sector—that function as a conduit and propagator of ideas and policies. Civil society networks educate users within countries about best practices and networking strategies, lobby governments, and operate largely irrespective of national boundaries.[8] The networks that tend to get the most attention are those for the promotion of human rights such as access to information, freedom of speech, and privacy. These networks come in a variety of shapes and sizes. Some are independent and largely grassroots in origin; others have been drawn into a support structure synchronized to the foreign policy goals of major governments such as the United States and the European Union. But few of them, especially the more important ones, operate only in a domestic policy setting.

Private sector actors are responsive to and seek to develop commercial opportunities across national boundaries and are increasingly a part of the global system's mechanisms and dynamics of cyberspace controls. Particularly relevant in this respect is the cybersecurity market, estimated to be on the order of $80 billion to $140 billion dollars annually.[9] Commercial providers of networking technology have a stake in the securitization of cyberspace and can inflate threats to serve their more parochial market interests.[10] Private actors also own and operate the vast majority of the

infrastructure and services that we call cyberspace. For that reason alone, their decisions can have major consequences for the character of cyberspace and are examples of the growing exercise of private authority in world politics.[11] It is not too far a stretch to argue that some companies have the equivalent of "foreign policies" for cyberspace, in some ways going beyond individual governments in terms of scope and influence.

In this article, we present an overview of information controls exercised in cyberspace as they have emerged over the past several decades, contrasting those controls with the constitutive rules, norms, and principles they are displacing. We then lay out a research framework for the study of global dynamics and mechanisms of the growth of cyberspace controls. Typically, international relations research on the spread of norms in global governance focuses on what might be construed as "positive" norm development: the spread of human rights, democracy, or the end of slavery, to give just a few examples. As Paul Kowert and Jeffrey Legro have pointed out, there is a bias in the study of norm propagation toward what might be considered good norms:

> A related bias in the study of norms is the "good norms" problem. Analysts tend to focus on those issues that are normatively desirable—e.g., the spread of democracy, the rise of human rights, the integration of world society, and prohibitions against the use of force. Yet undesirable norms are equally possible. Examples include norms of military autonomy and the use of force, economic domination, the acceptability of intrastate violence (e.g., civil war), and the disintegrative tendencies that exist in international politics (e.g., nationalism, religious exclusivity). These issues too deserve attention from the emerging sociological approach. . . . But "bad" or threatening norms remain understudied.[12]

In contrast, we analyze what might be considered "norm regression" in global governance: the growth and spread of practices that degrade cyberspace as an open commons of information and communication.[13] The aim is not to provide an exhaustive analysis of these dynamics and mechanisms as much as it is to sketch out a conceptual and analytical framework for further research. Drawing primarily from constructivist theories, we lay out several areas where such dynamics and mechanisms might be found and investigated further. In the conclusion, we consider some of the reasons why research in this area is important for the study and policy of global cyberspace governance and practice.

From Open Commons to Controlled Access

In the early period of the Internet's development, it was widely assumed that the distributed and highly decentralized technology would be difficult, even impossible, for governments to regulate.[14] The Internet's founding

architects designed a set of technological and normative principles that laid the foundations for the network and guided how it should be accessed and operated. One of the most important design principles of the Internet is the end-to-end argument (e2e) formulated by Jerome H. Saltzer, David P. Reed, and David D. Clark (1984), which organizes the placement of functions in a distributed computing network sharing a basic common protocol (TCP/IP). It states that access to and use of applications on the network should be nondiscriminatory, meaning that users on the edge of the network should freely control applications and services and be enabled to develop new applications to distribute over the network as long as they conform to the principle.[15] The e2e formed one of the central principles of the Internet for technological reasons. However, beyond its technological importance, e2e has had economic, political, and social effects, and has been advocated as a key driver for innovation.[16] An associated principle stemming from e2e is *network neutrality*, which can be defined as the "right of users to access content, services and applications on the Internet without interference from network operators or government," and the "right of network operators to be reasonably free of liability for transmitting content and applications deemed illegal or undesirable by third parties."[17]

The foundational principles of Internet communications would have remained limited and largely experimental were it not for important conscious policy decisions made by the United States and other Western countries to "keep the state out" of Internet governance. Recognizing at the time that this new mode of communication would help trigger new forms of ingenuity and economic growth, key policy decisions were made in the 1990s to separate out institutions of Internet governance from the direct oversight of states—in particular, the United States. Although the latter still wielded important indirect and structural controls, operating and other decisions were made primarily by the Internet's engineers following a model of consensus building and request for comments more familiar to the university-based computer science and engineering community that gave birth to the Internet than to political parliaments and assemblies. These decisions were paradigmatic in the short term and set a framework for other countries to follow suit.[18]

The combination of the technological and normative aspects of the Internet in this period frame the Internet as an "open commons" in which the domain was considered a separate space resistant to state regulation and control.[19] Over time, however, these assumptions have been called into question as governments, often operating in coordination with the private sector, have erected a variety of information controls and once-disparate technological ecosystems and new technologies have begun to converge around the Internet, sometimes bringing with them alternative modes of governance that do not conform with the Internet's foundational principles. The resulting communications environment, which we call cyberspace,

exhibits a tension between older norms, rules, and principles and those that are gradually displacing them. From the starting point of an open commons of information and communication, these new practices can be described as a form of "normative regression" because they revert back to traditional state-based forms of control that are typical of the pre-Internet days of territorialized regimes of communications.

We define *information controls* broadly as actions conducted in and through cyberspace that seek to deny, disrupt, manipulate, and shape information and communications for strategic and political ends. Information controls include an array of technologies, regulatory measures, laws, policies, and tactics. These can include media regulation, licensing regimes, content removal, libel and slander laws, and content filtering. Countries vary widely in terms of their transparency and accountability around such practices and in terms of the methods by which they carry out information controls. Invariably, the private sector actors who own and operate the vast majority of cyberspace infrastructure are being compelled or coerced to implement controls on behalf of states.

Perhaps the most basic form of state control in cyberspace is *Internet filtering* or censorship, which is the prevention of access to information online within territorial boundaries.[20] Rationales for national filtering regimes vary. Some states justify Internet filtering to control access to content that violates copyright, concerns the sexual exploitation of children, or promotes hatred and violence. Other countries filter access to content related to minority rights, religious movements, political opposition, and human rights groups. The OpenNet Initiative (ONI) has been studying national Internet filtering since 2003 and, through a combination of technical interrogation, field research, and data analysis methods, conducts tests to verify the presence of Internet filtering in more than sixty countries on an annual basis.[21] The reports of ONI provide a "snapshot" of accessibility at the point of time of testing from the perspective of national information environments. When ONI started documenting Internet filtering in 2003, only a handful of governments engaged in the practice. The latest reports of ONI indicate that more than forty countries engage in some form of Internet filtering, a growing number of them being democratic industrialized countries. Some of the nondemocratic regimes that engage in Internet filtering do so using commercial filtering products developed in the United States and Canada.[22] Others have developed more homegrown solutions. Some states provide "block pages" for banned content that explain the rationale and legal basis for the blocking; others provide only error pages, some of which are misleading and meant to misdirect users from the states' intentions. It is now fair to say that there is a growing norm worldwide for national Internet filtering, although the rationale for implementing filtering varies widely from country to country.

The trajectory of greater government intervention into cyberspace has developed beyond Internet filtering. Governments have shown a greater willingness to employ a broader range of regulatory, legal, covert, and offensive means to shape cyberspace in their strategic interests. For example, there have been a growing number of incidents where states have disrupted or tampered with communication networks for political purposes, including around elections and public demonstrations. ONI calls these actions *just-in-time blocking*—a phenomenon in which access to information is denied during important political moments when the content may have the greatest potential impact such as elections, protests, or anniversaries of social unrest.[23] In 2011 both Egypt[24] and Libya[25] severed all Internet access for brief periods of time during the Arab Spring. Similar tactics have been employed in Nepal (2005),[26] Burma (2007),[27] and China (2009).[28] During the Green Revolution in Iran, the government was suspected of ordering Internet ISPs to tamper or "throttle" bandwidth and the use of certain protocols associated with censorship circumvention and anonymity tools as a means to control opposition movements.[29] Disruptions of access to communications in response to protest and social unrest have also been called for, and in some cases implemented, in democratic states. In response to the 2011 UK riots, Prime Minister David Cameron made a speech to the House of Commons in which he stated "we are working with the police, the intelligence services and industry to look at whether it would be right to stop people communicating via [social media] when we know they are plotting violence, disorder and criminality."[30] In the summer of 2011, the Bay Area Rapid Transit System (BART) shut down cell phone service to four stations in San Francisco in reaction to a planned protest in an effort to disrupt its organization.[31] These and numerous other similar cases are examples of the sea change that has occurred over the past decade in terms of government approaches to cyberspace.

One important element of growing cyberspace controls is the downloading of responsibilities to the private sector, a phenomenon known as *intermediary liability*.[32] For example, both industrialized and developing governments have begun to legislate greater responsibilities on ISPs, telecommunications companies, and mobile operators to "police the Internet." These companies are being required by law to retain and archive user data, and share that data with law enforcement and intelligence agencies, in some cases without judicial oversight. As these requirements grow, the functions of network operators have incrementally changed toward a more fine-grained inspection and manipulation of the flow of traffic in ways that begin to impinge on e2e and network neutrality. Some large-scale network operators have even begun to take more offensive measures to police the Internet on their own. The concept of *active defense*, for example, which is now gaining widespread currency, describes actions taken by private sec-

tor network operators to take down and neutralize offending network nodes and traffic at their source, regardless of their geographic origin.[33]

The spectrum of information controls and their growing emergence across democratic and authoritarian states that we outlined above shows that, whereas once the dominant metaphor of state involvement in cyberspace was hands off, today the dominant metaphor is one of control. But how did these control norms spread internationally?

International and Global Mechanisms and Dynamics

Awareness and documentation of growing cyberspace controls on a per-nation basis is on the rise. Missing, however, is a consideration of the international and global mechanisms and dynamics of growing cyberspace controls. The field of international relations is premised on the notion that there are factors that affect state identity and behavior operating at an international systemic or global level. To put it simply, states are embedded in a global order that affects who they are (constitutive norms), what they do, and how they do it (regulative norms).

Although some of this scholarship has been rightly criticized in the past for reifying the international system and ignoring domestic level processes, it nonetheless identifies an important dimension of political behavior that needs to be considered.[34] States' policies are formed in interaction with other states in the international system and through interactions with transnational actors like civil society and the private sector.[35] However much domestic struggles and local threats motivate what states do, their interactions with each other, their perceptions of adversarial actions and intentions, and their involvement in institutions at a global level matter as well.

In the following section, we draw primarily from social constructivist approaches to illuminate where mechanisms and dynamics can be found in cyberspace practices and governance. Our aim is not to test or advance social constructivism as a body of theory per se. Rather, it is to use fairly well-established insights from international relations theory to help understand how information controls are spreading internationally. That said, cyberspace practice and governance may present an interesting case of "norm regression" for further research by international relations theorists since what we are describing is the emergence of norms, rules, and principles that undermine those related to a prior regime of shared practices. To be sure, what distinguishes good from bad norms is always in the eye of the beholder. But because the practices we trace diminish cyberspace as a global commons, and hold out the prospect of reinstituting a state-based governance regime that preceded it, we believe they can be accurately characterized as an example of norm regression.

Formal Organizations and Mechanisms

Norm Promotion Through International Institutions

The most obvious place to look for such international dynamics are the main forums of Internet governance: the International Corporation for Assigned Names and Numbers (ICANN), the International Telecommunication Union (ITU), the Internet Governance Forum (IGF), and others. These international institutions are important touchstones for the identification of the mechanisms and dynamics in which we are interested here.[36] Scholars of Internet governance have examined the stakeholders, processes, and policy outputs of these various institutions in detail for many years.[37] They are observing that these institutions are under new pressures as governments assert themselves more forcefully in cyberspace. As a consequence, the main issues that are addressed in some of these forums are changing; in technical governance forums, for example, previously unpoliticized or mostly technical issues are becoming the objects of intense political competition. Institutions such as the Internet Engineering Task Force (IETF) or the Regional Internet Registries (RIRs), which may have been overlooked in the past as overly technical and functional in nature, deserve renewed attention by scholars if only for the fact that some governments are now taking them seriously as vectors of policy formation and propagation.

For example, a loose coalition of like-minded countries have begun to develop strategic engagements with international institutions, like the ITU and the IGF, in ways that are quite novel and unlike previous engagements. Most strikingly, Russia and the Russian-speaking countries of the former Soviet Union have adopted a wide-ranging engagement with these forums to promote policies that synchronize with national-level laws around information security.[38] China has also recently explicitly stated not only its belief in the sovereign control over national information space, but that global cyberspace should be governed by international institutions operating under the United Nations.[39] Not surprisingly, their policies have been vocally supported by the secretary general of the ITU, Hamadoun Toure, who has called for, among other initiatives, a state-based cyber–arms control treaty that would imply significant renationalization of the Internet.[40] He has also been a vocal supporter of the United Arab Emirates, Indonesia, India, and others who have pressured companies like Research In Motion (RIM) to share encrypted data under the rubric of national security protections.[41] Every year since 1998, Russia has put forward resolutions at the United Nations to prohibit "information aggression," which is widely interpreted to mean ideological attempts, or the use of ideas, to undermine regime stability.[42] At least twenty-three countries now openly support Russia's interpretation of information security.

Sometimes engagement at these forums is intended to stifle or stonewall rather than promote certain policies. For example, Chinese delegations have been quite prominent at the IGF meetings, ironically as a means to stall the forum from gaining credibility and to undermine the broadening of Internet governance to civil society and other nonstate stakeholders. At the November 2009 IGF meeting in Egypt, for example, a book launch of an ONI volume, *Access Controlled*, was disrupted by UN security officials because of a poster to which the Chinese delegation objected that contained a reference to the "Great Firewall of China."[43] The propagation of norms internationally can be facilitated not only by promotion, but also by obstruction of contrary tendencies.

What is perhaps most interesting is that the international institutions whose missions are primarily focused around technical coordination of the Internet—the Internet Assigned Numbers Authority (IANA), ICANN, the IETF, and RIRs—have become increasingly politicized and subject to securitization pressures. As Brenden Kuerbis and Milton Mueller note, while Internet authority is highly distributed, "elements of hierarchy do exist, especially around critical resource allocation, and it is likely that security and other concerns will lead to continuing efforts to leverage those hierarchies into more powerful governance arrangements."[44] The securitization pressures are evident in the direct presence of law enforcement agencies (LEAs) in ICANN and RIR engagements. Examples include continuing efforts of LEAs to influence domain-name search (WHOIS) policy[45] and more recent negotiations on the Registrar Accreditation Agreement where LEAs have imposed demands that circumvent the bottom-up policymaking process to push for identity checks on domain name registrants and challenge the use of identity-shielding registration services.[46] Military, intelligence, and civilian agencies from the US government have also had a presence in key Internet governance bodies (especially in the IETF) and have pushed agendas to secure Internet resources. These interactions are sometimes done directly, but more often through contractors. These agencies have typically participated in these forums as peers among other stakeholders that are present.[47] As demands for secure Internet resources mount, the desire for LEAs and other agencies in both democratic and nondemocratic regimes to seek influence in Internet governance bodies and agendas will continue.[48]

Governments whose strategic interests are oriented around legitimization of national controls are viewing these cyberspace governance forums as important components of a broader, more comprehensive international policy engagement. For example, a coalition of Russian-speaking countries, supported by China and India, have put forward a proposal through a submeeting of the ITU to give governments veto power over ICANN decisions.[49] Generally speaking, engagement in these various international

forums is an attempt by some countries to reassert the legitimacy of national sovereign control over cyberspace by promoting such a norm at international venues. Ironically, in other words, international institutions are perceived by policymakers of these countries as vehicles of nationalization. Such a strategic perception of international institutions has been characterized by Amitav Acharya as "norm subsidiarity," whereby marginal states promote norms through international institutions to "preserve their autonomy from dominance, neglect, violation or abuse by more powerful central actors."[50]

Policy Coordination Through Regional Organizations

Although international institutions are important conduits of norm propagation and legitimization, they can also be unwieldy and diffuse. As a consequence, coalitions of like-minded states are increasingly operating through more manageable lower-level organizations such as regional institutions.[51] Some of these forums attract little attention, meet in relative obscurity, and thus take actions that rarely see the light of day and are ignored or overlooked by activists and others concerned with Internet freedom and cyberspace governance. But the actors who comprise them treat them seriously and use them as vehicles of policy coordination and information sharing.

One example is the Shanghai Cooperation Organization (SCO), which is a regional organization made up of China, Kyrgyzstan, Kazakhstan, Russia, Tajikistan, and Uzbekistan.[52] India, Iran, Mongolia, Afghanistan, and Pakistan have observer status, and Belarus, Turkey, and Sri Lanka are considered dialogue partners. Iran is engaged in the SCO, but prevented from formally joining because of UN sanctions. However, it is considered an active participant in the SCO summits, which have been held regularly throughout the region since the early 2000s. The SCO aims to share information and coordinate policies around a broad spectrum of cultural, economic, and security concerns, among them cyberspace policies. Generally speaking, experts see the SCO as a regional vehicle of "protective integration" against international norms of democracy and regime change, with shared information policies being seen as critical to that end.[53] Recently, the SCO issued a statement on "information terrorism," which drew attention to the way in which the countries have a shared and distinct perspective on Internet security policy. The SCO has also engaged in joint military exercises and missions, described by some observers as simulations of how to reverse color-style revolutions and popular uprisings.[54] Unfortunately, the SCO's meetings tend to be highly secretive affairs and therefore not easily subject to outside scrutiny. But they are likely to become important vehicles of policy coordination, giving unity, normative coherence, and strength to the individual countries beyond the sum of their parts.

Norm Diffusion Through Bilateral Cooperation

Norms can diffuse internationally in the most direct way by governments sharing resources and expertise with each other in bilateral relationships. There has been long-standing speculation that China and Chinese companies are selling technology to regimes that export its filtering and surveillance system. For example, information technology experts from China's Military Intelligence Division recently visited Sri Lanka, ostensibly to offer advice on how to filter the Internet.[55] According to a *Wall Street Journal* report, the Chinese telecom giant Huawei pitched its products and services to the Iranian government for a national mobile communications project on the basis of its expertise in filtering and surveillance.[56] However, these discussions and arrangements are rarely transparent, typically shrouded in the type of secrecy that accompanies matters of national security, law enforcement, and intelligence matters. They are likely to become more important vehicles for the promotion of these states' strategic interests as they seek to propagate practices internationally that are supportive of their own domestic policies.

Informal Mechanisms

Although these forums and bilateral relations are important, they do not exhaust by any means the dynamics and mechanisms of cyberspace controls at play at the international level. Here, it is important to underline the many different means by which norms, behaviors, and policies are propagated globally. Although formal sites of governance, such as those described above, are important, norms can propagate through the global order in a variety of ways. *Norm diffusion* is the process through which norms are socialized and shared, and then become internalized, accepted, and implemented by national actors. This process is uneven and mixed, and can vary in different contexts depending on the depth by which the norm penetrates societies. Norms enter into and are accepted into national contexts depending on preexisting belief systems of a national society that support or constrain their acceptance. Norms can be propagated internationally by norm entrepreneurs (transnational actors, nongovernmental organizations [NGOs], and businesses acting as conveyor belts or conduits) or through imitation, learning, socialization, and competition.[57] The latter processes are often difficult to document empirically because of their epistemic or cognitive foundations. But they are important factors in explaining the spread and adoption of policies like Internet filtering. To understand the growth of cyberspace controls over the past decade, we need to better understand the mechanisms and dynamics of this diffusion internationally.

Imitation and Learning

Among theories of international relations of all stripes, there is a basic understanding that government policies are formed on the basis of the dynamic relations with other states in the international system.[58] Governments are outward looking as much as they are inward looking. When one government sees another doing something, the pressures may build to do likewise or risk being left behind. Studies of learning and imitation in international relations offer up a number of hypotheses that can be collected and imported into the study of cyberspace controls.[59] A number of anecdotes suggest that this is a potentially fruitful area of inquiry.

In the most elemental sense, states learn from and imitate each other's behaviors, speech acts, and policies. They borrow and share best practices, skills, and technologies. They take a cue from what like-minded states are doing and implement policies accordingly. Fear and "self-help" are among the most important and perennial drivers of imitation and learning. States implement policies based on reactions to what other governments are doing for fear of being left behind or overtaken by adversaries.[60] This dynamic may be particularly acute around cyberspace given the pace of technological change. As David Dolowitz and David Marsh explain, "Technology can also push governments into policy transfer because of the speed with which it forces change. Governments, not knowing how to deal with the issues technological advances create, turn to each other for precedents and ideas."[61] A current example of such a dynamic can be seen clearly in the rush by many countries to pressure RIM, the Canadian maker of BlackBerry products, to cooperate with local law enforcement and intelligence. After the United Arab Emirates went public with its concerns that RIM might have made an arrangement with the US National Security Agency that it wanted extended to its own security services, numerous other governments chimed in and joined the line, including India, Bahrain, Indonesia, and Saudi Arabia.[62]

The most intense forms of imitation and learning occur around national security issues because of the high stakes and urgency involved. For example, in reaction to revelations of Chinese-based cyberespionage against US companies and government agencies, former US director of national intelligence Dennis Blair asserted that the United States needs to be more aggressive in stealing other country's secrets. After reports surfaced of major compromises of the Indian national security and defense establishment traced back to the Chinese criminal underground, some members of the Indian government proposed legislation to give immunity and a stamp of approval for Indian hackers to do the same to China.[63] India also blocked imports of Chinese telecommunications equipment and moved swiftly to establish cyberwarfare capabilities within its armed forces.[64]

In what will be familiar to international relations theorists, we are now entering into a classic "security dilemma" arms race spiral in cyberspace as

dozens of governments look to other states' actions and perceived intentions to justify the need to bolster offensive cyberwarfare capabilities.[65] Cyberspace has many of the characteristics identified by international relations theorists as associated with exacerbating the logic of the security dilemma: offense is considered to be overwhelmingly dominant;[66] deterrence is difficult to implement because of problems around attributing the source of cyberattacks; there is a lack of transparency around many cyberspace information operations, which are typically undertaken behind a veil of secrecy; and, finally, the barriers to entry are low, to the point where even individuals can participate in consequential cyberattacks.[67]

The imitation and learning process is not uniform, but mixes with national interests and local culture to create a warp and woof.[68] Governments can look to other states in the international system to lend legitimacy to slightly modified or even altogether different policies. For example, after the United States and other industrialized countries adopted antiterror legislation, many countries of the Commonwealth of Independent States (CIS) did likewise. However, their policies were much more far-reaching and oriented more toward the stifling of minority independence and political opposition movements and the shoring up of regime stability than fighting international terrorism.[69] This process of normative reshaping around local circumstances and interests in this case conforms to Acharya's argument that a norm will more likely be adopted if it will enhance the legitimacy and authority of extant institutions and practices.[70]

A similar process can be seen in the spread of cybercrime and copyright protection legislation. Under the umbrella of an international norm intended for one purpose, states can justify policies and actions that serve more parochial aims. For example, Russia and other authoritarian regimes have used the excuse of policing copyright to seize opposition and NGO computers, in at least one case with the assistance of companies like Microsoft.[71] Similarly, the now widespread belief that it is legitimate to remove videos from websites that contain "offensive" information can be interpreted broadly in various national contexts. For example, Pakistani authorities have repeatedly pressured video hosting services to remove embarrassing or politically inflammatory videos under this rubric.

Some authoritarian and competitive authoritarian regimes that are otherwise geographically remote appear to be learning from each other's "best practices" when it comes to dealing with cyberspace controls over opposition groups. For example, a growing list of countries have banned short message services (SMS) and instant messaging services prior to national crises or significant events like elections or public demonstrations. Although it is possible that each of these countries is doing so in isolation, it seems more likely that inspiration is drawn from other countries' actions. India,[72] Cambodia,[73] China,[74] Mozambique,[75] Turkmenistan,[76] Egypt,[77] and

Iran[78] have all disabled SMS and text messaging during or leading up to recent elections, events, or public demonstrations as a way to control social mobilization.

Imitation and learning are major components of normative propagation, but they are processes that are difficult to document empirically. Unless government representatives or policymakers specifically point to an instance or act from which they are drawing inspiration, imitation and learning processes can be obscure and have to be deduced from behavior or practices.

Commercial Conduits

Norms can spread internationally carried by private actors and, in particular, by companies offering a service that supports the norm. For example, a major market for cybersecurity tools and technologies has exploded in recent years in response to pressing cybersecurity issues and the growing cyber–arms race. Companies are naturally gravitating to this exploding market in response to commercial opportunities. But they can also influence the market itself by the creation of products and tools that present new opportunities for states. There are, for example, a wide range of new products that offer deep packet inspection and traffic shaping capabilities in spite of the fact that such activities are contrary to fading norms around network neutrality at the heart of cyberspace governance. There are also companies that offer services and products designed for offensive cybernetwork attack operations. For example, during the events of the Arab Spring, Egyptian protesters broke into the headquarters of the Egyptian security services and discovered what appeared to be a contract between a German-UK company and the Egyptian security services for computer network exploitation products and services.[79] Naturally, the principals of these companies have a vested interest in ensuring the market continues to expand, which can in turn influence government policies.

The market for surveillance and offensive computer operations that has emerged in recent years was preceded and is supplemented by a market for Internet filtering technologies. The latter were developed initially to serve business environments, but quickly spread to governments looking for solutions for Internet censorship demands. ONI research throughout the 2000s was able to document a growing number of authoritarian countries using US-based commercial filtering products, including Smartfilter in Iran and Tunisia, Websense in Yemen, and Fortinet in Burma. More recent ONI reports document a Canadian company's products being used in Yemen, Qatar, and the United Arab Emirates.[80] Some of these products appear to have been tailored to meet the unique requirements of authoritarian regimes. For example, the Websense product had built-in options for filter-

ing categories that included human rights and NGOs. In one case, a PowerPoint presentation by the company Cisco (the maker of telecommunications routing equipment) surfaced in which the argument was made that a market opportunity presented itself for the company working in collusion with China's security services.[81] Commercial solutions such as these can help structure the realm of the possible for governments. Whereas in the past it might have been difficult or even inconceivable to engage in deep packet inspection or keyword-based filtering on a national scale, commercial solutions open up opportunities for policymakers looking to deal with vexing political problems on a fine-grained scale.

International Vacuums *(Horror Vacui)*

Absence of Restraints

One of the least obvious mechanisms of norm propagation is the absence of restraints. Policies, practices, and behaviors can spread internationally when there are no countervailing safeguards or checks. Norm diffusion through the absence of restraints might be likened to the principle of nature abhorring a vacuum. Practices and behaviors fill a void in the policy arena. This mechanism is perhaps the most difficult to pin down empirically because it lacks any identifiable source or location. Yet it may be among the most important global dynamics of the spread of cyberspace controls.

One might hypothesize that norm diffusion via the absence of restraints is most amenable to the diffusion of bad norms precisely because there are no countervailing restraints. For example, the spread of cybercrime, and the blurring of cybercrime and espionage, can be explained in part because of the ways in which these actors are able to exploit fissures in the international system. Bad actors act globally and hide locally in jurisdictions where state capacity is weak and beyond the reach of law enforcement where the victims are located. Some governments may even be deliberating cultivating a climate favorable for crime and espionage to flourish by their inaction. For example, major cyberespionage networks and acts of cybercrime have been traced back to China, Russia, and other countries that take little or only symbolic measures against perpetrators, in part because of the strategic benefits that accrue to these countries by the flourishing of those activities. These governments can reap the windfalls of the ecology of crime and espionage through the black market while maintaining a relatively credible position of plausible deniability.[82] The same logic might be applied to the market for offensive computer network exploitation and attack capabilities: in the absence of restraints to the contrary, businesspeople will seek out and exploit commercial opportunities of a growing cyber–arms race.

Conclusion

Consideration of the international dynamics and mechanisms of cyberspace controls is important for several theoretical and practical reasons. First, there are unique processes that occur at the international level distinct from what happens domestically. These dynamics and mechanisms help explain why a growing norm around Internet filtering and surveillance is spreading internationally. States do not operate in isolation, but are part of a dense network of relations that influences their decisions and actions. Without considering these dynamics and mechanisms, we may be missing some of the more important explanations for growing cyberspace controls that, up until now, have been primarily attributed to domestic-level causes. The framework that we provide in this article is meant to be a first step in identifying some of the most important sources of those dynamics and mechanisms.

The focus on the spread of cyberspace controls, as we outlined, may offer an important contribution to the study of international norm diffusion. Up until now, scholarship in this area has been focused predominantly on the propagation and diffusion of good norms such as landmines and chemical weapons bans, the abolition of slavery, and the spread of democratic values.[83] The examples we described show that propagation and diffusion of (what may be considered by some as) bad norms can happen along the same lines and employ some of the same dynamics and mechanisms. Further research into the spread of cyberspace controls may shed light on some unique dynamics and mechanisms employed by authoritarian or democratically challenged regimes. It is sometimes assumed that these governments are, by definition, inward looking and have an aversion to internationalism and multilateralism. Some of the examples we pointed out show, to the contrary, that these regimes have active international and regional engagements that are likely going to continue to grow.

Third, a focus on international dynamics and mechanisms underscores the iterative and relational quality of state behavior. States' actions and behaviors are formed very much in response to other states' decisions, often in unintended ways. This observation has important policy implications for democratic industrialized countries. The policies that domestic governments implement may be picked up on by authoritarian regimes to legitimize their actions at home in ways considerably different than their original intent. Unfortunately, there is not a lot that can be done to guard against this dynamic. But it is important to be alert to it and recognize it when it occurs. General statements about the war on terror or copyright controls can be turned into excuses for a broad spectrum of otherwise nefarious actions by authoritarian regimes. These dynamics also underscore the importance of consistency, transparency, and accountability in democratic regimes. For example, shortly after Secretary of State Hillary Clinton admonished governments for pressuring RIM to collude with security serv-

ices, the Barack Obama administration introduced legislation that would put in place precisely the same procedures as those requested by Saudi Arabia, the United Arab Emirates, India, and others. Governments are embedded in an international system and, thus, a dense network of social relations. One cannot understand the spread of cyberspace controls without understanding their international dynamics and mechanisms.

Finally, interpreting these developments through a constructivist lens at the international level can help clarify where those with aims to mitigate norm regression in cyberspace might direct their efforts. One of the principal characteristics of constructivism is the contingent and open-ended nature of international politics. While the trends we described here are powerful and reflect deep-seated dynamics and interests of major powers, they are not irreversible. A large and distributed social movement, which cuts across civil society, the private sector, and governments, exists with aims to protect and preserve cyberspace as an open commons of global information. While this movement faces an uphill struggle, the multiple ways in which cyberspace controls spread internationally can give a more detailed and precise road map for points of legal, regulatory, and discursive intervention and robust checks and balances. 🌐

Notes

Ronald J. Deibert is director of the Canada Centre for Global Security Studies and the Citizen Lab, Munk School of Global Affairs, University of Toronto.

Masashi Crete-Nishihata is currently research manager at the Citizen Lab, Munk School of Global Affairs, University of Toronto.

An earlier version of this article will appear in L. Diamond and M. Plattner, eds., *Liberation Technology: Social Media and the Struggle for Democracy* (Baltimore: Johns Hopkins University Press, 2012), and was presented at the International Studies Association annual conference, San Diego, 2012.

The authors are grateful to the following people for comments and assistance: Larry Diamond, Roger Hurwitz, Camino Kavanagh, Brenden Kuerbis, Marianne Lau, Marc Plattner, Ken Rogerson, Eneken Tikk, and Adam Senft.

1. The US Department of Defense presently defines *cyberspace* as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"; see US Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: US Joint Chiefs of Staff, 2010), p. 86. This definition acknowledges that cyberspace encompasses more than the Internet and is an interdependent network of technological infrastructure of which the Internet is one part. We further extend this definition to include the regulatory level (the norms, rules, laws, and principles that govern cyberspace) and the sphere of ideas through which videos, images, sounds, and text are produced and circulated among users.

2. R. Deibert, J. Palfrey, R. Rohozinksi, and J. Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press, 2008).

3. R. Deibert, J. Palfrey, R. Rohozinksi, and J. Zittrain, eds., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press, 2010).

4. For example, the OpenNet Initiative (ONI) has published an annual series of country and regional reports that are based on an empirical examination of country-level controls. The OpenNet Initiative is a collaborative partnership of three institutions: the Citizen Lab at the Munk School of Global Affairs, University of Toronto; the Berkman Center for Internet and Society at Harvard University; and the SecDev Group (Ottawa). Its aim is to investigate, expose, and analyze Internet filtering and surveillance practices in a credible and nonpartisan fashion. See OpenNet Initiative, http://opennet.net.

5. T. Hopf, "The Promise of Constructivism in International Relations Theory," *International Security* 23, no. 1 (Summer 1998): 171–200.

6. By "positive" and "negative," we do not mean to imply a normative judgment to the policies, but rather describe the processes around which policies are formed.

7. J. H. Herz, "Idealist Internationalism and the Security Dilemma," *World Politics* 2, no. 2 (1950): 157–180.

8. Margaret E. Keck and Kathryn Sikkink, *Activists Beyond Borders: Advocacy Networks in International Politics* (Ithaca: Cornell University Press, 1998).

9. Deepa Seetharaman, "Arms Makers Turn Focus from Bombs to Bytes," Reuters, 10 September 2010, http://in.mobile.reuters.com/article/AfricaInvestment10/idINTRE6893EI20100910 (accessed 6 June 2011).

10. Stephen M. Walt, "Is the Cyber Threat Overblown?" *Foreign Policy*, 30 March 2010, http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown (accessed 6 June 2011).

11. R. Abrahamsen and M. Williams, *Security Beyond the State: Private Security in International Politics* (Cambridge: Cambridge University Press, 2011).

12. Paul Kowert and Jeffrey Legro, "Norms, Identity, and Their Limits: A Theoretical Reprise," in Peter Katzenstein, ed., *The Culture of National Security: Norms and Identity in World Politics* (New York: Columbia University Press, 1996), pp. 485–486.

13. For an extensive treatment of "norm regression," see R. McKeown, "Norm Regress: US Revisionism and the Slow Death of the Torture Norm," *International Relations* 23, no. 5 (2009): 5–25.

14. T. L. Friedman, "Censors Beware," *New York Times*, 25 July 2000; Robert Wright, "Gaining Freedom by Modem," *New York Times*, 28 January 2000.

15. J. H. Saltzer, D. P. Reed, and D. D. Clark, "End-to-end Arguments in System Design," *ACM Transactions on Computer Systems* 2, no. 2 (1984): 277–288.

16. M. A. Lemley and L. Lessig, "The End of End-to-end: Preserving the Architecture of the Internet in the Broadband Era," *UCLA Law Review* 48 (2001): 925–972.

17. M. L. Mueller, "Net Neutrality as Global Principles for Internet Governance," Internet Governance Project, School of Information Studies, Syracuse University, http://internetgovernance.org/pdf/NetNeutralityGlobalPrinciple.pdf.

18. W. J. Drake, ed., *The New Information Infrastructure: Strategies for U.S. Policy* (New York: Twentieth Century Fund Press, 1995).

19. R. Deibert, J. Palfrey, R. Rohozinski, and J. Zittrain, "Access Contested: Toward the Fourth Phase of Cyberspace Controls," in R. Deibert, J. Palfrey, R. Rohozinski, and J. Zittrain, eds., *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (Cambridge: MIT Press, 2011).

20. N. Villeneuve, "The Filtering Matrix: Integrated Mechanism of Information Control and the Demarcation of Borders in Cyberspace," *First Monday* 11, nos. 1–

2 (2006), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1307/1227.

21. ONI uses the following technical methodology to verify Internet censorship. Lists of websites and keywords are collected that cover topics that might be targeted for censorship including pornography, gambling, international and independent news media, human rights, and political content. A data collection software client designed to query these predefined lists of URLs is distributed to researchers within countries suspected of engaging in Internet censorship. The list of URLs is accessed simultaneously over http both in the country suspected of Internet filtering and a country with no filtering regime (e.g., Canada). The data gathered from the country with no filtering is used as a control to compare the data from the country suspected of filtering. Where appropriate, the tests are run from different locations to capture the differences in blocking behavior across ISPs. See R. Faris and N. Villeneuve, "Measuring Global Internet Filtering," in R. Deibert, J. Palfrey, R. Rohozinski, and J. Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press, 2008).

22. H. Noman and J. C. York, "West Censoring East: The Use of Western Technologies by Middle East Censors, 2010–2011," OpenNet Initiative, March 2011, http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011.

23. R. Deibert and R. Rohozinski, "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet," in R. Deibert, J. Palfrey, R. Rohozinski, and J. Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press, 2008), pp. 123–149.

24. M. Crete-Nishihata and J. York, "Egypt's Internet Blackout: Extreme Example of Just-in-Time Blocking," OpenNet Initiative Blog, 28 January 2011, http://opennet.net/blog/2011/01/egypt%E2%80%99s-internet-blackout-extreme-example-just-time-blocking.

25. J. Cowie, "Libyan Disconnect," *Renesys*, 18 February 2011, www.renesys.com/blog/2011/02/libyan-disconnect-1.shtml.

26. OpenNet Initiative, "Nepal," 10 May 2007, http://opennet.net/research/profiles/nepal.

27. OpenNet Initiative, "Pulling the Plug: A Technical Review of the Internet Shutdown in Burma," 2007, http://opennet.net/research/bulletins/013.

28. OpenNet Initiative, "China Shuts Down Internet in Xinjiang Region After Riots," 6 July 2009, http://opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots.

29. B. Setlet and B. Stone, "Web Prices Lid of Iranian Censorship," *New York Times*, 22 June 2009, www.nytimes.com/2009/06/23/world/middleeast/23censor.html?_r=1&hpw.

30. British Prime Minister's Office, "PM Statement on Disorder in England," 11 August 2011, www.number10.gov.uk/news/pm-statement-on-disorder-in-england.

31. Bay Area Rapid Transit, "Statement on Temporary Wireless Service Interruption in Select BART Stations on Aug. 11," 12 August 2011, www.bart.gov/news/articles/2011/news20110812.aspx.

32. E. Zuckerman, "Intermediary Censorship," in R. Deibert, J. Palfrey, R. Rohozinski, and J. Zittrain, eds., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press, 2010).

33. J. P. Kesan and C. M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," Illinois Public Law Research Paper No. 10-35, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1805163; US Department of Defense, Strategy for Operating in Cyberspace, July 2011, www.defense.gov/news/d20110714cyber.pdf.

34. For criticism along these lines, see Robert O. Keohane, ed., *Neorealism and Its Critics* (New York: Columbia University Press, 1986).

35. Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999); Alexander Wendt, "Anarchy Is What States Make of It: The Social Construction of Power Politics," *International Organization* 46, no. 2 (1992): 391–425.

36. For a discussion of how international organizations can influence state behavior autonomously from their original design, see M. Barnett and M. Finnemore, "The Politics, Power, and Pathologies of International Organizations," *International Organization* 53, no. 4 (1999): 699–732.

37. For a review of the literature see R. Deibert and R. Rohozinski, "International Organization and Cybergovernace," in Robert A. Denemark, ed., *The International Studies Encyclopedia*, vol. 7 (West Sussex: Wiley-Blackwell, 2010), pp. 4203–4218; M. L. Mueller, "Internet Governance," in Robert A Denemark, ed., *The International Studies Encyclopedia*, vol. 7 (West Sussex: Wiley-Blackwell, 2010), pp. 4610–4627.

38. "Policy Statement by Igor Shchegolev, Minister of Telecom and Mass Communications of the Russian Federation," International Telecommunication Union plenipotentiary conference, Guadalajara, Mexico, 4 October 2010, www.itu.int/plenipotentiary/2010/statements/russian_federation/shchegolev-ru.html (accessed 6 June 2011).

39. See B. Kuerbis, "Reading Tea Leaves: China Statement on Internet Policy," Internet Governance Project, 8 June 2010, http://blog.internetgovernance.org/blog/_archives/2010/6/8/4548091.html (accessed 6 June 2011).

40. T. Gray, "U.N. Telecom Boss Warns of Pending Cyberwar," *TechNewsDaily*, 10 September 2010, www.msnbc.msn.com/id/39102447/ns/technology_and_science-security (accessed 6 June 2011).

41. "RIM Should Open Up User Data: UN Agency," *CBC News*, 2 September 2010, www.cbc.ca/news/technology/story/2010/09/02/rim-user-data-un.html (accessed 6 June 2011).

42. Tom Gjelten, "Seeing the Internet as an "Information Weapon," National Public Radio, 23 September 2010, www.npr.org/templates/story/story.php?storyId=130052701&sc=tw&cc=share (accessed 6 June 2011).

43. Jonathan Fildes, "UN Slated for Stifling Net Debate," *BBC News*, 16 November 2009, http://news.bbc.co.uk/2/hi/technology/8361849.stm (accessed 6 June 2011).

44. B. Kuerbis and M. Mueller, "Negotiating a New Governance Hierarchy: An Analysis of the Conflicting Incentives to Secure Internet Routing," *Communications and Strategies* 81 (2011): 125–142, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2021835.

45. M. L. Mueller and M. Chango, "Disrupting Global Governance: The Internet WHOIS Service, ICANN, and Privacy," *Journal of Information Technology and Politics* 5, no. 3 (2008).

46. M. Mueller, "Our Vaunted Multistakeholder Institutions Spring into Action," Internet Governance Project, School of Information, Syracuse University, March 2012, http://blog.internetgovernance.org/blog/_archives/2012/3/1/5008119.html.

47. B. Kuerbis, "Securing Critical Internet Resources: Influencing Internet Governance Through Social Networks and Delegation" (PhD diss., Syracuse University, 2011), http://surface.syr.edu/it_etd/65/; B. Kuerbis and M. Mueller, "Securing the Root," in L. DeNardis, ed., *Opening Standards: The Global Politics of Interoperability* (Cambridge: MIT Press, 2011).

48. See, for example, M. Mueller, M. van Eten, and B. Kuerbis, "In Important Case, RIPE-NCC Seeks Legal Clarity on How It Responds to Foreign Court Orders," Internet Governance Project, School of Information, Syracuse University, November 2011, http://blog.internetgovernance.org/blog/_archives/2011/11/23/4944.

49. G. Francis, "Plutocrats and the Internet," CircleID, 4 October 2010, www.circleid.com/posts/20101004_plutocrats_and_the_internet (accessed 6 June 2011).

50. A. Acharya, "Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule Making in the Third World," *International Studies Quarterly* 55, no. 1 (2011): 95–123.

51. For explanations of the attraction of regional organizations in this regard, see A. Hurrell, "Explaining the Resurgence of Regionalism in World Politics," *Review of International Studies* 21, no. 4 (1995): 331–358.

52. See A. Scheineson, "The Shanghai Cooperation Organization," Council on Foreign Relations, 24 March 2009, www.cfr.org/publication/10883/shanghai_cooperation_organization.html (accessed 6 June 2011).

53. R. Allison, "Virtual Regionalism, Regional Structures and Regime Security in Central Asia," *Central Asian Survey* 27, no. 2 (2008): 185–202; R. Weitz, "China, Russia, and the Challenge to the Global Commons," *Pacific Focus* 24, no. 3 (December 2009): 271–297.

54. R. Weitz, "What's Happened to the SCO?" *The Diplomat*, 17 May 2010, http://the-diplomat.com/2010/05/17/what's-happened-to-the-sco/ (accessed 6 June 2011).

55. S. Sirimanna, "Chinese Here for Cyber Censorship," *Sunday Times*, 14 February 2010, www.sundaytimes.lk/100214/News/nws_02.html (accessed 6 June 2011).

56. S. Stecklow, F. Fassihi, and L. Chao, "Chinese Tech Giant Aids Iran," *Wall Street Journal*, 27 October 2011, http://online.wsj.com/article/SB10001424052970204644504576651503577823210.html?mod=iPhone.

57. M. Finnemore, and K. Sikkink, "International Norm Dynamics and Political Change," *International Organization* 2, no. 4 (Autumn 1998): 887–917.

58. K. N. Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979); R. O. Keohane, *Neorealism and Its Critics* (New York: Columbia University Press, 1986).

59. B. Goldstein, "Imitation in International Relations: Analogies, Vicarious Learning, and Foreign Policy," *International Interactions* 29, no. 3 (2003): 237–267.

60. See K. Holzinger and C. Knill, "Causes and Conditions of Cross-national Policy Convergence," *Journal of European Public Policy* 12, no. 5 (2005): 775–796.

61. D. Dolowitz and D. Marsh, "Who Learns What from Whom: A Review of the Policy Transfer Literature," *Political Studies* 44, no. 2 (1996): 343–357.

62. "Factbox: BlackBerry Under Fire from States Seeking Access," Reuters, 4 August 2010, www.reuters.com/article/2010/08/04/blackberry-idUSLDE6720FI20100804 (accessed 6 June 2011).

63. J. T. Philip and H. Singh, "Spy Game: India Readies Cyber Army to Hack into Hostile Nations' Computer Systems," *Economic Times*, 6 August 2010, http://economictimes.indiatimes.com/news/news-by-industry/et-cetera/Spy-Game-India-readies-cyber-army-to-hack-into-hostile-nations-computer-systems/articleshow/6258977.cms (accessed 6 June 2011).

64. R. Blakely, "India Blocks Deals with Chinese Telecoms Companies over Cyber-spy Fears," *The Times* (London), 10 May 2010, http://business.timesonline.co.uk/tol/business/markets/china/article7121521.ece (accessed 6 June 2011).

65. The message sent by the establishment of the United States Cyber Command should not be underemphasized in this regard. Such an institutional innovation in the armed forces of the world's largest superpower sends a major signal to the defense community internationally.

66. H. Butterfield, *History and Human Relations* (London: Collins, 1951); J. H. Herz, "Idealist Internationalism and the Security Dilemma," *World Politics* 2, no. 2 (1950): 157–180.

67. We are grateful to Eli Jellenc of iDefense for suggesting these characteristics in an unpublished 2011 brief shared with us. See also R. Deibert, R. Rohozinski, and M. Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War," *Security Dialogue* 43, no. 1 (2012): 3–24.

68. For a general discussion, see J. Legro, "Which Norms Matter? Revisiting the 'Failure' of Internationalism," *International Organization* 51, no. 1 (Winter 1997): 31–63.

69. For example, a joint "antiterror" exercise was held in May 2011 between China, Kyrgyzstan, and Tajikistan in the Xinjiang region to coordinate efforts to suppress local revolts and separatist violence. See "China, Neighbours Hold Anti-Terror Drill," Agence France-Presse, 7 May 2011, www.rnw.nl/english/bulletin/china-neighbours-hold-anti-terror-drill.

70. A. Acharya, "How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism," *International Organization* 58, no. 2 (2007): 239–275.

71. C. J. Levy, "Russia Uses Microsoft to Suppress Dissent," *New York Times*, 22 September 2010, www.nytimes.com/2010/09/12/world/europe/12raids.html (accessed 6 June 2011).

72. H. S. Singh, "India's Top Court Delays Decision on Holy Site," CNN, 23 September 2010, http://edition.cnn.com/2010/WORLD/asiapcf/09/23/india.holy.verdict/index.html (accessed 6 June 2011).

73. P. Mankad, "Cambodia Bans Text Messaging," *Foreign Policy*, 30 March 2007, http://blog.foreignpolicy.com/posts/2007/03/30/cambodia_bans_text_messaging (accessed 6 June 2011).

74. A. Krishnan, "China: Will 'Crush Dalai Lama Clique,'" *The Hindu*, 2 March 2012, www.thehindu.com/news/international/article2954854.ece.

75. J. Gunter, "Mozambique: Government Interference in SMS Service," *Global Voices*, 21 September 2010, http://advocacy.globalvoicesonline.org/2010/09/21/mozambique-government-interference-in-sms-service (accessed 6 June 2011).

76. A. Nurmakov, "Turkmenistan: Instant Messenger agent.mail.ru Banned in Turkmenistan," *Global Voices*, 7 September 2010, http://globalvoicesonline.org/2010/09/07/turkmenistan-instant-messenger-agent-mail-ru-banned-in-turkmenistan (accessed 6 June 2011).

77. S. Ashour, O. el-Hadi, and M. Megahed, "SMS Messaging Restricted in Bid to Preempt Pre-election Activism," *Al-Masry Al-Youm* (English), 11 October 2010, www.almasryalyoum.com/en/node/194067 (accessed 6 June 2011).

78. N. Fathi, "Iran Disrupts Internet Service Ahead of Protests," *New York Times*, 11 February 2010, www.nytimes.com/2010/02/11/world/middleeast/11tehran.html?ref=global-home (accessed 6 June 2011).

79. See K. McVeigh, "British Firm Offered Spying Software to Egyptian Regime—Documents," *The Guardian*, 28 April 2011, www.guardian.co.uk/technology/2011/apr/28/egypt-spying-software-gamma-finfisher (accessed 6 June 2011).

80. H. Noman and J. C. York, "West Censoring East: The Use of Western Technologies by Middle East Censors," OpenNet Initiative, March 2011, http://open

net.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011 (accessed 6 June 2011).

81. B. Reese, "PowerPoint Presentation Appears to Implicate Cisco in China Censorship," *Network World*, 20 May 2008, www.networkworld.com/community/node/27957 (accessed 6 June 2011).

82. See Information Warfare Monitor and Shadowserver Foundation, *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, 6 April 2010, www.shadows-in-the-cloud.net (accessed 6 June 2011).

83. One exception is R. McKeown, "Norm Regress: US Revisionism and the Slow Death of the Torture Norm," *International Relations* 23, no. 5 (2009): 5–25.