Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

A New Normal? The Cultivation of Global Norms as Part of a Cyber Security Strategy

Roger Hurwitz

Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology

2013

This material is based on work supported by the U.S. Office of Naval Research, Grant No. N00014-09-1-0597. Any opinions, findings, conclusions or recommendations therein are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

MINERVA INITIATIVE
DEPARTMENT OF DEFENSE

14

A New Normal? The Cultivation of Global Norms as Part of a Cybersecurity Strategy

ROGER HURWITZ

Contents

States are facing a growing crisis of cybersecurity. With many state and non-state actors now having significant cyber attack capabilities, states need strategies that will protect their societies, economies, military, and governments from such disruptive or destructive attacks. The challenge is greatest for the technologically advanced countries, like the United States, whose power and welfare most heavily depend on computationally managed processes and global networks. Their strategies will accordingly need multi-faceted scope and global reach. This chapter argues that an important part of such strategies is the development of international cyber norms, or shared expectations among states regarding their behavior and responsibilities in cyberspace.

States' acceptance of a norm can constrain and regulate their behavior in specific situations, and, to the extent that other states are likely to sanction a state's violation of the norm, the constraint will be greater. States will adopt some cyber norms and willingly accept the associated constraints, because they have a common interest in sustaining and developing cyberspace. Many states have acknowledged the contributions of the Internet to their economic and social development, and they are already accustomed to following mutually beneficial rules at the cyber operational level, most prominently, the network protocols. However, not all cyber behaviors will soon fall subject to broadly accepted norms. First, some states will likely reject proscriptions of certain behaviors by means of which they pursue in cyberspace larger competition with other states (e.g., China's use of cyber espionage as part of a "catch-up" strategy in information and communication technology [ICT] undermines the US's valued technological advantage in that sector). There will also be contention over the formulation and extent of some norms, in part for symbolic reasons, but also because particular wording can confer material or political advantage to a contending party. For example, a norm that a state's control of its national cyberspace is a matter of national sovereignty that can trump, as needed, its citizens' rights to information would support China in struggles with the West over Internet freedom. Finally, a state may choose to selectively follow an accepted norm, but other states will be reluctant to sanction its violations for fear of additional conflict.

Given these exceptions, the time taken for the adoption of norms, and the efforts needed to assure compliance, whatever normative regulation might be achieved seems insufficient to meet the cyber threats. Defense strategy for a technologically advanced state will also need a "reasonable deterrent" capability and "technological transformation." "Reasonable deterrence" includes capabilities for near-real-time, reasonably confident attribution of an attack and for in-domain or cross-domain retaliatory capability sufficient to give an adversary pause. "Technological transformation" seeks to reduce the vulnerability of a state's digital networks, so that efforts to exploit them for cybercrime and espionage or to attack them will either fail outright or become too costly to mount. Together the three strategic components comprise a vulnerability-driven, defense-oriented cybersecurity strategy.

However, efforts to establish some cyber norms can still pay off, even if other countries choose a more aggressive strategy, such as a preemptory one that identifies and suppresses threat actors. If there are regulatory norms, it will be easier to identify such agents and organize collective actions against them.

Consideration of international cyber norms as part of a triad resonates with the US 2011 "International Strategy for Cyberspace," which called for the same triad. That document notes the declared interest of almost all states in preserving the openness and interoperability of the Internet, asserts the importance of norms in enhancing stability, and specifies cyber norms, which the United States will promote for adoption. However, it neither identifies the areas for which states would most readily accept norms nor judges how much their acceptance would stabilize cyberspace by increasing predictability and preventing misunderstandings. This chapter tries to supply these answers and some concepts for the utility of cyber norms. Accordingly, the first section discusses the conditions that led major cyber powers to issue a joint call for discussions of norms and the responses to that call. The second section examines these powers' very different views of what needs to be subject to norms or regulations. The third section distinguishes different areas for norms and identifies those for which discussions are most likely to produce widely accepted norms. Viewing these results, the last section evaluates their potential contributions to stability in cyberspace.

A Call to Discuss Cyber Norms

Since early 2010, many governments, including those of the United States, China, and Russia, have signaled a willingness to discuss international norms for cyberspace. A significant breakthrough occurred in January 2010, when the "UN group of governmental experts on information security" drafted a recommendation, subsequently approved by the General Assembly, that states "discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure."[2] In working on this call, both the United States and Russia changed their respective decade-old positions: the United States had wanted to restrict such discussions to cooperation on cybercrime; Russia had aimed for talks regarding the control of offensive uses of cyber. These changes most likely responded to spikes in the number and severity of cyber attacks, continuing doubts about cyber deterrence, recognition of a common interest in reducing the threats, and realization of the need for inter national cooperation to combat the criminal misuse of information technology, create a global culture of cybersecurity, and promote other essential measures that can reduce risk.

> According to the call, no state is able to address these [cyber] threats alone. Confronting the challenges of the twenty-first century depends on successful cooperation among like-minded partners. Collaboration among states, and between states, the private sector, and civil society, is important and measures to improve information security require broad international cooperation to be effective.[3]

The group of experts expressed concern that the lack of "shared understanding regarding international norms pertaining to state use of ICTs" risked misperceptions and "could affect crisis management in the event of major incidents" (i.e., provoke escalation). On this euphemistically expressed view, shared norms are instrumental: they help solve planning and coordination problems by standardizing the meaning of an action, so both the agent and target of an action know how it will be interpreted and the likely response to it.[4] Put another way, norms reduce the variability, and hence increase the predictability, of the human contexts in which action is taken. Agreements on particular norms, however arbitrary, may therefore be in every agent's individual interests and reachable, especially if dire consequences are predictable absent the norms.

This notion is conceptually distinct from one that grounds norms on "doing the right thing" and judges the validity of a norm, as Kant does, according to its universality. It is also distinct from an idea, based on Rawls, of norm as a course of action or principle everyone would follow (or not reject) if ignorant of one's specific circumstances when one chooses an action. These last two notions are closer to our commonsense ideas of morality. Contrary to realist theories of international relations, they seem relevant to the United States' and other liberal democracies' policies on human rights and some of their thinking on cyber norms. Thus the "International Strategy for Cyberspace" asserts that one basis of cyberspace norms is the principle that states must respect fundamental freedoms of expression and association, online as well as off. The problem here is that the American and other governments that include Internet freedoms on their lists of cyber norms do not recognize they are juggling two or more concepts of norms. As a consequence, they do not have a basis for prioritizing the norms they would like adopted. While the “International Strategy” does acknowledge that some norms it proposes will be accepted only by the “like minded,” it cannot identify the conceptual impediments to wider acceptance of these norms, much less how to address them. To be sure, the Russian and Chinese views that cyber norms be based on an inviolate principle of national sovereignty are no greater help i prioritizing norms for discussion and possible adoption.

National Positions for International Cyber Norms

Unsurprisingly, opportunities have been missed for moving on to substantive discussions. For example, the British government sponsored a conference in late 2011 with the announced purpose of laying out “cyber rules of the road.”[5] It showcased strong speeches on Internet Freedom, a riposte to an earlier Russian draft for a cyber convention that would have countries cooperate in suppressing online material that any country deemed a threat to its political stability. According to some apologists, the point was to split non-aligned nations from Russia and China. Yet the conference was ill-prepared by the British Foreign Office to deal with technical and institutional issues.[6] Such occasions suggest that the adoption of specific cyber norms will be hard won, and any set of widely accepted norms will be fairly limited in scope. As noted, the US cybersecurity strategy paper acknowledges that scenario: it anticipates that some cyber norms, favored by the United States, will be observed only among coalitions of the “like minded” (i.e., North Atlantic Treaty Organization [NATO] and some Pacific Rim allies). Since the United States is, of course, a participant to norms discussions, this view implies, at this time, that it will not consider compromise on some of its proposed norms in favor of more widely acceptable ones. It is not alone in this respect.

Broadly speaking, Chinese and Russian policymakers seek to extend the principle of national sovereignty to cyberspace by establishing a norm of the state being the final arbiter of matters relating to cyberspace in their territory.[7] Their likely motives are, first, to control the ideational space that cyber networks afford their populations, and, second, to prevent inquiry into their governments' or state proxies' uses of cyber for military campaigns, political espionage, industrial espionage, and crime. Russia, China, other members of the Shanghai Coordinating Organization, and other authoritarian governments consider the Internet a vector for dissident political information and organizing—one not easily suppressed, but easily exploited by external rivals, in particular the United States. Thus, when cyber-fueled protests occurred in Russia winter 2011–2012, their target, Premier and presidential candidate Vladimir Putin branded them the work of "foreign enemies,"[8] conveniently ignoring the grounds for the protests. On this view, outsiders in enabling dissent within a country do not contribute to its public debate; they are conducting "information warfare" to weaken regimes to the point of greater accommodation with them or even collapse. On that view, already in 2008, Russia, China, and other members of the Shanghai Coordination Organization (SCO) agreed to outlaw supporting or hosting the dissemination of socially disruptive information. In September 2011, in seeming response to foreign governments' and Diasporas' support for cyber activism in the Arab world, Russia proposed that countries log the online activities of their residents suspected of such disseminations, in order to facilitate the identification and suppression of such residents upon complaint of a target country. In practice, however, Russian governments have tolerated considerable online political discourse and protests, despite Chechen insurgents having used the Internet for publicity, recruitment, and coordination in their violent struggle against Russia. This relative openness might have several causes: the much greater emphasis placed by the governments on control of radio and television, strategies of government messaging competing with other online messages for trust, and lack of preparation for the sharp increase in broadband users over the past half decade.

China, on the other hand, has assiduously sought to control the online ideational spaces of its citizens by blocking access to many foreign sites, filtering queries, suppressing blogs, imprisoning bloggers, and taking other censorship measures. These are implemented both algorithmically and by hand to keep out material

> endangering state security, divulging state secrets, subverting state power, and jeopardizing national unification; damaging state honor and interests; instigating ethnic hatred or discrimination and jeopardizing ethnic unity; jeopardizing state religious policy, propagating heretical or superstitious ideas; spreading rumors, disrupting social order and stability; disseminating obscenity, pornography, gambling, violence, brutality, and terror or abetting crime; humiliating or slandering others, trespassing on the lawful rights and interests of others; and other contents forbidden by laws and administrative regulations.[9]

China's efforts and similar ones elsewhere, as in Iran or Belarus, where citizens' access to foreign sites was recently criminalized, hav sparked fears of cyberspace fragmentation and "Internet(s) in one country."[10] These practices represent an extreme in measures that a growing number of states—some liberal democracies among them—are taking to regulate their citizens in cyberspace. The milder measures can include banning online anonymity, prohibiting certain content, like child pornography, and requiring authorization of state security services to search users' data. While these steps can be justified as needed to prevent cybercrime, they imply that users' cyberspace is an extension of national territory and ultimately subject to a state's claim of sovereignty. It is interesting to note in this respect, an echo of the principle of "national sovereignty," as introduced in the Treaty of Westphalia (1648)—the "charter" of our current international system—to bar interventions by states to change the status of a religion in another state: *cuius regio, eius religio* (He who rules determines the religion of his realm).

In contrast, the United States and its NATO allies tend in their pronouncements to view cyberspace as a central institution for a global economy, a means for worldwide scientific and cultural exchange, a commons for political debate and development, and a social medium. Given this variety of its functions, there follows a multi-stakeholder model for cyberspace's control and defense, with states being one type of stakeholder, along with non-governmental organizations, service providers, ICT companies, critical infrastructure entities, corporate users, and individual users. Because cyberspace, particularly the Internet, is prey to attacks and exploits by criminals, terrorists, and even states, states, by virtue of their authority and capabilities, have primary responsibility to provide the needed security, without harming the interests of other stakeholders. Norms and treaties (e.g., the Budapest Convention on Cybercrime) are instruments for fulfilling such responsibility, as are the nurturing of a cybersecurity culture and capabilities around the globe.[11] This view of the Internet ignores the demographic and technological changes that are remaking cyberspace and expectations for it: the change from hundreds of millions of users concentrated in North America and Europe connected to the Internet through computers to billions of users, with the bulk in south and east Asia, connected through mobile devices, and the rise of an Internet of things. As a result, practices that might have once seemed in the interests of all are now controversial and contested.[12] As already noted, many regimes view the American opposition to online censorship and its provision of circumvention software as an effort to undermine them.[13] Similarly, the position that technologists be left free of political interference to decide cyber design issues is seen as a ploy to perpetuate US technological domination of cyberspace.

These differences are exacerbated by disagreements over the auspices for promulgation and monitoring of cyber norms as well as the administration of the Internet. American policymakers insist on the development of cyber architectures and protocols by independent groups, like the Internet Engineering Task Force (IETF), because that arrangement will keep the basic technologies of cyberspace free of political interference. China and many developing countries, however, consider such groups, as well as the Internet Corporation for Assigned Names and Numbers (ICANN) which administers the system of online identifiers, as vehicles for the US's continuing technological domination of the Internet. They contend that the shift in Internet demographics should give them a greater voice in running the Internet and consequently want either the International Telecommunications Union (ITU) or a new UN agency to become the key governing institution. The United States believes that China and other authoritarian states would dominate such an arrangement; they would use it to promote architectures that facilitate their control of domestic information flows and signal intelligence against adversaries. In short, the question of governance crystallizes the distrust among states regarding their respective exploitations of the Internet and many behaviors in cyberspace.[14]

Distrust and differences in concepts, interests, and experiences also separate the cyber powers with regard to the military uses of cyberspace, despite their desires to avoid escalatory conflicts and their agreement in principles. Almost all powers have signaled that they will consider cyber attacks at some level as rising to the level of "armed attack," and reserve the right to respond to it by all means, including the use of force, though none have indicated what that level might be or are likely to do so. With the possible exception of China, the major cyber powers also believe the law of armed conflict (LOAC) should apply to cyber attacks within the context of war: use of force limited to accomplishing military objectives, distinction between military and civilian targets, prohibition on excessive use of force, and efforts to minimize ancillary casualties.[15] There have been some bilateral discussions at the government advisory group level (Track 1.5 and Track 2 diplomacy) on how these constraints might apply to concrete situations of cyber conflict.[16] However, as discussed below, the lack of experience and public information on the effects of possible cyber attacks or of physical attacks on cyber infrastructures (e.g., underwater cables) will impede progress toward a broader understanding and agreements as to how LOAC should apply to cyberspace.

Doctrinally, Russia and China regard cyber attacks as part of information warfare that accompanies kinetic military activity and aims to undermine the adversary's capabilities for fighting, by disrupting its military organization and demoralizing its population. China places particular value on using cyber weapons to distract an enemy and to neutralize any advantages it has from technological superiority and intensely computerized C4ISR.[17] Russia has experience with but not necessarily enthusiasm for information warfare: during a bitter political struggle with Estonia in 2007, and its brief 2008 war with Georgia, the adversary states suffered distributed denial-of-service (DDoS) attacks on their telecommunications infrastructure, with consequent discomfort and even panic in their populations. The extent of Russian military involvement in these attacks, however, is not clear, since they were conducted by Russian hactivists and botnets were controlled by criminal gangs based in Russia.[18] China has not directly or indirectly engaged in information warfare, but it has conducted military, political, and industrial espionage, with the United States as prime target, so broadly that some US officials have described these activities as "economic warfare."[19] Some officials also fear that China may have planted malware or "logic bombs" inside American critical infrastructure and military networks to be activated in case of conflict.

The United States has been more aggressive than either of these countries in integrating cyber in its war-fighting capabilities and, probably for that reason, demonstrated less appetite for "arms control"–type talks. In the 1990s and early 2000s, the American military developed a notion of net-centric warfare—the intense networking of geographically dispersed forces for more effective collaboration that has been partly realized through construction of the Global Information Grid. A 2007 experiment at the Idaho National Laboratory suggested the US government's interest in new types of cyber attacks, as well as defending US critical infrastructure from them. This experiment, which some observers consider a precursor to Stuxnet, demonstrated that remote penetration and corrupt instructions to an electrical generator control system could bring the generator to self-destroy. The US Cyber Command—a dedicated military unit, stood up in 2010—presumably has acquired the capability of launching such attacks or equally damaging ones. Its commanding officer and spokespersons have recently noted that the command's primary mission is to integrate defensive and offensive cyber options in the military's six combatant commands.[20] The pattern of development and their remarks suggest that the primary focus of the offensive capabilities would be on thoroughly dismantling an adversary's military and military support networks rather than panicking its population.

Given the differences across states regarding the appropriate norms for facets of behavior in cyberspace, many states will find something objectionable in any comprehensive proposal and will likely reject it *in toto*. This proved the case with the proposal for an international code of conduct for information security submitted to the UN by China, Russia, Tajikistan, and Uzbekistan, and the previously mentioned Russian draft for a convention on information security presented at Ekaterinburg.[21] Each has provisions that all countries can accept (e.g., assisting countries in developing cybersecurity policies, calling for mediation in cyber conflicts). The liberal democracies dismissed them, however, because the first proposal embraced a very state-centric model for Internet governance, as opposed to a multistakeholder one, and the second called on states to curb the serving from their territories information that another state declares to under mine its security. These political interactions deepened the divisions of states into several contending camps or information orders, one grouped around the United States and its European and Pacific allies, another consisting of SCO members, and a third composed of "non-aligned" nations. The last group, as represented by India, Brazil, and South Africa, wants to give states, especially developing ones, a larger voice in policies and governance for the Internet perhaps through a UN-based agency to replace ICANN. However, it does not support the Russian and Chinese position on issues of information rights and censorship.[22]

Norms for Specific Cyber Behaviors

An obvious lesson of the interactions is that states should avoid presenting grand plans for international cybersecurity. Instead they should seek to develop norms in areas where their current practices have been mutually acceptable or where they have expressed strong interests for cooperation. The remainder of this paper concerns specifying norms that might satisfy these criteria. This discussion is informed by a workshop, in October 2011, on international cyber norms, organized by the present writer and Joseph Nye, as co-chairs, with a thirteen-person committee. The American and allied government officials, academicians, think tankers, and practitioners who attended the workshop discussed potential norms in six principal issue areas: (1) military operations; (2) political, military, and economic espionage; (3) cybercrime; (4) development of underlying technologies and supply chain management; (5) public-private partnerships; and (6) global information society and Internet freedom.[23] Table 14.1 presents the norms that attracted the most interest, but the table should not be viewed as a consensus, since any consensus finding process was deliberately avoided.[24] Because discussions were under the Chatham House rule, individuals cannot be credited now for proposals and comments that might be repeated here in part or in whole, but all the participants deserve credit for any value found in this report. Any errors are entirely those of this writer.

The tabled norms tend to reflect a Western vision of how cyberspace should be constructed, since workshop participants came only

Table 14.1 Possible Norms Tabled at a Workshop Hosted by Harvard Kennedy School Belfer Center, MIT CSAIL, and University of Toronto, Canada, 2011

MILITARY OPERATIONS IN CYBERSPACE	POLITICAL, MILITARY, AND ECONOMIC ESPIONAGE	CYBERCRIME	TECHNOLOGICAL FOUNDATIONS AND SUPPLY CHAIN	PUBLIC-PRIVATE PARTNERSHIPS/ DEFENSIVE COORDINATION	INTERNET FREEDOM GLOBAL INFORMATION SOCIETY
In principle, apply law of armed conflict (LOAC) to cyber military responses and operations	Banning of large-scale commercial espionage which could be promoted as a universal customary norm to multiple international bodies and incorporated in bilateral relations	Norm to ensure states and other stakeholders educate themselves on cybercrime, including with respect to the hiring of criminal hackers	States should recognize the international implications of their technical decisions and act with respect for one another's networks and the broader Internet	Governments should seek cooperation with the private sector to assure a clean and healthy Internet	Promote Internet freedom as a global norm, but allow for ambiguity to reduce friction regarding the standards of Internet freedom
Confidence-building measures such as cyber hotline, greater differentiation of cyber incidents, establishing mechanisms for crisis management, and de-escalation	Regulate trade in espionage and surveillance services by defense contractors in developed countries to authoritarian countries for use versus political dissidents	Distinction between low- and high-impact criminals and expectations for cooperation in the pursuit of high-impact criminals	States should act within their authorities to help ensure the end-to-end interoperability of an Internet accessible to all	Norm that limits or calls for arrangements that limit (or specifies circumstances for) surveillance and data collection by private companies	

A structural norm (practice) of military involvement in the protection of domestic critical infrastructure from cyber attack	Encryption of computers and cloud servers to inhibit theft of politically sensitive information (a la WikiLeaks)	Data retention and transborder accessibility for high-impact crime	Respect the free flow of information in national network configurations; no arbitrary interference with internationally interconnected infrastructure
Norms to routinely share information, assist in disaster or attack, cooperate in forensics, collaborate in analysis of attacks	Duty to warn and duty to assist; analogies to mandatory notification should be institutionalized at the international level in data sharing procedures among Computer Emergency Response Teams (CERTs) and North Atlantic Treaty Organization (NATO) allies		Globally accepted norms and standards to assure cyber supply chain, including third-party certification of production centers, third-party assurances of hardware and software, a certification architecture enabling trusted chains of custody for components
	Letters of marque, issued by states to license private parties to pursue cyber spies		“Naming and shaming” of insecure producers, and barring their sales to government and defense sectors

from the United States and its allies. Yet the decomposition of cyberspace into issue areas enabled participants to evaluate the ripeness of facets of cyber behavior for formalization and the readiness of governments to accept the formulas as norms. Where possible, the proposed norms are distinguished as to whether they articulate principles for cyberspace, including norms for dealing with states of exception, like conflicts, or recommend best practices and operating rules.

Military Operations

Existing international laws specify neither the types of cyber operations that a targeted country could legitimately consider grounds for war (*ius ad bellum)* nor the constraints on cyber operations a country needs to observe in war (*ius in bello*). Governments have avoided specifying redlines whose crossings would provoke their retaliation, including armed response, for fear that would effectively license adversaries to mount less injurious operations. This reluctance is understandable and consistent with deterrence theory, which argues that leaving an adversary to guess whether an attack might provoke retaliation may be enough to deter the attack. However, this leaves the international community without shared expectations as to the limits of peacetime cyber behaviors, on one hand, and responses from countries subject to attacks, on the other. The uncertainty is compounded by the abilities of non-state actors to mount serious cyber attacks on one state from the territory of other states, and by the absence of norms that hold states responsible for preventing such attacks.

The short history of international cyber conflict provides few landmarks for this uncharted area. The 2007 DDoS attack on Estonia did not provoke retaliation from Estonia's NATO allies, although according to some reports Estonia did ask for some response under Article 5, the collective security provision, of the NATO treaty. With that attack in mind, an advisory group, headed by former US Secretary of State Madeleine Albright, recommended in 2010 that NATO's new strategic doctrine specify that transborder cyber attacks on a member state would ordinarily trigger consultations (Article 4) and certain attacks might even warrant a response under Article 5.[25] NATO, however, passed on this recommendation, preferring a policy of deciding the appropriate response on a case-by-case basis. Similarly, the

DDoS attacks on American government sites apparently did not warrant retaliation, even had the government been able to attribute them to a state actor with a reasonable confidence. (Although the North Korean military or security service was suspected to have launched the attacks, they were originally controlled from South Korea, then from US and European sites, with little evidence of a North Korean link.) The Stuxnet attack, which damaged rather than just disrupted Iranian facilities, generated no timely overt response from Iran, not even a complaint against unknown, presumably state, actors for endangering international security. Iran's leaders, of course, had their reasons for not responding: any complaint would draw more scrutiny to their nuclear program targeted by the attack and reveal-more vulnerability of their facilities. Other governments were also silent, some perhaps having been complicit in the attack, and many, no doubt, applauding this sabotage of the Iranian nuclear program.

The lack of forceful responses by the victims in these episodes may indicate a common uncertainty about the gravity of cyber attacks and a reluctance to extend, possibly escalate, a conflict over them. States might not be bluffing when they declare a right to respond to cyber attacks by any means, but in practice they seem either to have no clear redlines or, if they do, no attacks, so far, have crossed them. Scholars of international law and other observers have addressed this void with greater certitude, with at least one characterizing the disruption of critical infrastructure in Estonia as rising to the level of "armed attack."[26] Others set the bar higher, at Stuxnet-like attacks with the potential to destroy infrastructure like nuclear reactors and produce lethal results. In their opinion, these now apparent possibilities should prompt states to agree to prohibit certain types of attacks and to provide remedies for them, such as the right of a state under cyber attack to assistance from other states.[27]

This recommendation is not far fetched, especially if, absent generally accepted redlines, national security officials evaluate cyber attacks on a case-by-case basis and weigh responses to them with the traditional criteria for evaluating kinetic attacks, viz., scope, duration, and lethality. Applied to cyberspace, these criteria would distinguish between disruptive and damaging attacks and restrain military responses to the disruptive ones. Talks that affirmed the applicability of these criteria could get broad support from states and reduce the threat of escalation from relatively minor disruptive attacks. Adoption of these criteria would not rule out the use of force in response to damaging attacks, but the talks could help create a bias against it by advocating several norms, with potential for widespread acceptance, that would mitigate the damage and help identify parties responsible for the attacks. These include an e-SOS or "duty to assist" that requires states to offer help to a state whose cyber-based infrastructures were damaged, a related duty of states to inform others of malware threats they have discovered, cooperation in forensics, and a commitment to seek mediation for cyber-related conflicts.

As noted above, cyber powers, with the exception of China, agree that LOAC should apply to cyber conflicts. However, developing rules of engagement based on its principles of proportionality of response, avoidance of civilian targets, and minimization of ancillary casualties may prove difficult. There is little experience of cyber attacks in war-like contexts and insufficient knowledge of their consequences. While, according to the cliché, the damage done by a bomb of a particular size is well known, that for a cyber attack on a military network or critical infrastructure is not. It can depend as much on the configuration of the target's networks as on the intended scope of the attack. Moreover, cyberspace does not easily afford the distinctions upon which rules of engagement for "meat space" rely, viz., military vs. civilian, attack vs. espionage, state vs. non-state agents, intentional vs. accidental. For example, the US military uses civilian networks in over 90% of its communications, and the figures are probably similar for other militaries. Although international dialogue has begun about measures that might sharpen the distinctions (e.g., digital equivalents of insignia, on packets to indicate their military or humanitarian content), many points need to be addressed.[28] Also for such dialogue to reach results that are applicable to future cyber conflicts, states will need to disclose some of their cyber offensive capabilities and plans for using them.

Two other military-related issues can concern strategies that seek to stabilize cyberspace by promoting appropriate norms: the responsibility of states for attacks originating in their territories, perpetrated by non-state actors, and the involvement of the nation's military in the protection of domestic critical infrastructure. Acceptance of a norm that held states responsible for such attacks would be consistent with current international law for kinetic attacks, with UN efforts to foster a worldwide culture of cybersecurity and with efforts to curtail certain states' use of proxies. However, there might be difficulty in reaching agreement on the appropriate norm because of the various current suggestions as to what cyber attacks rise to a hostile act or armed attack. Some commentators who consider the 2007 DDoS attack on Estonia an armed attack emphasize the mental anguish Estonians suffered because of disrupted online services. Since authoritarian governments consider dissident political speech to disturb their countries' social stability, they could plausibly argue that under this definition, other states that allowed dissidents to communicate from their territories could be blamed for permitting "hostile acts" or "armed attacks." Hence, it might be sensible for the United States and its allies to support a distinction between disruption and damage before proposing a norm of a state's responsibility for cyber attacks originating from its territory.

The United States and many of its allies are currently deliberating about the role that their respective militaries should play in defending from cyber attacks critical infrastructures, which serves their civilian populations. Some officials believe the militaries should take a lead role or a co-equal one with any civilian agency, because the militaries are better resourced and, noted above, depend on the infrastructures. Others are uneasy with the idea because of its implications for the civil-military relationship in their states. Traditionally the militaries have been outward directed, with police and other security agencies responsible for internal protection. Also, giving the military a lead role in responding to an attack on the infrastructure could bias the conflict process toward retaliation and escalation, rather than resilience and recovery, because it introduces an offensive option. The current consensus in the United States and among its NATO allies is that the militaries should share in protecting the civilian networks, but let civilian agencies take the lead. However, the allocation of roles will likely be made country by country, as a matter of internal politics, so it is probably pointless to seek a global standard or best practice for the institutional arrangements.

Military, Political, and Economic Espionage

The use of cyber technology for espionage raises questions about the current norms that permit espionage under international law but allow its prosecution under domestic law. This is because:

- The technology allows the theft of secrets and intellectual property on an unprecedented scale.
- The spying at this scale is done remotely (electronically or digitally), leaving the victim with little in-domain recourse other than "naming and shaming" the perpetrator (i.e., no imprisonment or expulsion of captured spies).
- Cyber systems used in espionage and other intelligence, surveillance, and reconnaissance can blur the line between exploit and attack, causing damage and disruption as well as loss.

Given the traditional understanding of political and military espionage as needed for national security planning and preparation, proposals for their restriction would seem to have little chance of gaining traction. Nevertheless, because the scale of the cyber espionage may provoke aggressive responses from its victims, which in turn would destabilize the international system, some informal, unpublicized understandings might be reached on a bilateral basis as to an accepted level of espionage. In any case, the United States and many of its allies will insist that industrial espionage by state actors is condemned by international law, since it is not motivated by a national security concern or part of anticipatory self-defense. The question is whether this espionage should be considered "economic warfare," which threatens international security, or more an unfair trade practice, which can be redressed by economic penalties. The latter view has the advantage of leading to the decomposition of the charges of espionage to individual cases or types of cases, with some dissipation of the grievance. That consequence can be important, since almost all the industrial espionage has been attributed to China and its principal victim, the United States, has progressed from annoyance to extreme irritation with China over its practice.

Can the United States and like-minded states effectively promote and sufficiently enforce a norm banning industrial spying, so that it might eventually be widely accepted and followed? One model proposed for such an effort is the "proliferation security initiative" (PSI) in nations that through bilateral and multilateral agreements have committed not to traffic in weapons of mass destruction and to act to interdict shipments of such materials. Adherence to the PSI grew from a core of eleven nations to nearly one hundred in less than a decade, despite controversy over the legality of interdiction on the high seas and opposition from China and many non-aligned nations, including India and Indonesia. For a comparable initiative on industrial espionage, the United States and other interested countries would need laws enabling them to try in their own courts foreign nationals and companies for economic espionage originating outside their national boundaries. Prosecution of the same suspects by a number of states might both end the suspects' espionage and force the World Trade Organization (WTO) to develop specific rules and remediation for industrial espionage that states could enact (e.g., damage awards against offending companies, tariffs against-existing states). One major obstacle for this scenario is, in contrast to the PSI, which spoke to the fears of many nations over weapons of mass destruction, only the United States and a few other states with major intellectual property stores are victimized by the industrial-espionage. Consequently, gaining broader support would depend less on exemplary cases against the espionage but more on the expenditure of diplomatic and political capital—similar to the expenditures by advanced countries to get less developed ones to support their proposals for global copyright and patent protection—in changing domestic laws, assessing the extent of damages, and providing evidence for the charges in domestic courts and international forums. Moreover, the prosecutions of alleged spies, even under new enabling legislation, might prove difficult: many companies will shy at explicitly identifying what properties were stolen, while intelligence agencies may be reluctant to provide the evidence they have for fear of disclosing their sources or their own espionage activities. Galvanizing the international community against industrial espionage should be a goal for its victims, but without a compelling model for doing so, it should not be a high-priority goal. Perhaps more can be accomplished in serious bilateral talks between the respective victims and the chief culprit.

The daily reports of successful penetrations of cybersecurity by unknown hackers indicates that enhanced cybersecurity awareness and hygiene, as called for in the UN resolution noted above, will do little to halt cyber espionage of any type. Because the incumbent cyber technologies are vulnerable, states and non-state actors will find ways to get to the targets of their choice. The value to their take, however, could be reduced by adherence to a norm at the operational level of end-to-end encryption or, failing that, encryption enablement of computers and servers that host politically or economically sensitive data. Enabling these practices should be one goal of international cooperation for capacity building in less developed countries.

An issue related to espionage is the surveillance (and censorship) by governments of their own citizens' online activities, often accomplished in less developed countries with technologies acquired from developed ones. For states that are committed to a global human rights agenda, such surveillance threatens the citizens' rights for information, expression, and political association. One response has been proposals of norms among like-minded states that would impose or broaden existing export controls on the technologies. Such an initiative can prove effective quickly, because the technology suppliers are mainly in a small number of liberal democracies, where public opinion in support of such controls can be grown. In some cases, public reports that a company has supplied an obnoxious regime with such technology has already caused the company to claim it has or will stop the supply. At the operational level, however, there needs to be some distinction between "lawful" and "unlawful" use of the technologies so that vendors will cooperate in enforcing the norms, rather than fear significant loss of sales.

Cybercrime

Strategies that promote international cooperation to combat cybercrime are vital for the stabilization and positive development of cyberspace. This is because cybercrime organizations breed new attack techniques, which can then be acquired by states, and the capabilities of these organizations, when augmented with outsourced specialized skills, can exceed those of almost any state acting alone. Yet a strategy that would focus on international cooperation for the apprehension and prosecution of cyber criminals now faces the choice of promoting the expansion of the Budapest Convention on Cybercrime or advocating a new treaty. The United States and other supporters of the convention argue that it sets a standard for international cooperation in investigating and prosecuting cybercrime, notwithstanding its having acquired only thirty-one signatories over a decade. Critics fault the convention for being regional in character, deficient in provisions for handling data, and outdated by the new types of cybercrime, which have accompanied the exponential growth of Internet use, proliferation of mobile devices, and the emergence of an Internet of things (devices).[29] They also note that many states in the East and South will not join the convention because of its North Atlantic origins.

However, a strategy that campaigns for either the old treaty or a new one might not be cost effective in reducing crime. There will be costs in trying to overcome the resistance that many states will have to joining. There are a variety of reasons for this resistance. Russia and some other states will not easily end policies of giving safe harbor to cyber criminals in return for their intelligence gathering and plausibly deniable offensive cyber operations (e.g., DDoS). Some states will be concerned about limits to their national sovereignty, changes in their criminal laws and procedures, or data retention practices that a new treaty or a revised Budapest convention will require.

Undoubtedly there are benefits from a treaty, including standardizing investigatory procedures at an international level, harmonizing some laws across states, and possibly retarding the growth of cybercrime in member states. Apparently a state's membership in the Budapest convention correlates with fewer cyber attacks originating from its territory than from a demographically comparable nonmember state.[30] Possibly joining the convention signaled that the state would henceforth be more cybersecurity aware, and the criminals consequently relocated their operations to more permissive places.

Nevertheless, the promotion of norms that reduce either the vulnerability of users or the incentives for criminals might more easily produce similar effects on the levels of cybercrimes. These norms include information sharing and a duty to warn (or inform). The duty to warn or inform becomes increasingly relevant with the growth of situations where individuals, organizations, or governments are unaware that (1) their information systems are at risk, (2) their data have been stolen, or (3) new organizational routines can produce new vulnerabilities. This duty has already been partially formalized at domestic levels by laws mandating notification of security breaches. It has begun institutionalization at the international level in data-sharing procedures among Computer Emergency Response Teams (CERTs) and regional organizations of states (e.g., NATO). Cloud vendors and tier-1 ISPs, whose operations are not confined to any one state, should also be subject to such norms and laws, although there is no appropriate supervisory authority at this time. Because of their alignment with the UN resolution on cybersecurity, such norms can gain widespread acceptance but will probably not become ubiquitous in practice. Some states and organizations will ignore these expectations due to their imposition of processing costs, reputational risks, and disclosures of possible improprieties in data collection. Moreover, some old vulnerabilities will persist and new ones will be created and with them cybercrime. For that reason, a strategy should also deter cybercrime by promoting passive measures that interfere with criminals' getting their payoffs (e.g., blocking the ways that stolen information is monetized).

This approach, which emphasizes prevention over apprehension, does not preclude cooperation between members and members of the Budapest convention in the investigation of cyber crimes. It recommends that rather than seeking a comprehensive framework for such cooperation, arrangements be developed in the context of bilateral relations, such as extensions, where needed, of mutual assistance treaties, or on a more informal, *ad hoc basis*. To that end, states, such as the United States, which are zealous in the pursuit of cybercrime will need to convince states like Russia and China that such cooperation is also in their interest, possibly by seeking cooperation only in cases of major criminality (e.g., terrorism) or regarding online activities that are unambiguously criminal in the respective jurisdictions (e.g., child pornography). Successful instances of cooperation in such cases can provide reusable routines and encouragement for more cooperation. Thus, China's Minister of Public Security said, after an unprecedented operation involving his police and the US FBI closing down a child pornography ring: "Although China and the U.S. have different judicial systems and cultural values, the two sides share a common view in crime-fighting." The Minister then pledged China would continue to strengthen its law enforcement cooperation with foreign countries and vigorously fight transnational illegal activities, especially crimes committed through the Internet.[31]

Technological Foundations

On the American view, conflict over the development, operations, and supply of equipment for the Internet can be minimized if, as a rule, decisions are based only on the technological merits of the various options and all parties aim for an open and safe Internet, without hidden vulnerabilities. The Chinese government and other governments in less developed nations tend to see demands to that end as subterfuge for maintaining US technological domination of the Internet. It therefore appears sensible for the United States and other states that want to keep technological matters in the hands of technologists to seek support for that position from the technical communities in these states. However, several factors may prevent such a strategy from being effective in gaining acceptance for a norm of technological independence. First, the technologists in developing countries have not yet or are just beginning to work with international bodies that have roles in developing cyberspace (e.g., Internet Engineering Task Force [IETF]) or assuring its security (e.g., International Organization for Standardization [ISO]). Second, the technologists in some of these countries might not have the freedom to take positions that conflict with their governments' views. Third, the standards bodies, which the United States trusts, have not yet worked out standards at the international level for cloud and mobile computing and supply chain assurance.[32] So to ask technologists to support the norm is tantamount to asking them to take on faith that such bodies will do the right thing.

A fallback position, then, in the effort to keep development and operations in cyberspace free of political interference at national levels is for the United States and like-minded nations to articulate principles that approximate the list below, without expecting or demanding that other states will immediately accept them:

- States need to recognize the international implications of technical decisions made at the national level, and act with respect for each other's networks.

- States should act within their authorities to help ensure end-to-end interoperability and accessibility to all.
- States should respect the free flow of information in national network configurations, ensuring they do not arbitrarily interfere with internationally interconnected infrastructures.
- States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse.

In the meantime steps can be taken to route around countries that do not follow such principles; the consequent loss of transit revenues or complaints about degraded service might then nudge governments in question toward accepting these principles.

A strategic goal with greater priority is winning commitments to norms and standards that assure the integrity of the supply chain, since that is key for trustworthy ICT. It is important that such expectations be shared widely among consumers so that there will be pressure on producers to satisfy them. Foreseeable operational norms or standard practices would involve third-party certification of production centers, third-party assurances of hardware and software, a certification architecture enabling trusted chains of custody for components, "naming and shaming" of insecure producers, and barring their sales to government and defense sectors. There might initially be a need for incentives or government pressure for large corporations on both the supply and consumer sides to enter such a system. Ultimately, however, the spread and strength of these operational norms will depend on education of consumers and market mechanisms: perceptions of better quality, on one hand, and suspicions of possibly compromised ICT, on the other, can drive the growth of a market segment for secure hardware and assured software. The development of such norms is something of a necessity for most states. The alternative is for states to directly control the manufacture of components for military and critical infrastructure, as the United States now does to some extent and China and Germany are planning to do. But that would be too costly for many states, and providing the needed, trusted oversight could be beyond their capabilities.

Public-Private Partnerships

The UN resolution for cybersecurity, various national strategy papers, and even the Russian draft convention for international information security expect the private sector to play a significant role in protecting cyberspace. Consequently, there should be support for a campaign to encourage states to develop organizational frameworks or at least working relations with local and international private companies to accommodate this participation. The acceptance at the operational level of such a norm can create a "win-win" situation: The companies frequently have more capabilities and practice in dealing with threats in cyberspace but often need authorization from states to act more effectively, as demonstrated by the collaborations against Conficker and other recent malware pandemics.

These collaborations of ISPs, vendor, some governments, and researchers reveal the presence of several "invisible norms," or regular practices, based on the willingness of system operators to cooperate in keeping their networks clean. Because of Conficker's extent, the collaboration grew to over one hundred top-level domain operators and Microsoft in daily touch with ICANN and less frequently with governments. These partners implemented an extensive strategy of prevention, through blocking botnet command and control sites, and remediation, through the disinfection of host computers. This collaboration exposed the difficulties of cooperation at the legal/policy level compared with the relative ease of cooperation at technical levels. In some countries, there was a need to work around legal hurdles, for instance, contractual barriers to take down, anti-trust laws, and protection of privacy. Major legal difficulties were avoided because the prevention strategy could be implemented locally, through blocking at the name (for the C&C) resolution level, and did not require any transborder activity. But despite their success, the anti-Conficker Cabal and other anti-malware collaborations had an *ad hoc* character, with ICANN and other stakeholders lacking the authority to institutionalize the mechanism.

The organizational form for the public-private partnerships will vary over states. In some European countries, these partnerships are well developed for many sectors, and domestic laws to support them are in place. In other countries ICT trade groups exist for information sharing, but governments have sometimes lagged in connecting to them. In less developed countries, there are few such partnerships. National and international organizations, with experience in public and private-sector partnering on economic matters (e.g., the Asian-Pacific Economic Cooperation [APEC]) should be encouraged to guide and nurture the growth of partnerships in such places. However, governments and companies might have different visions and desire different tempos in implementing their partnerships. For example, companies like Goldman Sachs or Lockheed Martin, which operate globally, will want to harmonize the rules across countries, while a government, even if it views itself as an enabler, will face local and legacy issues that might keep it from accepting such norms. Also, some companies might anticipate that by meeting the standards set in their cybersecurity partnership, they can deflect regulation by the government partner in the future. A government agency that suspects such a motive might then move cautiously in such a partnership. In view of these possibilities, perhaps the most states can expect of one another—and what can be formulated in a norm—is that they will seek partnerships with the private sector to assure a clean and healthy Internet.

Internet Freedom and a Global Information Society

As noted earlier, Internet freedom or the free, unfettered flow of information, is the most contentious issue regarding daily operations of the Internet and governments' positions on the Internet's administration and future. This is both a human rights and a cyber issue, since the rights to information, expression, and association have underpinned the use and growth of cyberspace. Yet that growth has led to pushbacks from states whose political and cultural traditions are quite different from those of the liberal democracies where cyberspace first developed. While paying lip service to human rights, these states have claimed that national security concerns, such as internal social stability and terrorist threats, require some restrictions on these rights. In some cases these claims are self-serving and protect authoritarian regimes. In others, they can be partly justified by evidence of ethnic violence or insurgency. In any case, in response to the cyber fueled upheavals in the Middle East, states have increased their restrictions on Internet and social media use. More than forty countries are now involved in developing second- and third-generation filtering techniques.

These circumstances will thwart the effort by the United States and like-minded liberal democracies to gain general acceptance of Internet freedom as a cyber norm. The effort can be seen as divisive. It can also be subject to the criticism that the free flow- of information is no longer, if it ever was, an essential driver for development of the Internet, especially now that the economic and social uses of the Internet eclipse the political ones. Critics can also attack the American commitment to openness of information as hypocritical: they can note the readiness of the US Congress to mandate blocking access to certain hosts for commercial reasons (copyright protection), much like China and other states block access to sites for political reasons, and the questionable treatment of the American soldier who downloaded classified material to WikiLeaks.

The bleak prospects for a global norm should not stop a group of like-minded states from adopting norms of openness and unfettered information flows. However, a more fruitful long-term discussion would concern the limits to online dissent and disruption, because even the most liberal states have secrets, resources, and operations to protect. The norm that might emerge from such discussions would almost certainly allow for different and situation-specific standards of free information flows and thereby reduce some of the frietion regarding Internet freedom.

Conclusions

The establishment of norms of behavior for international cyberspace quintessentially fits what international relations theorist Arnold Wolfers called a “milieu goal.” By that he meant situations, patterns, or regularities whose attainment would enable a state to maintain its position in an international system or more easily obtain more tangible assets, which Wolfers called “possession goals.”[33] Because states are interconnected and interdependent in cyberspace, on one hand, and threat capabilities have proliferated rapidly, on the other, an optimal milieu pertains when all states accept the same norms and these tend to conflict avoidance and non-interference. For that reason, state officials who believe that the acceptance of norms by states can help secure their state's cyber activities should promote only a small number whose acceptability has already been signaled by key actors. The review of candidate norms identified five meeting these criteria:

- States should distinguish between disruptive and damaging cyber attacks and evaluate a damaging attack on the basis of its scope, duration, and lethality.
- States have a duty to assist other states that have suffered a major cyber attack or disaster, and also have a duty to inform others of new threats in cyberspace.
- States should cooperate in the certification of ICT supply chains.
- States whose territories or citizens are involved in transborder cyber activities that are unambiguously criminal in their states should cooperate in the investigation of these crimes and the apprehension of their perpetrators.
- States should enable the formation of public-private partnerships for cybersecurity, which include both local and international ICT companies operating in their territories.

These potential norms can win widespread support for two reasons. First, with the exception of cooperation in criminal investigations, they are directed toward reducing vulnerability and confrontation rather than in suppressing threat actors. In some sense then, they demand less action from the state actor, but if all states behave according to these norms, there will be significant reduction in threats and conflicts. Second, these norms are more concerned with maintaining cyberspace for all states rather than satisfying particular parties' agendas. Put another way, they are *status quo* oriented. They respond to that vision of the Internet as a network whose value grows with the number of its users and thus to an expanding positive sum or classic cooperative game. There is, of course, a concurrent competitive game being played between states over this same game board, with rewards, such as status and power, that lie beyond it. For that reason, cybersecurity strategies need the additional components of technological transformation and "reasonable deterrence."

Endnotes

1. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
2. United Nations General Assembly A/65/201; 7/30/2010. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, http://unidir.org/pdf/activites/pdf5-act483.pdf (retrieved February 1, 2012).
3. Id.
4. As demonstrated by the collaborations among cyber security practitioners, companies, and government agencies in response to the Conficker worm, effective international cooperation can be realized *ad hoc*; see M. Bowden, *Worm: The First Digital World War* (New York, 2011). The problem is the lack of ways to institutionalize such success and remove impediments to it for the next time.
5. Perhaps an echo of the "information superhighway" image?
6. London Cyber Conference: Don't be vague, listen to Hague, *The Economist*, November 2, 2011, http://www.economist.com/blogs/newsbook/2011/11/london-cyber-conference; P. Apps, Disagreements on cyber risk east-west cold war. Reuters, February 3, 2012, http://www.reuters.com/article/2012/02/03/us-technology-cyber-idUSTRE8121ED20120203.
7. See the Russian draft for a "Convention on International Information Security," presented to the International Meeting of High-Ranking Official Responsible for Security Matters, Ekaterinburg, Sept. 21–22, 2011, isocbg.files.wordpress.com/.../russian-draft-un-cyber-convention-english.doc
8. Bohm, Michael. Putin Chasing Imaginary American Ghosts, *The Moscow Times*. http://www.themoscowtimes.com/opinion/article/putin-chasing-imaginary-american-ghosts/452802.html.
9. Information Office of the State Council of the People's Republic of China, The Internet in China. June 8, 2010. http://www.china.org.cn/government/whitepaper/node_7093508.htm, q.v. "Protecting Internet Security."
10. Extensive literature, particularly Deibert et al., ed., *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (Cambridge, MA: MIT, 2010); *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (Cambridge, MA: MIT, 2011). On Iranian efforts to create a national Internet, see http://arstechnica.com/tech-policy/news/2012/02/iran-reportedly-blocking-encrypted-internet-traffic.ars (retrieved February 11, 2012).
11. See UN General Assembly Resolution 64/211: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, adopted March 17, 2010.
12. R. Deibert and R. Rohozinski, Contesting cyberspace and the coming crisis of authority, in R. Deibert et al., *Access Contested: Security, Identity and Resistance in Asian Cyberspace* (Cambridge, MA: MIT, 2011), 21–41.

13. The US position is more ambiguous with regard to blocking access or filtering links to sites that host pirated intellectual property, as seen in the recent debates over proposed anti-piracy legislation, viz., SOPA and PIPA. These would have required search engines to bar links to such sites, and Internet service providers to block access to such sites. Responding to a petition against these bills, the Obama Administration said it would not support legislation with provisions that could lead to Internet censorship, squelching of innovation, or reduced Internet security, but supported closing down such sites by judicial means.
14. See P. Yannakogeorgos, The new frontier and the same old multilateralism, in S. Reich, *Global Norms, American Sponsorship and the Emerging Patterns of World Politics* (Houndsmill, UK: Palgrave, 2011), 147–177.
15. J. Westby, A call for geo-cyber stability, in H. Touré et al., *The Quest for Cyber Peace*. International Telecommunications Union, 2011, 67. http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf; the Russian draft for a Convention on International Information Security, presented to the "International meeting of high-ranking officials responsible for security matters," Ekaterinburg, Russia, September 21–22, 2011, proposes, "in any international conflict, the right of the States Parties that are involved in the conflict to choose the means of 'information warfare' is limited by applicable norms of international humanitarian law."
16. These efforts include but are not limited to the Russia-US bilateral on critical infrastructure protection, Working toward rules for governing cyber conflict, EastWest Institute, February 2011.
17. For Chinese and Russian doctrines of information warfare see, respectively, T. Thomas, *Dragon Bytes: Chinese Information—War Theory and Practice* (Ft. Leavenworth, KS: Foreign Military Studies Office, 2004); T. Thomas, The Russian understanding of information operations and information warfare, in D. Alberts and D. Papp, eds., *Information Age Anthology: The Information Age Military* (Washington, DC: DoD, C4ISR Cooperative Research Program, 2001), 777-815; W. Hagestad II, *21st Century Chinese Cyberwarfare* (IT Governance, 2012).
18. Direct involvement of the Russian government or military command in organizing DDoS attacks on Georgia or the earlier ones on Estonia is a matter of debate, but undoubtedly the government knew of them beforehand and condoned them afterward. Another possible use of cyber weapons during a military action is Israel's alleged penetrations of Syrian military networks to neutralize the missile defense around the nuclear reactor that Israel bombed in 2007, see R. Clarke and R. Knake, *Cyberwar* (New York: Ecco, 2010).
19. See Information Warfare Monitor & Shadowserver Foundation, *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, April 6, 2010, http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0; Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network*, March 29, 2009, http://www.nartv.org/mirror/ghostnet.pdf; US-China Economic and Security Review Commission, *2010 Report to Congress* (Washington,

DC: US Government Printing Office, 2010), 236–247, http://origin.www.uscc.gov/sites/default/files/annual_reports/2010-Report-to-Congress.pdf, p. 236.

20. Z. Fryer-Biggs, U.S. Military Goes on Cyber Offensive, *Defense News*, March 24, 2012, http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive; J. Miller, DoD Using Cyber Teams Like Aircraft—For Offense and Defense, FederalNewsRadio.com, May 5, 2012, http://www.federalnewsradio.com/?nid=394&sid=2852854.
21. Letter dated September 12, 2011, from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary General, http://cs.brown.edu/courses/csci1800/sources/2012_UN_Russia_and_China_Code_o_Conduct.pdf
22. IBSA Multistakeholder meeting on global Internet governance, September 1–2, 2011, Recommendations. http://www.culturalivre.org.br/artigos/IBSA_recommendations_Internet_Governance.pdf; see also T. Ramachandran, Plan for new global body to oversee Internet governance evokes mixed response. *The Hindu*, October 23, 2011. http://www.thehindu.com/scitech/internet/article2565390.ece.
23. The Cyber Norms Workshop, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, October 19–21, 2011. For agenda, participants, framing questions, and preliminary report, see http://www.citizenlab.org/cybernorms/. The sponsors included The Belfer Center for Science and International Affairs at the Harvard Kennedy School of Government; The Canada Centre for Global Security Studies and Citizen Lab at the University of Toronto's Munk School of Global Affairs; Explorations in Cyber International Relations (ECIR), a joint Harvard-MIT research project; Microsoft Corporation's Office of Global Security Strategy and Diplomacy (GSSD); MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL); and The John D. and Catherine T. MacArthur Foundation. The opinions, findings, conclusions, or recommendations expressed here do not necessarily reflect those of any of these organizations. A second cyber norms workshop in September, 2012, was sponsored by Belfer Center, Canada Centre, Citizen Lab, MacArthur Foundation, and Microsoft. For information and panel summaries, see http://www.citizenlab.org/cybernorms2012/
24. Table 14.1 is based on C. Kavanagh, Wither "rules of the road" for cyberspace? CyberDialogue2012, March 18–19, 2012, Toronto, Canada. http://www.cyberdialogue.ca/briefs/.
25. R. Wall, NATO urged on missile and cyber-defense. *Aviation Week*. May 18, 2010. http://www.stopnato.net/?p=45463
26. M. Schmitt, Cyber operations and the jus ad bellum revisited. *Villanova Law Review*, 56 (2011), 569–605.
27. For example, D. Hollis, Could deploying Stuxnet be a war crime? *Opinio Juris,* January 25, 2011. http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/. "Conditions cry out for (a) states to devise

specific rules for launching or defending against cyber exploitations and cyber attacks; and (b) adopting an e-SOS as a first principle for mitigating or avoiding the most severe cyber threats. I don't think such rules would necessarily mean states could never deploy a Stuxnet (or that Iran would have an absolute right to issue an e-SOS if they did so). Rather, I think states themselves will have to devise the specific contours of acceptable (and unacceptable) behavior in cyberspace and then defend their own acts on such terms. Without those rules, I worry that the very technology that we have welcomed for its transformative effects on our everyday lives may generate new forms of death and destruction for which the Stuxnet episode is merely an opening act."

28. K. Rauscher and A. Korotkov, Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace. EastWest Institute, January 2011.
29. S. Schjølberg, Wanted: A United Nations cyberspace treaty. In A. Nagorski, ed., *Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway*. EastWest Institute, 2010, 11.
30. S. Kim et al., A comparative study of cyberattacks. *Communications of the ACM*, 55:3, March 2012, 66–73.
31. Chinese police chief vows international cooperation in fighting Internet crimes. *Xinhua*, August 30, 2011. http://news.xinhuanet.com/english2010/china/2011-08/30/c_131085036.htm. Unfortunately the FBI, which initiated the investigation, gave the Chinese police very little credit in its press release on the operation. By not appreciating the importance the Chinese attached to the cooperation, it missed an opportunity for building a relationship.
32. J. Mallery, private communication.
33. A. Wolfers, Discord and collaboration: essays on international relations. Baltimore, MD: 1962, cited in J. Nye, *The Future of Power*. New York: 2011, 16.