STRATEGIC STUDIES QUARTERLY

Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot

Mark Raymond

Abstract

The cyber-regime complex is governed by a sprawling array of rules, implemented in a decentralized manner by a large number of public and private actors. Since there is no guarantee that the future evolution of the cyber-regime complex will occur in a manner conducive to Internet stability and global interoperability, the "responsibility to troubleshoot" (R2T) is an important hedge against the significant costs associated with cyber disruption.

Even if a global prohibition regime were adopted, there would be good reasons to ensure the existence of a robust set of institutionalized mechanisms for mitigating and remediating various kinds of intended and unintended disruptions to Internet stability and interoperability. While prohibition may be worth pursuing, it is clearly insufficient. At least for the foreseeable future, previously agreed-upon mitigation and management processes will also be required.

✳ ✳ ✳ ✳ ✳

The cyber domain is widely acknowledged to be in the midst of a process of global rulemaking that includes an array of public and private actors from across the globe.[1] Many of these rules pertain, more or less directly, to issues of international security. Indeed, the question of cyber norms has been on the agenda of the First Committee of the United Nations General Assembly since 1998. Their work has made significant progress in the two most recent reports of its Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.[2] The work of the GGE is vitally important; however, this state-centric process cannot be treated in isolation from the broader landscape of

Mark Raymond is the Wick Cary Assistant Professor of International Security at the University of Oklahoma and a Fellow at the Center for Democracy and Technology. He holds a PhD in political science from the University of Toronto.

Internet governance and Internet policy—even though it concerns matters traditionally understood as the exclusive purview of states. Security and intelligence practitioners increasingly affect, and are affected by, decisions made about Internet governance and Internet policy in a variety of contexts at the global, regional, and even domestic levels. Many of these decision-making processes occur at least partially within the private rather than the public sphere.[3] Collectively, these processes of rulemaking entail the emergence of a broader cyber-regime complex alongside the narrow technical regime for Internet governance in an era characterized by the impending integration of the Internet and cyberspace with virtually every domain of human activity.[4] This process of regime complex formation is ongoing and remains contentious. Contention over Internet issues and the creation of this emerging cyber-regime complex is driven by a variety of factors, including the breadth of issues implicated (trade, security, human rights, etc.) and the diversity of participants in terms of actor type, interests, values, and views of legitimate procedures for rulemaking.[5]

Even the most optimistic projection for the nascent cyber-regime complex must acknowledge that, for the foreseeable future, most governance will remain decentralized. Decisions about policy, rules, and norms will be made by an extremely heterogeneous set of players that will often operate with a high degree of autonomy. Even where there are clear hierarchical authority relations between participants, the sheer complexity and pace of governance in this area will create autonomy in practice. Yet the shared global physical and logical resources crucial to the cyber domain mean that decisions made by these various parties may have implications for, and intended or unintended effects on, those outside their own jurisdictions. As a result, decisions made in one part of the cyber-regime complex can negatively impact the stability and interoperability of the network for others. The combination of the possibility of such effects and a highly decentralized regime complex exacerbates challenges of coordination and conflict resolution among an extremely diverse set of actors.

Since the various participants in the emerging global cyber-regime complex have distinct and at least partially incommensurate values and interests, policy coordination efforts are likely to remain limited. They will also be inhibited by the complexity of the subject matter. In such situations, one possible approach is to establish a shared commitment to "do no harm" or to refrain from taking steps that could negatively affect the stability or global interoperability of the cyber domain and the ability of the players to make use of it. Such an approach motivates recent calls for a norm of noninterference in what has been called the "public core" of the Internet.[6] Elimination of such cyber behavior is unlikely, in part because actors cannot agree completely (or even substantially) on the bounds of acceptable behavior. Accordingly, simple rules and norms of prohibition are unlikely to be sufficient for ensuring the viability of the cyber-regime complex. Further, a simple prohibition regime would likely be insufficient even in a world of angels. The reality of a massively complex, open global system built on the principle of "permissionless" innovation, combined with the law of unintended consequences, suggests the desirability of having previously agreed-upon means of responding when the activities of one group have negative implications (intended or not) for others.

This article argues that the capacity to effectively manage the set of challenges can be enhanced by cultivating a responsibility to troubleshoot (R2T).[7] First it argues that the decentralized nature of the global cyber-regime complex combines with the shared logical resources and physical infrastructure of the Internet to produce both strategic opportunities and externalities that affect other parties. One solution to these problems would be to establish a prohibition regime. Next it surveys other prohibition regimes employed to address international security threats. In doing so, it gives context to the common wisdom that prohibition is virtually impossible in the cyber domain and shows that elements of a proto-prohibition regime for the cyber domain are identifiable.[8] However, while prohibition may be worth pursuing, it is clearly insufficient. At least for the foreseeable future, mitigation and management processes will also be required. Accordingly, the third section explores options for an R2T as a core component of the global cyber-regime complex.

Decentralized Governance of a Global System

While cyberspace is often understood as a global commons or even a pure public good, it is more accurately described as a set of nested "club" goods, since it is excludable and typically non-rivalrous in consumption[9] and since decisions about cyberspace are taken in a myriad of separate institutional contexts arrayed in complex and variable authority relations.[10] At the most basic level, all Internet users are members of a single club: the club of global Internet users. Simultaneously, all users are also members of at least two other kinds of clubs—a club of Internet users in a particular state and a club of Internet users relying on a particular Internet service provider (ISP). Each of these clubs has different procedural rules for rulemaking and interpretation. National clubs of Internet users typically work according to the corresponding state's processes for legislation, regulation, and jurisprudence, though some states also have multi-stakeholder bodies governing some aspects of Internet policy. Clubs of users relying on a particular ISP are more commonly governed by contractual arrangements and terms of service, with civil law as a backdrop. Other notable clubs include those with special responsibility for core Internet technical functions, such as the Internet Corporation for Assigned Names and Numbers (ICANN) or the Internet Engineering Task Force (IETF).

As the Internet has become enmeshed with more and more aspects of economic, social, and political life, the narrow legacy Internet governance regime concerned with core technical functions such as the development of technical protocols and the management of Internet names and numbers has been drawn into a nascent global cyber-regime complex.[11] The result is that organizations with primary interests and responsibilities removed from the Internet and cyberspace are beginning to make decisions and to enact rules that can have significant unintended consequences for the stability and interoperability of the cyber domain. These actors include military and security agencies, antitrust regulators and consumer watchdogs, human-rights bodies, international-trade bodies, and others.

These various entities and organizations nevertheless share the same physical infrastructure as well as globally harmonized standards and protocols for exchanging packets between the various independent networks that comprise the Internet and for resolving Internet domain names into Internet protocol (IP) address numbers. The combination of the end-to-end principle and the principle of permissionless innovation has been central to the rapid global spread of Internet access and to its economic potential; however, these principles have also enabled the actions and decisions of individual organizations to have far-ranging effects on the stability and interoperability of the broader global network.

Such effects are often unintended consequences of attempts to exercise control over Internet content in the service of various social, economic, and political policy objectives. Examples include a global YouTube outage caused by Pakistani attempts to block domestic access to video content deemed inappropriate on religious grounds, domain name seizures by American law enforcement agencies intended to enforce intellectual-property laws, and ongoing European efforts to implement a "right to be forgotten" with respect to online search engines. These examples, and others, are indicative of what has been called "the turn to infrastructure in Internet governance."[12]

Cyber attacks, financially motivated cybercrime, and cyber espionage, whether conducted by states or firms, employ Internet infrastructure and mechanisms of technical Internet governance to accomplish unrelated objectives. Like content filtering and blocking measures, these activities can have negative unintended consequences for global Internet stability and interoperability. Some effects may be quite direct in nature. Manipulating the underlying technology and protocols may simply be done badly and cause technical problems. Given the low and rapidly falling barriers to entry in this field, significant cyber capabilities are likely to be acquired by a large number of public and private organizations with relatively low levels of expertise and sophistication; such novices may be particularly prone to execution errors. Other negative unintended effects on Internet stability and interoperability will be indirect in nature. The most likely pathways for ill effects include: (1) attempts to "harden" networks to make them less susceptible to intrusion but sacrifice openness as a result, leading the network topology to more closely resemble a "cybered Westphalia"[13]; and (2) escalating spirals of retaliation that cause episodic service interruptions and other collateral damage to third parties.

All of these diverse activities are enacted for reasons. Whether we evaluate these as good or bad reasons is beside the point of the argument being advanced here. The key point is that a large number of actors will be capable of forming their own views about the desirability of such forms of cyber conduct and also of *acting* on the basis of such views. It is this potential for autonomous action—which itself may have *further* unintended consequences—that makes these problems especially serious.

One approach to managing problems associated with unintended consequences in a decentralized governance environment would be to pursue prohibition of various forms of problematic cyber conduct. Grounds for such a ban might be rooted entirely in considerations of long-term consequences for Internet stability and interoperability, or they might also draw on complementary justifications having to do with respect for state sovereignty or individual human rights. Several bans on particular kinds of international conduct exist, and some have persisted for extended periods of time. What follows is a survey of several existing global prohibition regimes and the prospects for applying such an approach to cybersecurity governance.

Prohibition Regimes and International Security Governance

The common view of international politics—as a lawless Wild West in which sovereign states confront an anarchic system that compels them to act ruthlessly or perish—is mistaken. Political scientist Tanisha M. Fazal, whose research focuses on the relationship between sovereignty and international law, has convincingly shown that—at least since 1945—the rate of "state death" has fallen sharply in response largely to changing norms of conquest.[14] While international norms, like all social rules, may sometimes be violated, the norm against acquiring territory by conquest appears to exert a significant constraining effect on state behavior to the point where many states in the international system, including several permanent Security Council members, appear to have ruled it out entirely as a policy option. International condemnation of Russia's actions in Crimea demonstrates the continuing strength of the norm even as it requires acknowledgment that enforcement is imperfect.

Predation is hardly the only international conduct subject to prohibition. The extensive international relations literature documenting such regimes catalogs numerous cases of varying success.[15] Here the focus is on cases prohibiting conduct directly relevant to international security, to make three important points: (1) prohibition regimes are useful tools for achieving security policy objectives, (2) there are initial signs of a developing prohibition regime that captures multiple kinds of cyber conduct, and (3) even in a perfect world, such a prohibition regime is insufficient to address the problems associated with decentralized governance of a shared global facility.

One prominent global prohibition regime bans gross violations of fundamental human rights. An example is the ban on genocide codified in the Convention on the Prevention and Punishment of the Crime of Genocide (1948)—a prohibition that is also a *jus cogens* norm of international law under Article 53 of the Vienna Convention on the Law of Treaties.[16] Similarly, the prohibition against torture is also such a norm of international law in addition to a treaty obligation under the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (1984). In both cases, bans on particular forms of international conduct are framed in terms of these norms, which are binding on states regardless of their consent and which do not permit derogation. This latter quality of *jus cogens* norms substantially limits the varieties of special pleading open to states under the area of customary international law known as the law of state responsibility.[17]

Another class of internationally prohibited behaviors pertains to battlefield conduct. Wayne Sandholtz, a professor of international relations and law, has shown, for example, that wartime plunder has moved from a normal and expected part of war to prohibited behavior.[18] Similarly, political scientist Ward Thomas has argued that there is a relatively robust international norm against assassination.[19] There is also a ban on particular kinds of weapons. For example, biological and chemical weapons are subject to bans. The Biological Weapons Convention (1972) prohibits not only the use but also the production of this class of weapons,[20] though it lacks provisions for monitoring or inspection. In contrast, the Chemical Weapons Convention provides for extensive inspections in support of the associated taboo.[21] Bans have also been created for certain classes of conventional weapons. Examples include the ban on antipersonnel landmines[22] as well as the ban on cluster munitions.[23] In contrast, attempts to impose control on the international transfer of small arms and light weapons have been less successful.[24]

Prohibition in the Cyber Domain

There are also signs of a developing global prohibition regime in the cyber domain. This proto-regime has at least three notable components. The first deals with promoting international cooperation on cybercrime. The Budapest Convention on Cybercrime commits state parties to harmonizing their domestic legal regimes with respect to computer crime. It also commits parties to good-faith cooperation in investigating and prosecuting such crimes across borders.[25] As such, it effectively seeks to deal with the problem of decentralized governance by negotiating common standards at the global level and leaving implementation to domestic authorities. While a useful step, it has been ratified by only 47 nations, primarily advanced industrial democracies.

The second component of the emerging cyber prohibition regime consists of work primarily by the United Nations GGE seeking to clarify the applicability of the law of armed conflict in the cyber domain. The group includes the governments of the United States, China, and Russia; it therefore reflects the preferences and understandings of key states. The 2015 report made several key advances. It expressed the belief that "voluntary, non-binding norms of responsible State behavior can reduce risks to international peace, security and stability." It further made several concrete recommendations for such norms. Finally, in a discussion of the application of international law to information and communications technologies (ICT), the GGE explicitly noted "established legal principles . . . including, where applicable, the principles of humanity, necessity, proportionality and distinction."[26] American officials have indicated, though, that some states are thus far unwilling to make "more robust statements on how international law applies" in the cyber domain.[27] These efforts are preliminary, at best, and a great deal will depend on how these norms are implemented in concrete cases.

The final component of this proto-regime is the least developed. It involves the bilateral agreement between China and the United States regarding economic cyber espionage. In a September 2015 statement, the two governments indicated that "neither the U.S. nor the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage." The agreement also provided for the establishment of additional government-to-government contacts for the review of cybercrime allegations.[28] Published reports have indicated that American firms continue to suffer intrusions originating in China that are said to be attributable to government-linked hackers.[29] Accordingly, it is important to be realistic about the likelihood of Chinese compliance; however, it may be that the value of the agreement is in publicly committing China to a norm from which its derogation can be criticized. International relations professor Daniel C. Thomas, whose research focuses on issues of European integration and international governance, has argued that the Helsinki Accords had this effect in committing the Soviet Union to human-rights norms and thereby helping to bring about the end of Communist rule.[30]

Thus, prohibition regimes are an important component of a global-governance toolkit. There are good reasons to believe that some of the regimes discussed above have at least reduced the incidence and severity of particular kinds of undesirable conduct; however, these regimes vary in their comprehensiveness, formality, and effectiveness. In assessing the likely effectiveness of a cyber-prohibition regime, a number of foreseeable problems arise pertaining both to whether other actors can be convinced to adopt a prohibition regime and whether a prohibition regime can be effectively implemented even if other actors are convinced of its utility and appropriateness.

Prohibition regimes are typically employed to deal with conduct that is widely agreed to be immoral or unethical. Thus, the degree of moral revulsion generated is an important determinant of whether actors will agree to them. To the extent that some actors see different forms of cyber conduct as consistent with their identities or their substantive understandings of justice, they are unlikely to agree to prohibit such conduct. State conduct of economic cyber espionage provides an illustrative example. Some states and their populations may retain a more mercantilist understanding of what Australian constructivist scholar Christian Reus-Smit has called "the moral purpose of the state"[31] and thus believe aiding national firms counts (at least in the domestic arena) as praiseworthy state conduct. Such an argument is consistent with international security specialist Jacques Hymans's finding that leaders' perceptions of national identity are an important driver of state decisions regarding nuclear proliferation.[32]

Even if actors agree on what behaviors they want to prohibit, there may be other reasons a global prohibition regime lacks effectiveness. Political scientists Margaret Keck and Kathryn Sikkink have suggested that transnational advocacy networks are most successful in achieving their objectives when they are opposing conduct that entails physical harm to innocents and when that harm is the result of a short causal chain that easily connects the behavior with the resulting harm.[33] Given that many cyber harms accrue in the first instance to corporations rather than individuals (for example, intellectual property or brand damage), it may be difficult to generate sufficient moral revulsion to support a broad regime prohibiting many forms of problematic cyber conduct. Further, many cyber harms typically involve highly complex and opaque causal chains that individual policy makers and voters are unlikely to understand in any depth.

Convincing others to support a prohibition regime dealing with particular forms of cyber conduct will also be more difficult to the extent that prohibiting such conduct will also undermine actors' attempts to achieve other valued goals. There are a variety of problems associated with dual-use technology. State security agencies, for example, may see particular forms of malicious code as critical to fulfilling their war-fighting and intelligence-gathering missions—even if they might agree that some uses of such technologies should be restricted.

Research also indicates that the presence of powerful champions on either side of an issue can affect the success or failure of advocacy efforts.[34] Such champions matter not only in terms of persuading other actors but also in determining which issues advocates decide to contest; further, champions may be organizations occupying positions of network centrality, in addition to individual norm entrepreneurs.[35] While the United States has attempted to champion a norm against economic cyber espionage, its efforts have been undermined by revelations about the activities of the American intelligence community. Most technology sector and civil-society organizations have focused on contesting privacy and other human-rights issues, whether or not in response to state surveillance online. Reluctance to publicly disclose data breaches to protect reputation and share value may well limit the willingness of other firms to champion prohibitions on many forms of problematic cyber conduct.

Implementing Cyber Prohibition

Aside from challenges in securing political agreement on an expanded, robust cyber prohibition regime, there are two important aspects to address in implementing any such measures: the use of formal versus informal instruments and complications arising from monitoring and enforcement.

Most global-prohibition regimes rely heavily on formal legal instruments that codify the proscribed behavior and obligations of various parties for monitoring, enforcing, and otherwise implementing the ban. However, considerable risks are associated with the use of hard-law instruments in this context; soft-law modalities may be more effective.[36] First, treaties and customary international law bind only states. Given the low barriers to entry and the key role of the private sector in the cyber domain, a hard-law global-prohibition regime would not directly bind many of the relevant actors. Further, insofar as a hard-law instrument binds states to implement and enforce prohibitions within their own borders and to cooperate with other states in doing so, it could be expected to lead to a substantial number of requests under existing mutual legal-assistance treaties. Where mutual legal assistance is not effective, there may also be attempts to employ the law of state responsibility to pursue remedies. Such measures would place states in the difficult position of being responsible for the management of problem-solving on a global network that is expected to expand to several billion connected devices and on which it is often difficult to attribute particular conduct to specific actors. Even for advanced industrial democracies, it is questionable whether such arrangements are feasible; for emerging markets and developing states, the situation would be even more difficult.

A second reason to be skeptical of hard-law instruments for prohibiting problematic cyber conduct is that there are legitimacy risks associated with the codification of rules that are either unlikely to be obeyed or extremely difficult to enforce. Such rules risk becoming dead letters and serving as constant temptations for violators to argue that actors do not believe the proscribed conduct is actually inappropriate.

Finally, monitoring and enforcement present serious challenges for a global-prohibition regime in the cyber domain, whether it is implemented via hard- or soft-law mechanisms. The issue presents clear enforcement problems among a large number of actors on an issue where attribution is generally difficult. Therefore, violations are both likely and difficult to prevent or punish. Access to the technology required to conduct such activities is already widespread and available from a large number of suppliers based in different countries. These technologies also typically have multiple purposes, further complicating efforts to curtail proliferation.

Despite these considerable challenges, soft-law prohibition norms are generally inexpensive to promote and can have substantial constraining effects on behavior when internalized. Accordingly, current prohibition efforts should be pursued with the realization that they will not provide sufficient tools to deal with problems arising from decentralized governance of a shared global facility. In particular, prohibition should be coupled with robust, institutionalized means of responding to intended and unintended disruptions to Internet stability and interoperability.

The Responsibility to Troubleshoot

The insufficiency of global-prohibition norms to deal with problematic cyber conduct means that there will be an ongoing need for mechanisms to mitigate and manage such conduct when it does occur. While these mechanisms will naturally involve technology (improving hardware, software, and related technical standards), policy must also include attempts to address the social dimensions of such conduct or run the risk that bad actors will adapt and innovate, finding new ways to realize their goals. Measures should be aimed at reducing the frequency and severity of disruptive cyber conduct, fostering cooperation in repairing damage caused by misconduct, and preventing the escalation of such incidents into even more serious disputes or conflicts. Cultivating a responsibility to troubleshoot can enhance global capacity to manage challenges associated with decentralized cyber governance.

Coping with Unintended Consequences

The core challenge is to cope with negative effects on the stability or global interoperability of cyberspace. Since these kinds of effects are not typically intended outcomes, the remainder of this article emphasizes means for coping with unintended consequences rather than with intended effects. However, since determining intention is often difficult in practice, there is a strong argument for presuming any such negative effects to be unintended. If nothing else, publicly treating such events under a presumption that they are unintended serves two valuable purposes. First, it reduces the likelihood of hostility and escalation. Second, refusal to cooperate in resolving problems may provide prima facie evidence to third parties that the effect was intended (or at least welcomed) and demonstrate bad faith on the part of the responsible actor, thereby increasing reputational costs from engaging in such conduct.

Resolving these problems requires effective and reliable methods of quickly identifying and remedying the effects of malicious code and other means of disrupting cyberspace. These tasks are complicated not only by technical problems of diagnosis, attribution, and implementation but also increasingly by problems of jurisdiction in what Naval War College professors of strategy Chris C. Demchak and Peter Dombrowski have termed a cybered Westphalian age.[37] The decentralized nature of the international system and the cyber-regime complex create or exacerbate a host of problems in securing broad, reliable cooperation in responding to disruptions in the cyber domain. Aside from complications arising from domestic politics and international rivalries, these difficulties include differences in culture, institutions, specific domestic legal regimes, and basic capacity (infrastructure, skilled personnel, and financing).

Furthermore, it is not immediately obvious who should be responsible for *providing* such cooperation. Most Internet infrastructure is privately owned, and most jurisdictions have multiple large-network operators. Are such firms responsible, and if so, are they individually or collectively responsible? Further, a variety of actor types transmits information over these networks. In some cases, this information itself may be responsible for the disruption. What responsibility do Over-The-Top content providers, non-technology firms acting as Internet consumers, state actors, civil-society groups, and private individuals bear? Computer emergency response teams (CERTs) typically assume responsibility for this level of cooperation and assistance as part of their mission statements,[38] but CERTs are highly varied in their capacity and in their scope of work.[39]

These difficulties will not be quickly or easily overcome. One useful step in doing so, however, would be to supplement prohibition efforts with the cultivation of a norm that all relevant actors must participate in good faith in efforts to resolve threats to the stability and interoperability of cyberspace. This requirement can be understood as an R2T. The underlying rationale for this suggestion is that norms shape behavior in a number of ways, for example by reducing the propensity of actors to engage in conduct that violates applicable norms and by shaping responses to violations by prompting criticism or sanctions.[40] Note, especially, that because they enable criticism and sanctioning behavior, norms can have significant and helpful effects even in cases where compliance falls substantially short.

The notion that even sovereign states have international responsibilities should not be controversial. The most basic of these—noninterference in the domestic affairs of other states—is foundational to the modern international system. Several other responsibilities are inherent to modern international law. These include the principle that treaties must be observed (*pacta sunt servanda*) and other *jus cogens* principles. The bodies of customary and conventional international law are also similarly binding on sovereign states. Among the latter, the UN Charter deserves special mention in creating responsibilities pertaining to the use of force and to compliance with measures authorized by the UN

Security Council. The 2015 GGE report affirmed the applicability of the charter, in its entirety, in the cyber domain.[41]

As with any other field of social life, actors will sometimes fail to live up to their responsibilities. International law explicitly contemplates such situations. It does so in the first instance by making states responsible for their internationally wrongful acts, requiring them to provide apologies, damages, and other forms of restitution. Absent their willingness to do so, international law also authorizes wronged states to take certain self-help measures. Most importantly, even in exercising self-help, states have responsibilities to do so according to the terms of identifiable rules. As with rules of the road in many other areas of international politics, the law of state responsibility has taken important steps toward codification (and thus greater precision) in the latter half of the twentieth century. [42] This effort has, thus far, culminated in the publication of the International Law Commission's *Draft Articles on Responsibility of States for Internationally Wrongful Acts*.[43] While not yet formally adopted by states in the form of a treaty, the articles have been endorsed on multiple occasions by the UN General Assembly.

If anything, contemporary understandings of sovereignty are increasingly qualified by concomitant responsibilities. The "responsibility to protect" (R2P) is an important recent example.[44] Further, notions of international responsibility are increasingly extended to non-state actors. The International Criminal Court recognizes individuals as bearing responsibility for certain kinds of grievous offenses even when undertaken in an official state capacity. Efforts to inculcate an ethos of corporate social responsibility, such as the UN Global Compact, also seek to create and uphold responsibilities for firms. It should not be controversial to extend notions of international responsibility, including an R2T, to various kinds of non-state actors.

Relationship to Responsibility to Protect

The R2P is arguably the most significant addition to the body of international responsibilities since 1945. Rather than a single responsibility, it entails three related responsibilities arranged to ensure the greatest possible redundancy while reducing costs in terms of both sovereignty and enforcement. The primary obligation is that of the state to its own citizens, specifically, to protect them from genocide, war crimes, and crimes against humanity. This obligation includes not committing or inciting those acts against the state's own population, as well as protecting the population against the perpetration of such acts by third parties. The international community also has, in the first instance, the obligation to "encourage and assist" states in carrying out this obligation to their own citizens. In cases where states are unwilling or unable to fulfill the primary responsibility, R2P holds that the international community has a collective responsibility to provide such protection. It specifies that this is preferably done by peaceful means but that stronger measures are authorized if such means are impractical or unsuccessful.[45]

While the legal status of R2P is admittedly uncertain and the analogy between the R2P and any potential R2T is imperfect at best, surveying these shortcomings is instructive for effectively advocating and implementing an R2T. First, given the privatization of key Internet infrastructure, the limited capacity and expertise of many states with cyber operations, the low barriers to entry for the creation of significant cyber disruptions, and the difficulty of decisively attributing specific conduct to particular actors, allocation of an R2T exclusively to states would be unlikely to prove effective. In keeping with the avowedly multi-stakeholder nature of Internet governance, any R2T would need to be borne not only by states but also by firms and voluntarily by organizations with the means to contribute to ensuring its efficacy.

Second, the nature of the foundational responsibility in the two situations differs. The R2P is foremost an obligation of the state to its own citizens. In contrast, an R2T would be offered equally by states to citizens and noncitizens since it pertains in substance to the functioning of a global communications facility. Further, if the R2T is borne in part by non-state actors, it cannot be owed on the basis of the relationship between state and citizen. The conception of the Internet as a governance system comprised of a set of nested clubs, as mentioned earlier, provides two distinct and non-mutually exclusive bases for grounding an R2T. On one hand, the obligation can be grounded in reciprocity: the responsibility of all clubs of Internet users to refrain from disruptive cyber conduct in return for the assurance that all other clubs will provide them the same consideration. This ground creates an obligation owed by groups to other groups. On the other hand, the obligation can also be grounded in the terms of membership for the most basic and universal club: the club of all global Internet users. This ground creates an obligation owed by members of a group to each other. Both routes are possible, and both can be pursued without contradiction since the substantive obligation is the same in both cases. Given the lack of a strong cosmopolitan ethos and the strength of more particularistic attachments in social life, the first basis may well prove more compelling overall, but the cosmopolitan basis resonates more clearly with the human-rights regime.

Third, the nature of the subsidiary collective responsibility also differs. The difficulty of attributing cyber conduct poses severe challenges for any efforts to implement collective action to intervene in the case of major cyber disruptions or extremely significant levels of other problematic cyber conduct such as large-scale economic cyber espionage. Taking steps that might include property damage or loss of life, at least with the collective authorization envisaged by the R2P, will likely demand the ability to demonstrate culpability in a public and convincing manner. At a more pragmatic level, inaccurately directed responses are unlikely to eliminate the undesired conduct and are further likely to prompt retaliation and loss of legitimacy. It is also doubtful whether there are any forms of cyber conduct sufficiently grave to satisfy the proportionality standards implicit in the R2P, which applies only in situations of genocide, war crimes, and crimes against humanity. Prior to reaching this level, such cases would almost certainly trigger other rules permitting a collective response, like the UN Charter provisions for self-defense and for the maintenance of international peace and security. The R2T is a means for addressing conduct of serious international concern that falls short of the extreme acts that trigger the R2P. Therefore, there is no need for the R2T to require (or authorize) more than the use of peaceful, cooperative means. The concept of a responsibility to troubleshoot cannot be a panacea to answer all problems arising from the cyber domain. To the extent that this responsibility is adopted, however, some problems can be made less severe and perhaps reduced in frequency. It is therefore a potentially important component of the broader cyber-regime complex currently in the process of formation. The R2T proposed here is consistent with the recommendations of the 2015 Group of Governmental Experts. The GGE endorsed assistance for less-developed countries but also indicated that "capacity-building involves more than a transfer of knowledge and skills from developed to developing States, as all States can learn from each other about the threats that they face and effective responses to those threats." This speaks to a broad awareness that international cyber assistance is not simply a matter of development. Further, the group proposed several candidate norms that indicate general support for the notion that providing assistance is appropriate international behavior.[46] These candidate norms are discussed in more detail below. In general, the GGE recommendations are primarily focused on state actors and do not develop the notion that an R2T might also apply to non-state actors. Further, given the preliminary state of international legal development in this area, the GGE merely expresses support for candidate norms. This is a sensible starting point but falls well short of a notion of responsibility.

Implementing the Responsibility to Troubleshoot

Several current and future options exist for implementing the R2T. As in many other areas of Internet and cyber governance, states have useful roles. One such role pertains to information sharing. In general terms, this may involve sharing information on an ongoing basis to facilitate diffusion of best practices in cybersecurity. The GGE suggested, for example, that states should "encourage responsible reporting of ICT [information and communications technologies] vulnerabilities and share associated information on available remedies."[47] Information sharing may also involve more specific efforts in response to particular instances of problematic cyber conduct. This cooperation will often involve law enforcement agencies. In this vein, the GGE called for states to "consider how best to cooperate to exchange information, assist each other, prosecute terrorist or criminal use of ICTs, and implement other cooperative measures to address such threats."[48]

State involvement in implementing an R2T will need to go beyond information sharing to encompass a direct role in incident response. States are already significant network operators; their activities in this regard may have unintended effects on other parties. Further, as states play larger regulatory roles in the cyber domain, the number of channels through which state action can produce negative effects on Internet stability and interoperability is likely to grow. Finally, many states have created bodies to assist firms and individuals in dealing with cyber disruptions. These bodies may themselves produce unintended consequences for users outside the state's jurisdiction. In each of these cases, the state is itself the source of a kind of problematic cyber conduct. It is not unreasonable to suggest, therefore, that it bears a degree of responsibility to those affected by its actions. Even where the state is not the direct cause of cyber conduct that damages others, it may bear some responsibility under international law to states whose citizens are adversely affected.

The GGE took preliminary steps toward recognizing such responsibilities in proposing that states should "respond to appropriate requests for assistance by other States whose critical infrastructure is subject to malicious acts" and that they should "respond to appropriate requests to mitigate malicious activity aimed at the critical infrastructure of another State emanating from their territory."[49] While promising, these candidate norms are limited only to acts that target the critical infrastructure of other states, leaving most firms and citizens of other states relatively unprotected. In limiting the candidate norms to covering "malicious acts" the GGE also left unintended consequences (the primary problem discussed in this article) unaddressed. Further, there are numerous ambiguities in the phrasing. It is not clear, for example, what constitutes an "appropriate request" or even what is included under "critical infrastructure." Even if these candidate norms are ultimately accepted by most states, additional work remains to be done.

The work of mitigating and resolving problematic cyber conduct once it has begun is in large part dependent on technical competencies in engineering and computer science. But such work cannot occur effectively and reliably at the global level without proper governance and administrative structures to enable it. Over the last several years, Internet governance issues have become increasingly contested. Individual governments, including those of the United States, China, Russia, Brazil, and others, have initiated or increased efforts to exert influence over these issues. Incumbent entities including the Internet Corporation for Assigned Names and Numbers, the Internet Engineering Task Force, and the Internet Society (ISOC) have also undertaken efforts to defend or expand their roles, and other players like the International Telecommunication Union (ITU), Organization for Economic Cooperation and Development (OECD), and World Economic Forum (WEF) have also sought enhanced roles. Of particular importance in implementing the R2T, however, are organizations dedicated to emergency response. CERTs, sometimes called computer security incident response teams (CSIRT), can—and often do—play important roles in efforts to respond to cyber disruptions.

Since 1990, the Forum of Incident Response and Security Teams (FIRST) has provided a degree of coordination among these groups.

Its membership is relatively global but includes little representation in Africa and the Middle East.[50] Further, members are disproportionately clustered in the developed world, and developing world members generally lack resources and expertise. FIRST has also undertaken efforts to coordinate with the International Organization for Standardization (ISO) and ITU to ensure lessons learned from computer security incidents are incorporated into efforts to revise and create technical standards. It is also currently in the process of developing a curriculum to ensure CSIRT training is consistent and of high quality. Individual members also organize and join special interest groups on a voluntary basis according to their interests.

The GGE explicitly recognized the importance of CSIRTs in its 2015 report. It called on states to "not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams . . . of another State" and further indicated that states should "not use authorized emergency response teams to engage in malicious international activity."[51] These candidate norms suggest that there may be support for providing CSIRTs with a degree of protected status under international law.

Existing CSIRT programs and initiatives provide a solid foundation for implementing many parts of an R2T, especially if their trustworthiness and freedom to operate can be protected under international law, but in several important areas further development would be beneficial. First, expanding educational offerings will provide an important service to the global community. Second, additional work is needed in creating organizations in areas of the world where CSIRTs are less common. While FIRST cannot accomplish this alone, it can play an important advocacy and mobilization role alongside assistance from other Internet community organizations and other stakeholders, including governments acting in their capacity as providers of and catalysts for development aid and capacity building. Third, the CSIRT community needs to engage in broader outreach to educate a wider array of organizations about its role and importance. Network operators, technology firms, universities, and some large financial institutions either have their own CSIRTs or are accustomed to working with them, but as the "Internet of Things" dramatically broadens the number of Internet-connected devices and objects, these concerns will become broadly relevant to firms both as producers and consumers. Ensuring that stakeholders are apprised of appropriate points of contact and available resources will facilitate timely, cooperative mitigation and remediation. These functions all parallel the requirement in R2P that actors assist each other in carrying out their primary responsibility. They are also consistent with other norms in the international system emphasizing the importance of providing capacity-building and technology transfer assistance to developing states.[52] Capacity in this sense includes not only technology itself but also knowledge about governance issues pertaining to information and communications technologies.

The suggestions above deal with education, outreach, and capacity building. In addition, it would be helpful to increase and institutionalize CSIRT cooperation and coordination at a more operational level. One modest first step in this regard would be the establishment of a global clearinghouse system for notification of cyber disruptions and other problematic cyber conduct. Beyond notification, such a system could also perform a "handshaking" function, connecting parties experiencing issues with verified, trustworthy groups with the expertise and willingness to assist. Such a system could also help reduce duplication of effort. Finally, FIRST might play a role in developing and disseminating best practices. States and other stakeholders could play critical supporting roles in these endeavors, including by encouraging or requiring actors to make use of these mechanisms in responding to cyber disruptions rather than (or at least in addition to) employing private means of response.

Many forms of problematic cyber conduct revolve around access to sensitive information. Further, efforts to mitigate such conduct may bring CSIRT members and law enforcement officials into contact with the sensitive information of third parties, including those in other legal jurisdictions—for example, of individuals whose devices are part of illicit botnets. Accordingly, it is vital that efforts to implement an R2T are especially sensitive to compliance with human-rights protections and civil liberties, to prevent the inadvertent agglomeration of excessive powers by law enforcement and security agencies. The GGE recognized the importance of human rights, calling on states specifically to "respect Human Rights Council resolutions 20/8 and 26/13 . . . as well as General Assembly Resolutions 68/167 and 69/106."[53] Each of these resolutions pertains to digital rights. This requirement of an R2T is parallel to the Brazilian notion of a "responsibility while protecting" governing conduct of the international community in upholding the

R2P.[54] Whereas in implementing R2P the primary danger is to individuals' physical security, in R2T the primary danger is to their privacy and digital rights. Accordingly, a responsibility while troubleshooting (RWT) will reflect this difference.

Efforts to implement an R2T must also consider financing mechanisms. Insufficient funding for work on Secure Sockets Layer (SSL) was revealed to have played a role in the failure to identify and rectify the "Heartbleed" flaw.[55] Only after the flaw was publicly revealed did major technology firms agree to provide funding for the development of what had become a backbone of Internet commerce.[56] Financing mechanisms to implement the R2T will need to take advantage of a variety of modalities, including private-sector funding as well as public-private arrangements. However, there are reasons to be wary of unorthodox funding streams and to preserve the notion of public-sector financing (including at the global level) for some key functions.

While voluntary Internet-community efforts to fund and develop technology standards have been largely successful, these efforts may be prone to market failures of the kind that afflicted SSL. Further, it is not immediately obvious that SSL should need to rely on the private sector for funding, given that governments are among its most important users. Government reliance on SSL appears to be increasing. On 8 June 2015, a White House memo announced the requirement that "all publicly accessible Federal websites and web services only provide service through a secure connection" and noted explicitly that "the strongest privacy and integrity protection currently available for public web connections is Hypertext Transfer Protocol Secure (HTTPS)," which may use SSL.[57] Setting aside questions about the wisdom of designating a specific single encryption standard for government web services, this public reliance on a particular technology raises the question whether the public should play a role in funding the development and maintenance of that technology.

Regardless of questions about the proper roles for the public and private sectors in financing efforts to deal with problematic cyber conduct, there is a need to ensure that funders do not acquire undue influence over the implementation of R2T. Steps should be taken to implement arms-length arrangements that guard against the corruption or capture of such efforts in the service either of profit or of national interest.

Fully developing and implementing an R2T, including a set of best practices for RWT, would require considerable consultation and care among a diverse set of global stakeholders. The most recent GGE report provides grounds to conclude that major governments may be receptive to some steps in this direction. As international law expert Duncan Hollis has argued, other parts of this agenda may also emerge from regional, bilateral, or even unilateral steps.[58] It would likely also be possible for the technology industry and technical Internet governance bodies to make meaningful progress without including states; however, such scenarios must take into account the possibility that some states could block efforts in their own territory on national security or other grounds and that purely private efforts would likely underprovide services in the developing world.

Conclusion

That states have international responsibilities is beyond doubt, though the nature of those responsibilities continues to evolve. While the notion that non-state actors have international responsibilities is more novel, it is nonetheless increasingly well established in international criminal law, international humanitarian law, corporate social responsibility, and in other issue areas. Nevertheless, there are multiple reasons to doubt the likelihood that efforts to ban problematic cyber conduct will succeed in the foreseeable future. At most, it may be plausible to generate support for a commitment to "do no harm" to the stability and interoperability of the Internet for others, even if some states are determined to exercise increasing surveillance powers and control over access to content within their own borders. Even if a global prohibition regime were adopted, there would be good reasons to ensure the existence of a robust set of institutionalized mechanisms for mitigating and remediating various kinds of intended and unintended disruptions to Internet stability and interoperability.

This article has explored possible modalities for, and challenges in implementing, a responsibility to troubleshoot. An R2T would need to apply to states, international organizations, and technology firms as well as to large commercial Internet users and relevant civil-society groups. The Forum of Incident Response and Security Teams is well positioned for an expanded role; however, realizing this potential will require a great deal of assistance from other actors. Especially in its initial phases, the R2T should be embodied in hortatory soft-law instruments that permit greater flexibility and experimentation, that carry lower negotiating costs than formal hard-law instruments of international law, and that more easily enable the participation of non-state actors.[59] The R2T should additionally be accompanied by a responsibility *while* troubleshooting that commits engaged parties to implementing best practices for the protection of sensitive data encountered in the process of mitigating and remediating threats to Internet stability and interoperability.

The creation of an R2T and an accompanying RWT will ultimately require a sustained advocacy campaign by a transnational network including government officials, international organization staff, corporate officers, and especially civil-society technologists and activists. Securing agreement on the desirability of social rules and successfully implementing them will no doubt be difficult. However, the alternative is not a scenario in which the cyber domain is entirely ungoverned by rules and in which actors have no responsibilities whatsoever. Cyberspace is already governed by a sprawling array of rules, implemented in a decentralized (and sometimes only partially overlapping) manner by a large number of public and private actors. Further, it is extremely likely that this emerging cyber-regime complex will continue to develop. New rules will be made to govern the cyber domain, some existing rules will fall into disuse, and others will be reinterpreted, changed, and applied in novel ways. The only question is the eventual trajectory of this rule system. Accordingly, it is not immediately clear that the development of an R2T is significantly less likely than other less desirable outcomes. Moreover, the likelihood of particular outcomes can be shaped by the exercise of agency. Since there is no guarantee that the future evolution of the cyber-regime complex will occur in a manner conducive to Internet stability and global interoperability, the R2T is an important hedge against the significant costs associated with cyber disruption in a context of highly decentralized governance. SSQ

Notes

1. Laura DeNardis, *The Global War for Internet Governance* (New Haven, CT: Yale University Press, 2014); Mark Raymond and Laura DeNardis, "Multistakeholderism: Anatomy of an Inchoate Global Institution," *International Theory* 7, no. 3 (2015): 572–616, doi:10.1017/S1752971915000081; and Madeline Carr, "Power Plays in Global Internet Governance," *Millennium: Journal of International Studies* 43, no. 2 (2015): 640–59, doi:10.1177/0305829814562655.

See also Tim Maurer, "Cyber Norm Emergence at the United Nations—An Analysis of the Activities at the UN Regarding Cyber-security," Discussion Paper 2011-11 (Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011), http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

2. United Nations (UN), Office for Disarmament Affairs, "Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security," UN General Assembly (UNGA) A/68/98 (2013), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement; and UNGA A/70/174 (2015), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement. For scholarly assessments of the earlier iterations of the GGE, see Maurer, "Cyber Norm Emergence," and Eneken Tikk-Ringas, "Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee, 1998–2012" (Geneva: ICT4Peace Publishing, 2012).

3. Mark Raymond, "Engaging Security and Intelligence Practitioners in the Emerging Cyber Regime Complex," *Cyber Defense Review* 1, no. 2 (forthcoming).

4. Joseph S. Nye Jr., "The Regime Complex for Managing Global Cyber Activities," *Global Commission on Internet Governance Paper Series*, no. 1 (Waterloo, ON: Centre for International Governance Innovation, 2014), https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

5. Mark Raymond and Gordon Smith, eds., *Organized Chaos: Reimagining the Internet* (Waterloo, ON: Centre for International Governance Innovation, 2014); and Samantha Bradshaw, Laura DeNardis, Fen Osler Hampson, Eric Jardine, and Mark Raymond, "The Emergence of Contention in Global Internet Governance," *Global Commission on Internet Governance Paper Series*, no. 17 (Waterloo, ON: Centre for International Governance Innovation, 2015), https://www.cigionline.org/publications/emergence-of-contention-global-internet-governance.

6. Dennis Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance* (Amsterdam: Amsterdam University Press, 2015), http://www.wrr.nl/fileadmin/en/publicaties/PDF-Rapporten/The_public_core_of_the_internet_Web.pdf.

7. Duncan Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal* 52, no. 2 (2011): 374–432, http://www.harvardilj.org/2011/07/issue_52-2_hollis/. The concept of R2T is similar to what Hollis has called an "e-SOS" facility.

8. For such a view, see Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (2013): 30–36, doi:10.1162/ISEC_a_00138.

9. Mark Raymond, "Puncturing the Myth of the Internet as a Commons," *Georgetown Journal of International Affairs*, International Engagement on Cyber III (2013), 53–64, http://journal.georgetown.edu/wp-content/uploads/2015/07/gjia13005_Raymond-CYBER-III.pdf.

10. Raymond and DeNardis, "Multistakeholderism."

11. Nye, "Regime Complex."

12. Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, eds., *The Turn to Infrastructure in Internet Governance* (New York: Palgrave, 2015).

13. Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no.1 (Spring 2011): 32–61, http://www.au.af.mil/au/ssq/2011/spring/demchak-dombrowski.pdf.

14. Tanisha M. Fazal, *State Death: The Politics and Geography of Conquest, Occupation, and Annexation* (Princeton, NJ: Princeton University Press, 2007).

15. Ethan A. Nadelmann, "Global Prohibition Regimes: The Evolution of Norms in International Society," *International Organization* 44, no. 4 (1990): 479–526, doi:10.1017/S0020818300035384. Global prohibition regimes date to the earliest stages of the constructivist turn in IR theory.

16. Jan Wouters and Sten Verhoeven, "The Prohibition of Genocide as a Norm of Jus Cogens and its Implications for the Enforcement of the Law of Genocide," *International Criminal Law Review* 5 (2005): 401–4, doi:10.1163/1571812054940049. *Jus cogens* are fundamental principles of international law that are accepted by the international community of states as norms, from which no derogation is permitted.

17. UN, "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries," 2008, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

18. Wayne Sandholtz, *Prohibiting Plunder: How Norms Change* (New York: Oxford University Press, 2007).

19. Ward Thomas, "Norms and Security: The Case of International Assassination," *International Security* 25, no. 1 (2000): 105–33, doi:10.1162/016228800560408.

20. UN Office for Disarmament Affairs, The Biological Weapons Convention, 10 April 1972, http://disarmament.un.org/treaties/t/bwc/text.

21. Richard Price, "A Genealogy of the Chemical Weapons Taboo," *International Organization* 49, no. 1 (1995): 73–103, http://dx.doi.org/10.1017/S0020818300001582.

22. Richard Price, "Reversing the Gun Sights: Transnational Civil Society Targets Land Mines," *International Organization* 52, no. 3 (1998): 613–44, http://dx.doi.org/10.1162/002081898550671; and Adam Bower, "Norms without the Great Powers: International Law, Nested Social Structures, and the Ban on Antipersonnel Mines," *International Studies Review* 17, no. 3 (2015): 347–73, http://dx.doi.org/10.1111/misr.12225.

23. Matthew Bolton and Thomas Nash, "The Role of Middle Power-NGO Coalitions in Global Policy: The Case of the Cluster Munitions Ban," *Global Policy* 1, no. 2 (2010): 172–84, doi:10.1111/j.1758-5899.2009.00015.x; and Bonnie Docherty, "Breaking New Ground: The Convention on Cluster Munitions and the Evolution of International Humanitarian Law," *Human Rights Quarterly* 31, no.4 (2009): 934–63, http://muse.jhu.edu/article/363660.

24. R. Charli Carpenter, "Vetting the Advocacy Agenda: Network Centrality and the Paradox of Weapons Norms," *International Organization* 65, no. 1 (2011): 69–102, http://dx.doi.org/10.1017/S0020818310000329.

25. Council of Europe, Budapest Convention on Cybercrime (2004), accessed 17 January 2016, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

26. UNGA A/70/174 (2015), accessed 17 January 2016, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement. See especially 7–8 and 13.

27. Michele Markoff, "Advancing Norms of Responsible State Behavior in Cyberspace," DipNote: US Department of State Official Blog, 9 July 2015, https://blogs.state.gov/stories/2015/07/09/advancing-norms-responsible-state-behavior-cyberspace.

28. Ellen Nakashima and Steven Mufson, "U.S., China Vow Not to Engage in Economic Cyberespionage," *Washington Post*, 25 September 2015, https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html.

29. Ellen Nakashima, "China Still Trying to Hack U.S. Firms Despite Xi's Vow to Refrain, Analysts Say," *Washington Post*, 19 October 2015, https://www.washingtonpost.com/world

/national-security/china-still-trying-to-hack-us-firms-despite-xis-vow-to-refrain-analysts-say/2015/10/18/d9a923fe-75a8-11e5-b9c1-f03c48c96ac2_story.html.

30. Daniel C. Thomas, *The Helsinki Effect: International Norms, Human Rights, and the Demise of Communism* (Princeton, NJ: Princeton University Press, 2001).

31. Christian Reus-Smit, *The Moral Purpose of the State: Culture, Social Identity, and Institutional Rationality in International Relations* (Princeton, NJ: Princeton University Press, 1999).

32. Jacques E.C. Hymans, *The Psychology of Nuclear Proliferation: Identity, Emotions and Foreign Policy* (Cambridge, UK: Cambridge University Press, 2006).

33. Margaret E. Keck and Kathryn Sikkink, *Activists Beyond Borders: Advocacy Networks in International Politics* (Ithaca, NY: Cornell University Press, 1998), 27.

34. Joshua W. Busby, *Moral Movements and Foreign Policy* (Cambridge, UK: Cambridge University Press, 2010).

35. Carpenter, "Vetting the Advocacy Agenda."

36. On the distinction between hard and soft law, see Kenneth W. Abbott and Duncan Snidal, "Hard and Soft Law in International Governance," *International Organization* 54, no. 3 (2000): 421–56, http://dx.doi.org/10.1162/002081800551280.

37. Demchak and Dombrowski, "Rise of a Cybered Westphalian Age."

38. For example, see "FIRST Vision and Mission Statement," Forum of Incident Response and Security Teams (FIRST), accessed 8 September 2016, https://www.first.org/about/mission.

39. Mark Raymond, Aaron Shull, and Samantha Bradshaw, "Rule-Making for State Conduct in the Attribution of Cyber-Attacks," in Kang Choi, James Manicom, and Simon Palamar, eds., *Mutual Security in the Asia-Pacific: Roles for Australia, Canada and South Korea* (Waterloo, ON: Centre for International Governance Innovation, 2015).

40. These expectations are consistent with the constructivist literature in international relations. See, among many others: Emanuel Adler, "Seizing the Middle Ground: Constructivism in World Politics," *European Journal of International Relations* 3, no. 3 (1997): 319–63, doi: 10.1177/1354066197003003003; Martha Finnemore and Kathryn Sikkink, "Taking Stock: The Constructivist Research Program in International Relations and Comparative Politics," *Annual Review of Political Science* 4 (2001): 391–416, doi:10.1146/annurev.polisci.4.1.391; and Alexander Wendt, *Social Theory of International Politics* (Cambridge, UK: Cambridge University Press, 1999).

41. UNGA A/70/174 (2015), 12.

42. Kenneth W. Abbott, Robert O. Keohane, Andrew Moravcsik, Anne-Marie Slaughter, and Duncan Snidal, "The Concept of Legalization," *International Organization* 54, no. 3 (2000): 401–19; http://www.jstor.org/stable/2601339.

43. International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, 2001, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

44. International Commission on Intervention and State Sovereignty, *The Responsibility to Protect* (Ottawa, ON: International Development Research Centre, 2001), http://responsibilitytoprotect.org/ICISS%20Report.pdf.

45. Ibid.

46. UNGA A/70/174 (2015), 11.

47. Ibid., 8.

48. Ibid.

49. Ibid., 11.

50. A complete list of FIRST members (accessed 15 June 2015) can be found at https://www.first.org/members/teams.

[51] UNGA A/70/174 (2015), 11.

[52] On "special and differential treatment," see Alexander Keck and Patrick Low, "Special and Differential Treatment in the WTO: Why, When and How?" *WTO Staff Working Paper* No. ERSD-2004-03 (2004), accessed 15 June 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=901629.

[53] UNGA A/70/174 (2015), 11.

[54] Conor Foley, "Welcome to Brazil's Version of 'Responsibility to Protect'," *The Guardian*, 10 April 2012, http://www.theguardian.com/commentisfree/cifamerica/2012/apr/10/diplomacy-brazilian-style.

[55] James A. Lewis, "Heartbleed and the State of Cybersecurity," *American Foreign Policy Interests* 36, no. 5 (2014): 294–99, http://dx.doi.org/10.1080/10803920.2014.969176.

[56] Jon Brodkin, "Tech Giants, Chastened by Heartbleed, Finally Agree to Fund OpenSSL," *Ars Technica*, 24 April 2014, http://arstechnica.com/information-technology/2014/04/tech-giants-chastened-by-heartbleed-finally-agree-to-fund-openssl/.

[57] Tony Scott, Executive Office of the President, Office of Management and Budget, memorandum, subject: Policy to Require Secure Connections across Federal Websites and Web Services, 8 June 2015, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf.

[58] Hollis, "An e-SOS for Cyberspace," 426.

[59] Mark Raymond, "Renovating the Procedural Architecture of International Law," *Canadian Foreign Policy Journal* 19, no. 3 (2013): 268–87, http://dx.doi.org/10.1080/11926422.2013.845580; Abbott and Snidal, "Hard and Soft Law."

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.