Explorations in Cyber International Relations

Massachusetts Institute of Technology   Harvard University

Depleted Trust in the Cyber Commons

Roger Hurwitz

Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology

October 1, 2012

Depleted Trust in the Cyber Commons

Roger Hurwitz

Policymakers increasingly recognize the need for agreements to regulate cyber behaviors at the international level. In 2010, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security recommended "dialogue among States to discuss norms pertaining to State use of ICTs [information and communications technology], to reduce collective risk and protect critical national and international infrastructure."[1] Since then, the United States, Russia, China, and several other cyber powers have proposed norms for discussion, and in November 2011, the United Kingdom convened an intergovernmental conference to discuss cyber "rules of the road."[2] These activities are a positive change from the first decade of this century, when the United States and Russia could not agree on what should be discussed and the one existing international agreement for cyberspace—the Budapest Convention on Cybercrime—gained little traction. Nevertheless, the search for agreement has a long way to go. Homeland Security secretary Janet Napolitano noted in summer 2011 that efforts for "a comprehensive international framework" to govern cyber behaviors are still at "a nascent stage."[3] That search may well be disappointing. Council on Foreign Relations fellows Adam Segal and Matthew Waxman caution that "the idea of ultimately negotiating a worldwide, comprehensive cybersecurity treaty is a pipe dream." In their views, differences in ideologies and strategic priorities will keep the United States, Russia, and China from reaching meaningful agreements: "With the United States and European democracies at one end and China

and Russia at another, states disagree sharply over such issues as whether international laws of war and self-defense should apply to cyber attacks, the right to block information from citizens, and the roles that private or quasi-private actors should play in Internet governance."[4]

This essay joins that pessimism on the basis of a more extensive model of the emerging crisis in cyberspace. The essential argument is that maintaining a secure cyberspace amounts to sustaining a commons which benefits all users, but its overexploitation by individual users results in the well-known "tragedy of the commons."[5] Here the depletable common resource is trust, while the users are nations, organizations, and individuals whose behaviors in cyberspace are not subject to a central authority. Their actions, which harm the well-being of other users, diminish trust and amount to overexploitation of a common resource. The tragedy of the commons is used repeatedly as an argument for privatization and in retrospect to justify the enclosure movement by English agricultural capitalists in the seventeenth and eighteenth centuries. However, such a tragedy is not inevitable, even when users of a commons are assumed rational in the sense of maximizing self-interest. The late political scientist Elinor Ostrom received the Nobel Prize in economics for determining cases and conditions where, in the absence of government control, users successfully self-organized for sustainable use of a commons.[6] Unfortunately, as argued below, the current state of cyberspace and its users does not meet most conditions that encourage such self-organization. Both the affordances of the cyber technologies—that is, the way the technologies enable their use—and the mentalities of the users contribute to the unfavorable result.

Embedding the obstacles to international agreements within this wider perspective will highlight the challenging multilayered, complex, and transformative processes that cyberspace presents to states and other entities that would manage it. It is not a passive domain where states can pursue preexisting competitive or conflicting interests, but one whose rapidly changing technologies and applications create opportunities for conflict. It also reasons for cooperation. Accordingly, the next section develops the model of cyberspace as a social system based on a commons—a "socioecological system" (SES) and a "common pool resource" (CPR) to use Ostrom's terminology—that can be sustained but also depleted. The identification of trust as this "resource" and the implications of its depletion will receive particular attention. The third section reviews the variables which Ostrom and her associates have found to encourage self-organization and

evaluates them with regard to cyberspace. The last section considers which of the model variables that currently discourage self-organization could be changed in a more encouraging direction through feasible actions by agents, thus removing some obstacles to reaching international agreements. It also considers how states, absent these changes, might unilaterally respond to cybersecurity crises.

Challenges of the Cyber Commons

Governing a commonly accessible resource, or CPR, is a collective action problem, whether the goal is sustainable exploitation of a fishery or the secure, beneficial use of cyberspace. For natural CPRs, where regeneration of the stock occurs, some limits on individuals' use by amount or kind are needed, lest aggregate use exceed the "carrying capacity." This depletes the resource below the level at which natural processes can sustain it for profitable exploitation. As discussed below, this need for limiting exploitation can also hold for man-made or artificial resources like cyberspace. Limiting or regulating use usually requires a preexisting state or other authority with coercive power, in whose territory the CPR is found—with good reasons. Although the users might recognize the need for limits, individual users are tempted to exceed them in the belief that the added strain on the resource is negligible with regard to its sustainability. Also, individuals who notice their neighbors' violations might be unwilling to punish them for fear of retribution. Nevertheless, Ostrom found many cases where people successfully managed a CPR without the need for state intervention or privatization. In analyzing these, she conceptualizes the CPR as existing within a context of its users' socioeconomic and cultural practices. These practices affect both individual users' choices about exploiting the CPR and the possibility of their collective regulation to sustain it. The CPR and the social context taken together constitute the socioecological system.

One might wonder how a domain can be a commons when every bit of its physical substrate is owned by some organization or a state in contrast, say, to oceans, international airspace, and outer space. Several answers are useful to refining our notion of a cyber commons and any international agreements that would protect it. Lawrence Lessig referred to a model of Internet communication transport that includes layers for the physical substrate, the electronic packets or envelopes for the information, and the

information content itself. He identified the commons with the packet layer, which everyone has a right to access and to which everyone can contribute, so any blocks to the free flow of packets closes the commons.[7] On this view, the cyber commons is similar to the oceans or international airspace, with its users' primary concern being right of passage.[8] Lessig and others ultimately grounded this idea of the cyber commons in the human right to access information and express one's opinion. It also resonated with notions of freedom of mobility, global innovation for the Internet, and an evolving worldwide information sphere in which everyone could participate—with the resonance captured in a word: "open." Endeavors like Wikipedia, the Creative Commons, MIT's free courseware, and the emergent blogosphere could create a second commons—one of content. At the turn of the millennium, Lessig saw such efforts threatened by media content companies, with their broad interpretations of copyright at the expense of fair use and their enlistment of state authorities for draconian treatment of alleged copyright violations. He discounted the argument for a need to protect the intellectual resources from depletion by invoking Thomas Jefferson's image of the candle whose light is undiminished in lighting another candle—a trope for the Enlightenment that encapsulates the promise of the Internet. The unfolding drama was rather that of greedy organizations using the possible misdeeds of a few individuals as a pretext to privatize common intellectual property and undermine the access needed to sustain an Internet culture.[9]

This idea of a "cyber commons" appeared more than a decade ago, when the online population was a tenth of its present size and concentrated in North America and Western Europe, where the Internet was easily seen as another venue in an already rich, lightly regulated, information and communication ecology. It ignored, however, that the Internet was already used by groups in violent struggle against some states—Chechen separatists against Russia—and even liberal states were already proscribing access and distribution of certain information, such as child pornography. Since then, the use of cyberspace, now spilled well beyond the Internet, has become so ubiquitous a national security issue ("securitization") or a threat to regime stability, that many governments now filter or block certain packet flows, thus replacing the primary cyber commons with their own "safe" enclosures.[10] Nevertheless, the vision of a cyber commons informs significant parts of the cyber policies of the United States and many of its allies and the positions they take with regard to international regula-

tion of cyberspace. Most notable is the State Department's embrace of Internet freedom—the rights of cyber enablement of civic activism—but also significant is the emphasis on global interoperability, noninterference by states with packets passing through their territories, and decisions on Internet technology being made by technologists rather than by political authorities.[11]

A more identifiable CPR, in keeping with the Ostrom SES model, however, is bandwidth, which can be depleted by spam—an overexploitation of the resource—resulting in degraded delivery of more-valued communications. Spammers have been compared to industrial polluters of natural resource commons because they also pass along to a general public the negative externalities of their actions, whether in the form of users' wait times in a saturated network or added costs for more bandwidth, spam filters, and so forth.[12] The spam phenomenon can be generalized to the consequences of depletion in the general public's "sense of security"; as a by-product of online scams and identity thefts at the individual level; industrial espionage at the organizational level; and infrastructure attacks, like Stuxnet, at the national level. These spur broad demands for cybersecurity measures, which are expenses. The provision of these measures, which usually have little effect in stemming the threats, decreases the economic efficiency of cyber-based communications and control. Since the Internet's capability of lowering transaction costs is considered one of its primary benefits for economic and social development, the possible high costs of cyber security are challenging for many states and organizations, perhaps as challenging as the consequences of attacks in the absence of adequate security.[13]

Cyberspace as a Social System

Closely associated with such insecurity is the decline in public or social trust, which might be identified as the ultimate common pool resource in the cyber SES. Jacques Bus follows sociologist Nicolas Luhmann in explaining trust as "a mechanism that reduces complexity and enables people to cope with the high levels of uncertainty and complexity of (contemporary) life." He adds,

> Trust expands people's capacity to relate successfully to a real world whose complexity and unpredictability is far greater than we are capable of taking in. In this sense, it is a necessary mechanism for people to live their lives: to communicate,

cooperate, do economic transactions, etc. It enriches the individual's life by en-
couraging activity, boldness, adventure and creativity, and by enriching the scope
of the individual's relationships with others.[14]

The notion of public trust, as used here, also includes people's confi-
dence in the institutions, laws, government, and infrastructures of their
societies. Public trust with regard to cyberspace encourages individuals
and organizations to access and be accessed by one another online, and
that in turn enables the network effect in cyberspace; that is, the positive
externalities created as more people participate in the network and more
interactions occur. This is consistent with findings by social scientists of
strong positive correlations between public trust and economic growth.[15]

Public trust in cyberspace involves both confidence in the people and
organizations individuals deal with through the digital technologies and
the trustworthiness of the technologies themselves. Confidence in others
online is problematic because those others might be anonymous or only
partly identified, and the context of interactions with them is opaque or
confusing. It can be buttressed by assumptions about others' concerns
for reputation and commitments to roles and by online mechanisms, like
certificates and ratings, which can confirm claims made by others. Of late,
however, trust in cyberspace may be strained by the publicity for the vari-
ous cyber threats noted above, organizations' and governments' failures
in deterring them, and the compromise of online security mechanisms,
like stolen certificates. In addition, public trust suffers from many users'
awareness that their online activities are being monitored, whether for
commercial exploitation in the West or identification of political dissi-
dents in authoritarian countries.

These abuses may lower or deplete public trust—that is, the aggregate
willingness of users to go online—much like overexploitation by some of
its users depletes a CPR. On this view, public trust is a rival good whose
consumption by a user decreases the amount available for consumption
by others. By analogy, continuing abuses against a diminishing public
trust could lead to unsatisfactory provision of the online benefits which
public trust enables. In concrete terms, individuals and organizations fear-
ing cyber crime, invasions of privacy, and so forth would greatly decrease
their use of digital networks for economic transactions, information ex-
changes, and social interactions. But unlike the usual commons resources,
such as forests and fisheries, public trust in cyberspace is not always a rival
good. Mutually beneficial online interactions will sustain and increase,

and these are so plentiful at the individual and organizational levels that the abuses are often ignored or quickly forgotten. Consequently, there is little evidence of people exiting cyberspace or avoiding popular sites with controversial privacy policies. Still, in some democratic countries, relevant publics have demanded that service and search providers restrain tracking; some governments have already responded with regulatory policies, which will force adjustments by data aggregators and analysts. These actions can be read as instances of users defending a CPR by turning to existing authority for leadership and norm setting. They show that in addition to security technologies, sustaining trust in cyberspace requires rules, transparent practices, accountability standards, and means of redress acceptable to users. International efforts for agreements to protect and sustain cyberspace will therefore need to take such concerns into account, to some degree. That might not be a formidable challenge. Because cyber "apps" have become indispensable for so many users, they are likely to be reassured, at least momentarily, by small, facile steps by providers or regulators, including policy announcements, opt-out buttons, and new, if unintelligible, service agreements. Put another way, cyberspace is no longer a domain apart from its users, a place to visit at one's choosing, like a tourist resort, but has penetrated and rewoven the fabric of our lives.[16]

Arguably, the spammers, hackers, data collectors, criminal gangs, cyber activists, and state agencies which threaten public trust are not seeking to destroy the Internet or freeze cyberspace—no more than peasants who allegedly overgrazed the commons wanted to degrade it. Ostrom's work implies two types of agents damage the CPR: poachers from outside the group that maintains the SES and members of the group who exceed their rights to the CPR. By this reckoning, the spammers, cyber criminals, terrorists, and certain activists—for example Lulzsec—would be the poachers in cyberspace. In popular imagination, and sometimes in their own imaginations, they fill the traditional image of pirates—individuals and groups outside nations and beyond the laws of nations.[17] Indeed, some analysts believe that international cooperation to suppress such groups can be easily realized and comprise a first step toward more comprehensive agreements on cyberspace. Of course, as poachers or parasites, these groups are not seeking the demise of cyberspace, since that would put them "out of work."

The second type includes governments, online service providers, multinational corporations, and others—the so-called stakeholders—who recog-

nize the need for limits but will frequently flaunt such limits in the pursuit of individual interests. Even states that develop cyber weapons to damage cyber-based infrastructures and governments that spy on their online citizens value their own use of cyberspace while planning to constrain its use by others. The resulting ambivalence of many governments is perhaps best captured in a recent Chinese white paper, which celebrates the Internet for enabling economic and social development, notes its use in propagandizing the public and in campaigns against provincial corruption, but stipulates that

> no organization or individual may produce, duplicate, announce or disseminate information [on the Internet] having the following contents: being against the cardinal principles set forth in the Constitution; 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.[18]

On this view, the strategic problem with the Internet is not its dual use but its many uses. So many, in fact, that unilateral efforts like deep packet inspections to contain the "unwanted uses" themselves threaten the stability and sustainability of cyberspace.

Sophisticated actors who threaten public trust in cyberspace might foresee the adverse consequences of their acts. They might also calculate that whatever the damage they do, the depletion of public trust will be modest or the gains in using the Internet still so great that public trust and mutual accessibility will remain above some minimum threshold. As noted, recent trends support that calculation. Yet, to the point that their conduct cannot be generalized or continue indefinitely—without devastating consequences, that is—to the question, "What if everyone always acted like you?" they must still answer, like Yossarian, "I would be a damned fool not to." The alternative is for all the Yossarians to act together to change the situation. Is that possible in cyberspace under current conditions? Can a significant number of relevant actors abandon practices that threaten it and commit to rules that sustain it?

Self-Organizing Variables

Ostrom and her associates have identified 10 variables critical for self-organization in a socioecological system—that is, effective and enforced rules of use for a common pool resource in the absence of state authority.[19] Each variable is explained below, sometimes introduced with direct quotations from Ostrom (either italicized or in quotation marks), while manifestation in cyberspace is described and evaluated with regard to its effect on self-organization. Encouraging, discouraging, and neutral effects are indicated by +, –, or 0, respectively. The variables concern properties of the resources being exploited in the SES and characteristics of the user population. In keeping with the observation that public trust in cyberspace depends on the trustworthiness of its hardware and software, as well as the behavior of their users, their properties are considered in evaluating the relevant variables.

As will be seen, Ostrom's explanations of the variables' effects on the possibility for self-organization are consistent with a rational actor model: the probability of self-organization increases the more its contribution to sustaining the common resource exceeds the costs of bringing agents to agreements and enforcing those agreements. Hence, the lower these costs, the greater the probability of self-organization. The assumption with regard to its process is that states through multilateral agreements would set rules and regulations for cyberspace; they would either enforce these directly or empower an international agency to do so.

Size of Resource (–)

Large resources with ill-defined boundaries discourage self-organization because of the high costs of defining the boundaries, monitoring use, and tracing the consequences of malfeasance.

The size of cyberspace, as measured by the several billion devices connected to the Internet, discourages defining its boundaries and monitoring behaviors in it. As a thought experiment, suppose "boundaries" for a trustworthy cyberspace were defined by a centrally maintained giant list of several billion verified safe devices, with "safe" designating malware-free or not having been involved in spying or other penetration operations. This list would require continual updating to accommodate devices being added to the Internet and recurrent verification of the safe devices, because anyone could be vulnerable to attack from a host spoofing a safe device. This approach would be very expensive and only partly effective in

inspiring users' trust; some attacks are so stealthy as to be discovered only well after they have occurred, if at all.

Mapping boundaries and monitoring behavior can be more feasible, affordable, and convincing if national governments assume responsibility for the devices and users in their territories by certifying the machines and credentialing the users. Unilateral and multilateral means could then protect the defined national cyberspaces. Such means include implementations of "national firewalls" and the reduction of national portals, cyber passports for users, and assignment of consecutive IP addresses to specific territories. These steps would not stop all external attacks and exploits within a national cyberspace, but they would facilitate determining the origin of attacks and holding responsible authorities in the state where an attack originated.[20]

The resulting system would extend the principle of national sovereignty—the cornerstone of contemporary international relations—into cyberspace[21] and increase a state's control over its residents' online activities. Some states, including a few liberal democracies in the West, have already adopted or advocated some of these measures to deal with cyber security threats. However, many governments, organizations, and individual users will oppose full-blown development of the system for several reasons. First, it would sanction the fragmentation of the Internet into many an "internet in one country" with an attendant constriction of global communications. That process, already foreshadowed in China, Iran, and other authoritarian countries, would set back efforts to build a commons for discussion of items like climate change, scientific knowledge, and medical research on a global agenda. Second, multinational corporations and other agents of globalization, including economic managers in authoritarian countries, will consider this system an obstacle to a global economy in which businesses anywhere can have suppliers and customers everywhere. For them, a particularly threatening aspect of the projection of national sovereignty into cyberspace is the potential restriction in movement of information resources. Third, human rights advocates will oppose conceding the right to define a cyber attack to national governments, since their definitions can include a broad swath of content, as noted above in regard to China, as well as malicious code. Fourth, policymakers are likely to doubt whether governments will accept responsibility for cyber attacks originating in their territories under this system. These doubts can be grounded in

current practices of government claiming ignorance of the attack origins or that they do not have the means to suppress all of them.

Finally, national boundaries in cyberspace are a way of dissecting the commons and privatizing the pieces. Because this commons is a network, its dismantling involves a loss of value. That is, the sum of the values of the parts will be less than the value of the original whole. The loss will be defined in different ways, but its anticipation will motivate broad resistance to the idea of national cyber borders. Nevertheless, the idea brings into relief questions about the character of the cyber commons: whether it is a thin communications overlay on, and ultimately reduced to, diverse geophysical entities and jurisdictions, or does it provide sets of experiences— a mode of being—in which users might acquire new identities transcending national identity. Jacques Bus considers the question, thankfully free of the usual panegyrics about the Internet flattening the world:

> Globalization, driven clearly by new ICTs and the Web, creates understanding hence more trust through spreading information on history and reputation of societies, characteristics of societies and the lives of persons living in certain societies, and allowing easy worldwide communication. This may indeed lead to further erosion of the concept of "the human animal is best off at home." It may well lead to the need for a completely new view on societies and their cohesion and the role trust must play in this.[22]

Number of Users (–)

The more users of a CPR, the greater the transaction costs of getting them together and agreeing to change. So group size discourages self-organization, but "its effect on self-organization depends on other SES variables and the types of management tasks envisioned."

The two billion people who already access the Internet constitute the largest users group in human history. They should have opportunity to express their concerns in any international negotiations on the uses of cyberspace, since in many cases these are likely to be different from those of governments and other powerful stakeholders. For example, users in struggles against their own governments would certainly reject those governments' representation of their interests regarding anonymity, online tracking, and permitted content. On the other hand, recent world meetings on climate change and on cyberspace itself have demonstrated that processes which are open to groups claiming to represent individual citizens' interests can rapidly become unmanageable, time consuming, and unproductive. For that reason, an interpretation of national sovereignty,

per which states rightfully represent their citizens' interests, is expedient if not just.

Unfortunately, even this stratagem will not reduce the relevant stakeholders to a manageable number. Negotiations will need to include representation of industrial sectors, especially ICT, and international organizations represented, as well as the states, since these can provide the technical knowledge to inform proposals but can also block implementations of any agreements reached without them. As Ostrom suggests, the number of parties involved might not itself determine the difficulty in reaching an agreement. Rather when more parties are involved, especially when the issues are complex, there will be a greater number of competing claims that take time to reconcile, if they can be reconciled at all. Negotiations for the UN Convention on the Law of the Sea (UNCLOS), which regulates another commons, lasted a decade despite building on centuries of admiralty law and being more confined to issues of state sovereignty. There is much less legal tradition for cyber and, so far, no concerted efforts to harmonize state-level cyber laws. Thus, the very limited and regionally oriented Budapest Convention on Cybercrime has been slow in gaining adherence, with many of its signatories listing numerous reservations.[23] Perhaps some relief from these bleak prospects might be provided by cyberspace itself, in that aggregation of opinions, consultations, and negotiations can themselves now be conducted virtually as well as in person. By organizing information, lowering transaction costs, and speeding communications, cyber tools might permit decision making about their own futures.

Resource Unit Mobility (–)

> *Due to the costs of observing and managing a system, self-organization is less likely with mobile resource units . . . than with stationary units, such as trees and plants or water in a lake.*

Three types of mobility of devices make their effective, actionable monitoring difficult and costly. First, as already noted, the status of a device can change rapidly from "safe" to "compromised," frequently without the change being discovered until later, if at all. Second, over their course, wide-scale cyber attacks and exploitations will typically deploy different machines located at different IP addresses and geophysical locations. For example, during the massive July 2009 distributed denial of service (DDoS) attack on US government sites, the command and control (C2)

sites reportedly migrated from computers in South Korea to some in Chicago and Berlin. Therefore, any monitoring or defense specific to an attack, like blockading potential C2 sites, will probably involve multiple jurisdictions with consequent problems of coordination. Later investigations will be similarly complicated and attribution inevitably uncertain. As a result, parties to an agreement barring such attacks cannot rely on monitoring to verify that they are complying with the agreement or to identify violators. Third, the rise of mobile computing in the form of laptops, smart phones, and tablets has greatly increased the attack surface of cyberspace and the chore of any future monitoring program. The physical mobility of these devices also means they are exposed over their lifetimes to a variety of cyber threats and surveillance environments and to changes in their own security status. They will be more vulnerable than a machine tethered to a single server within an organization setting that has competent cyber security. They are more liable to penetration, theft of their information, and compromise. Once compromised, they can be turned into carriers for compromising networks to which they later connect, like corporate intranets.[24]

Importance of Resource to Users (+)

In successful cases of self-organization, users are either dependent on the [resource] for a substantial part of their livelihoods or attach high value to the sustainability of the resource.

An increasing amount of activity throughout the world involves the creation, collection, packaging, use, and distribution of information. The Internet and other parts of cyberspace are vital to these activities. Various government position papers on cybersecurity are clear in recognizing the economic, social, cultural, and scientific importance of cyberspace. In calling for the "creation of a global culture of cybersecurity," the UN General Assembly recognized that

> the increasing contribution made by networked information technologies to many of the essential functions of daily life, commerce and the provision of goods and services, research, innovation and entrepreneurship, and to the free flow of information among individuals and organizations, Governments, business and civil society.[25]

Even authoritarian regimes in Iran, Egypt, and elsewhere, which confronted massive protests organized by cyber means, have hesitated shutting

down the Internet in their countries because of their economies' dependence on it.

Governments and diplomats, however, have been less clear in recognizing how foundational public trust is for cyberspace. In calling for discussions of international norms for cyberspace, the UN group of governmental experts took mainly a national security perspective: Cyber crime and other cyber threats are disruptive to government, economic, and social functions; lack of a common understanding of the intents behind certain behaviors in cyberspace can lead to conflicts which might escalate to threaten international security.[26]

Productivity of System (+)

> *If [a resource] is aready exhausted or very abundant, users will not see a need to manage for the future. Users need to observe some scarcity before they invest in self-organization.*

The growth of cyber crime, the incidence of attacks and exploits, the proliferation of malware, and threats to critical cyber infrastructure have raised questions whether the benefits of cyberspace can be sustained under present security practices. These questions clearly motivate the various calls for international agreements on cyberspace behavior. Jacques Bus notes that the possibility of states being behind many cyber threats "proves the urgency to come to international agreements on restraints in and defense against cyber attacks and for international cooperation to bring it under control."[27] Having identified public trust as the depletable resource in cyberspace, Bus continues, "Public and private sector must work together at the international level to build a well balanced infrastructure of technology and law/regulation that will give citizens trust to use the opportunities of the new digital world."[28] In a speech to the 2011 Munich Security Conference, British foreign minister William Hague made similar connections:

> We are working with the private sector, to ensure secure and resilient critical infrastructure and the strong skills base needed to seize the economic opportunities of cyber space, and to raise awareness of online threats among members of the public. But being global, cyber threats also call for a collective response. In Britain we believe that the time has come to start seeking international agreement about norms in cyberspace.[29]

Predictability of System Dynamics (0)

System dynamics need to be sufficiently predictable that users can estimate what would happen if they were to establish particular . . . rules or no-entry territories.

The consequences of a continuing lack of international regulation are more predictable than the effect of agreement and monitoring for some standards of behavior. With deterioration of public trust in cyberspace, the expansion of use—in terms of time spent, applications, and dependencies—will decelerate, and that will be accompanied by lower growth or drop in the incentives for development. Some users may have already reduced their use of public networks for critical data transmission; some organizations have reduced the number of access points or portals to themselves. These steps might grow toward widespread delinking and fragmentation—phenomena which devalue cyberspace.

Projecting the loss in value of a vulnerable cyberspace compared to a safe one is problematic because of different models for evaluating the socio-economic value of cyber networks. However, it seems reasonable to suppose that as new users are drawn more from lower economic strata and less-developed countries, the economic value of the networks will increase at a lower rate than in earlier stages of their growth.[30] Such a trend has mixed implications for self-organization. First, providers will have little incentive to increase their investments in cyber security—especially if security costs are a linear function of the number of users. But inaction by the providers could put more pressure on governments to work for agreements that reduce threats. On the other hand, the trend also suggests that any exit of users will not initially diminish network value. So, until the situation is deemed intolerable and not just bad, governments, mindful of the costs of agreements, could resist pressure and delay self-organizing, despite their public calls for action.

Leadership (0)

When some users of any type of resource system have entrepreneurial skill and are respected as local leaders as a result of prior organization for other purposes, self-organization is more likely.

Leadership is lacking for potentially productive, state-level negotiations, but not for want of actors that have had roles in organizing cyber-

space. Over the past decade, the Internet Corporation for Assigned Names and Numbers (ICANN) has provided competent, although frequently criticized, administration of domain allocations and oversight of registration. It has accommodated the spectacular growth of the Internet and accompanying commercial demands with a redesign of policies for top-level domains. While it has not been particularly open to the grassroots participation specified in its multistakeholder model, it has retained the confidence of service providers and the respect of most states, as evidenced by the UN's restraint from seeking involvement in administration of the Internet. But the ICANN is no norms entrepreneur and lacks the political skills and leverage to reconcile competing interests among states over cyber behaviors and security. Additionally, it is seen by many states as a tool of US policy.

The Internet Engineering Task Force (IETF) has exercised leadership in Internet protocols, mostly as the endorser of standards. Its own history exemplifies self-organizing among stakeholders for management of a commons, but its amorphous decision-making process is an awkward model for negotiations on constraining human activities. In any case, it is unqualified to lead in such negotiations, its ambit is limited to the technical realm, its centrality in that realm has diminished as concerns now focus more on mobile computing apps and other layers beyond its purview, and its membership is still heavily American and European.[31]

The International Telecommunications Union (ITU), the UN agency responsible for ICT, has the ambition to lead policymaking and administration of cyberspace, and it led in organizing the World Summits on the Information Society (WSIS), which focused on soft issues: development-oriented uses of cyberspace, Internet governance, bridging digital divides. Seen in the West as a tool for Russian and Chinese policy interests, it lacks the political credibility to assume leadership on hard issues like cyber espionage, information rights, and so forth. It probably also lacks the technological competence; the cybersecurity standards it developed and promoted in collaboration with the International Organization for Standardization (ISO) have proved expensive and unworkable.

Norms/Social Capital (+)

If users share norms of reciprocity and sufficiently trust one another to keep agreements, they will face lower transaction costs in reaching agreements and monitoring. Continued economic globalization and the ab-

sence of major interstate wars could suggest that the major powers are developing adequate reciprocity structures and conflict avoidance mechanisms. Indeed, this assessment is supported by the fears expressed in the calls for cyber norms that misunderstandings about cyberspace behaviors could trigger unwanted conflicts. Nevertheless, the failure of negotiations on environmental regulations raises doubts that negotiations over cyberspace can fare any better, especially since the major powers have ideological differences regarding cyberspace, as great as the differences among economic interests that block resolutions of environmental issues.

Broadly speaking, the Russian and Chinese 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 its territory.[32] From a Western perspective, their motives are to control the ideational space that cyber networks afford their populations and to prevent inquiry into use of cyber by their governments or proxies for military campaigns, political espionage, industrial espionage, and crime. Recall, however, that the political traditions in Russia and China, even in the pre-Communist days, empowered state authorities to decide what their citizens should think, and that the principle of national sovereignty bars outsiders from interfering with the exercise of that power. Furthermore, Russian officials are keenly aware that Chechen insurgents or terrorists have used cyber technologies in their violent struggles against Russia. So an uncontrolled Internet can be politically threatening and easily exploited by external rivals, in particular the United States. For example, when cyber-fueled protests occurred in Russia, premier, presidential candidate, and target of the protests, Vladimir Putin, branded these protests the work of "foreign enemies."[33] On this view, outsiders enabling dissent within a country is no contribution to public debate; it is "information warfare" conducted to weaken regimes to the point of greater accommodation with the outsiders or even collapse. Already, in 2008, Russia, China, and other members of the Shanghai Coordination Organization (SCO) have agreed to outlaw supporting or hosting the dissemination of potentially 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 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 functions, there follows a multistakeholder model for control and defense of cyberspace, with states being one type of stakeholder, along with nongovernmental organizations, service providers, ICT companies, critical infrastructure entities, corporate users, and individual users. But because cyberspace, particularly the Internet, is prey to attacks and exploits by criminals, terrorists, and even states, by virtue of their authority and capabilities, states have primary responsibility to provide the needed security without harming the interests of other stakeholders. The diffusion of norms and treaties, such as the Budapest Convention on Cybercrime, are instruments for fulfilling such responsibility, as are the nurturing of a cyber-security culture and capabilities around the globe.[34]

This view, wedded to a decade-old vision 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 interest of all are now controversial and contested.[35] India, Brazil, and South America— leading voices on cyber issues among "nonaligned" countries—want these changes to be acknowledged as conceded major parts in any negotiations. They consequently favor transfer of authority away from technologically oriented agencies, reflecting the multistakeholder model, including ICANN and IETF, to a more policy-oriented agency, possibly under the UN, though not necessarily the ITU, that gives every state an equal voice.

Knowledge of the Socioeconomic System (+)

When users share common knowledge of relevant SES attributes, how their actions affect each other and rules used in other SESs, they will perceive lower costs of organizing.

The various calls for cyber rules reflect policymakers' knowledge that certain behaviors disrupt normal activities, sow public distrust, and threaten the sustainability of cyberspace. Their willingness to discuss issues beyond cyber crime acknowledges that those misbehaving may include their own governments and citizens. So, less time and money are needed to raise

consciousness or convince skeptics that a problem exists and international cooperation can help solve it. Choosing what to do requires more knowledge of the dependencies among various processes in cyberspace, particularly how the technological affordances affect social (agents') behaviors. The efforts at environmental regulation show that broad, comprehensive solutions will be opposed even when those who feel threatened by the proposal are offered side payments. So the problem space has to be decomposed with selection of some target whose proposed solution could gain traction, help reduce the overall level of cyber insecurity, and build confidence among the various agents, thus enabling pursuit of other targets. One frequent suggestion is that states cooperate to suppress cyber criminal gangs by denying their means to monetize their thefts. This suggestion understands (a) the gangs' dependency on particular banks and (b) that cyber crime serves as a development lab and testing ground for malware that might later be used by intelligence agencies in some states. Less known is how strongly these agencies depend on the gangs and, therefore, the incentives their states need to cooperate on the proposal.

Collective Choice Rules (0)

When users have full autonomy at the collective-choice level to craft and enforce some of their own rules, they have lower transaction costs as well as lower costs in defending the resource against invasion by others.

This variable implies that the more people can see themselves as authors of the rules they are expected to follow, the more they will follow those rules. This result is important for cyber security and public trust in cyberspace, because good "computer hygiene" at the organizational and individual levels can blunt a considerable amount of computer crime and exploits, perhaps as much as 80 percent.[36] Unfortunately, the number of users and the diffuseness of their representation would seem to preclude public participation in making rules, as mentioned before. Consequently, users will be less able to see their rule following as part of a global interdependent effort to sustain cyberspace and therefore their own benefit from it. The top-down directives they receive will more likely justify the rules only in terms of protecting the individual or organization.

Changing Variables and Crisis Response

The values of the Ostrom variables, summarized in the table below, do not favor self-organization in the cyber SES. Conditions are not ripe for productive, enforceable agreements under which stakeholders, especially states, limit their trust-eroding cyber behaviors. As indicated by the positive values for the "importance of the resource" and "productivity of the system" variables, the widespread expressions of fear for the future of cyberspace has sparked interest in such agreements. However, nothing beyond that should be expected until the values of some technological and other social variables change. Arguably, the pursuit now of a comprehensive global agreement or fallback to agreements among the "like-minded" will be counterproductive. It will likely deepen distrust among major cyber powers and discourage the sharing of useful knowledge of the cyber SES. That seems to be the primary outcome of the recent London conference on cyber "rules of the road."[37]

Variable	Value
Size of resource	–
Number of users	–
Resource unit mobility	–
Importance of resource	+
Productivity of system	+
Predictability of system dynamics	**0**
Leadership	**0**
Norms/social capital	+
Knowledge of SES	+
Collective choice rules	**0**

Several feasible measures could improve prospects for effective agreements and/or sustain public trust in cyberspace. Consider the following changes.

Develop Global Identity Management

Jacques Bus recommends the development of a "globally interoperable trustworthy system for Identification and Authentication" as essential for

trust among Internet users.[38] States, including some liberal democracies, are already requiring verified identification from Internet users. Interoperability of local standards would facilitate, if needed, the identification of a user of an Internet-linked device anywhere. Users could retain some anonymity or privacy under this regime, since different sites and transactions would demand different degrees of disclosure. Authoritarian regimes could more easily identify people in cyber networks of resistance, but they might find they are better off not identifying nonviolent resistors, while trying to identify and suppress violent ones. That strategy could channel opponents toward the nonviolent networks and give the regimes more breathing room. Their restraint in this regard could enable states that support their opponents to cooperate in the identification system. In terms of the Ostrom variables, identity management reduces some of the deleterious effects of resource mobility.

Increase Public Participation on Cyber Security

Discussions of cyber security policies in informed, relevant publics can have the double effect of putting pressure on respective national governments and involving these publics in rule-making processes. The UN resolution for the "creation of a global culture of cybersecurity" anticipates that national cyber security efforts will have broad societal involvement, including that of the private sector, civil society, academia, and private individuals, but it is silent regarding rule-making roles for nongovernmental actors. The public-private partnerships that have already emerged in Europe and North America appear focused on coordinating organization-level efforts and sharing information, without critiquing or innovating policies. But nongovernmental members, particularly any transnational corporation (TNC) and international nongovernmental agency (INGO), for example Freedom House, should be encouraged to suggest rules. Many have experienced cyber attacks in a variety of legal and technological environments and probably know better than observers or governments what cyber laws and practices need to be harmonized across countries as part of international agreements.

The Internet Governance Forum (IGF), a consultative body established by the UN and based on a multistakeholder model, might also be used for public input into global-level conversations on rules for cyberspace. Its meetings have discussed cyber security issues but have so far deferred to national governments and specialized agencies for policy proposals. But

the IGF could use cyber tools and techniques, such as online surveying and crowd sourcing to collect and aggregate public opinion about rules and regulations needed in any future agreements.

Confidence Building through International Cooperation on an "Easy" Task

Although comprehensive agreements on cyberspace behaviors might be unattainable, international cooperation on some cyber threats and emergencies can be strong and effective, for example, the worldwide response to the Conficker worm or the working alliance of the Japan, China, and South Korea CERTs. In these cases, the cooperation builds upon "invisible norms" or commitments shared among cyber technologists, but it can give onlooking policymakers some confidence about their countries' working together on cyber problems. So, their confidence could grow with more cases where a challenge triggers a widely shared professional commitment and the ensuing cooperation achieves some success. Some cyber crimes seem suitable candidates for the challenge, notably child pornography, low-level fraud, and identity theft. There is, however, a need for some agency to take the lead in promoting the urgency of suppressing the chosen crime.

This essay has used economic reductionism to argue that conditions are not ripe for reaching and enforcing international agreements on the uses of cyberspace. The argument holds that if people who exploit a commons know that overexploitation will degrade that commons they can agree to limit their behavior, providing the costs of coming to agreement and enforcing it are affordable. In this argument, self-limitation is in service to self-interest—to sustain one's benefits from the commons. As far as the actor, whether individual, organization, or nation is concerned, cyberspace is just another domain where it pursues its self-interest. Cyberspace is, of course, much richer. It has become the basis and means for reorganizing much of contemporary social, economic, cultural, and intellectual life in developed countries. It provides a principal means for a global conversation about shared issues. To the extent it retains public trust, cyberspace cultivates new social bonds and identities that augment preexisting ones, like nationality. For all that, it commands some allegiance.

Even its advocates do not think an international cyber treaty would sufficiently protect states, organizations, and individuals from the various attacks arising in cyberspace. Although a treaty would be a restraint on its

signatories and facilitate sanctions of its violators, adequate cyber defense at the state level would still require resistance (hardening) of digital networks, especially those supporting critical infrastructure; resilience of organizations likely to be attacked; and reasonable deterrence with respect to nonsignatories. In the absence of international agreement(s), reliance on these other components would increase moderately. Furthermore, because digital networks are necessary for economic globalization, states will continue to cooperate on the technical plane and with regard to Internet governance at least to the point of assuring interoperability at the global level. Such cooperation will not extend to control industrial espionage, protect critical information infrastructures or assure information freedom, three issues which have recently emerged as foci of distrust among states. These and other cyber issues at the international level will likely be addressed in the midterm future in disjointed and incremental fashion—the strategy of muddling through. These are not necessarily bad results, and few users will experience any loss of benefits from cyberspace. On the other hand, the insecurity there will persist, and the opportunity to build public trust on a global level will have passed. **SSQ**

Notes

1. UN General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/65/201, 30 July 2010, http://www.unidir.org/pdf/activites/pdf5-act483.pdf.

2. For a review of the London conference, see Peter Apps, "Disagreements on Cyber Risk East-West 'Cold War,'" *Reuters*, 2 February 2012, http://www.reuters.com/article/2012/02/03/us-technology-cyber-idUSTRE8121ED20120203.

3. "Remarks by Secretary Napolitano before the Joint Meeting of the OSCE Permanent Council and OSCE Forum for Security Cooperation," Department of Homeland Security news release, 1 July 2011, http://www.dhs.gov/ynews/speeches/2011-napolitano-remarks-osce-council-austria.shtm.

4. Adam Segal and Matthew Waxman, "Why a Cybersecurity Treaty Is a Pipe Dream," *Council on Foreign Relations*, 27 October 2011, http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325.

5. See G. Hardin, "Tragedy of the Commons," *Science* 162 (1968): 1243–48, for the classic formulation of the argument.

6. Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge, UK: Cambridge University Press, 1990); and Ostrom et al., "A General Framework for Analyzing Sustainability of Social-Ecological Systems," *Science* 325, no. 5939 (24 July 2009): 419–22.

7. Lawrence Lessig, "The Public Domain," *Foreign Policy*, 30 August 2005, http://www.foreignpolicy.com/articles/2005/08/30/the_public_domain.

8. See for such analogy Abraham Denmark and James Mulvenon, eds., *Contested Commons: The Future of American Power in a Multipolar World* (Washington: Center for a New American Security, 2010).

9. In using the society of the English village commons as their governing metaphor, advocates of an Internet where information flows freely may have tended toward an idyllic or prelapsarian vision. In a dismissive review of Lewis Hyde, *Common as Air* (New York: Farrar, Straus, and Giroux, 2010), the work of one such advocate, David Wallace-Wells, quotes E. P. Thompson's assessment in his classic *The Making of the English Working Class* (New York: Vintage Books, 1966) that English agrarian culture before enclosure was "intellectually vacant . . . and plain bloody poor." Ignoring that enclosure forced people off the land and did not improve the lot of those who remained, Wallace-Wells argues by analogy that we are doomed to cultural sterility without the enclosures of broad copyright in "The Pirate's Prophet: On Lewis Hyde," *Nation*, 15 November 2010, http://www.thenation.com /article/155619/pirates-prophet-lewis-hyde?page=0,0.

10. For the securitization of cyber in the United States, see M. Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (New York: Routledge, 2008). For types and extent of enclosure practices, see Ronald Deibert et al., eds., *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT, 2008); and Deibert et al., eds., *Access Controlled* (Cambridge: MIT, 2010).

11. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington: The White House, May 2011), http://www.whitehouse.gov/sites/default /files/rss_viewer/international_strategy_for_cyberspace.pdf. See also Secretary of State Hillary Clinton, "Remarks on Internet Freedom," 21 January 2010, http://www.state.gov/secretary /rm/2010/01/135519.htm. The State Department's high-profile decry of foreign governments' politically motivated filtering led it to oppose the congressional antipiracy bills (SOPA and PIPA), which would have mandated commercially motivated filtering of foreign sites.

12. "Jo Twist, Web Guru Fights Info Pollution," *BBC News*, 13 October 2003, http://news .bbc.co.uk/2/hi/technology/3171376.stm. Another type of inordinate bandwidth consumption, the distributed denial of service, is intended to directly inflict some types of costs, such as reputational, financial, or political, on its target by forcing the target's web servers to crash under the crush of demands for service. DDoS can rise to the level of a national security matter, as exemplified in the 2007 attack on Estonian government and critical infrastructure websites.

13. Discussion of the obstacles and costs of "adequate" security for the current inherently vulnerable technologies of cyberspace are beyond the present scope. In addition to costs for cyber security personnel, they include much-less-estimable costs for revamping organizational cultures. Many firms, especially in the financial sectors, have reportedly chosen to defer such costs and to treat any loss to cyber crime or espionage as costs of doing business, while making efforts to suppress publicity of such losses for fear of the costs to their reputations. As this article goes to press, I learned that L. Jean Camp, "Reconceptualizing the Role of Security User," *Daedalus* 140, no. 4 (2011): 93–107, also applies Ostrom's analytic of self-organization to the challenge of cyber security. Camp's focus, however, is on the possibilities of individual end users forming small-scale communities in which information sharing on cyber threats and cyber hygiene are effectively practiced.

14. Jacques Bus, "Societal Dependencies and Trust," in Hamadoun Touré et al., *The Quest for Cyber Peace* (Geneva: International Telecommunications Union, 2011), 18.

15. Ibid., 19, citing Francis Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity* (New York: Free Press, 1995), and Robert Putnam et al., *Making Democracy Work: Civic Traditions in Modern Italy* (Princeton, NJ: Princeton University Press, 1993). For a negative example, see Anthony Padgen, "The Destruction of Trust and Its Economic Consequences in the Case

of Eighteenth-Century Naples," in *Trust: Making and Breaking Cooperative Relations*, ed. Diego Gambetta (London: Basil Blackwell, 1988), 127–41.

16. Iranians' use of the TOR anonymizing networks suggests that some users need cyber so much that even a small amount of reassurance will induce them to return to using previously compromised applications, despite the risks involved. The graphs for usage are spiked, showing that immediately after Iranian authorities announce a blockade or monitoring of a particular TOR site, the number of Iranian users on the network drops precipitously. It picks up again after TOR developers announce a workaround to the Iranian measures. See https://metrics.torproject.org/users.html?graph=direct-users&start=2010-11-28&end=2012-02-26&country=ir&dpi=72#direct-users.

17. Daniel Heller-Roazen, *The Enemy of All: Piracy and the Law of Nations* (Cambridge: MIT Press, 2008).

18. Information Office of the State Council of the People's Republic of China, "The Internet in China," 8 June 2010, http://www.china.org.cn/government/whitepaper/node_7093508.htm.

19. Elinor Ostrom, "General Framework for Analyzing Sustainability of Social Ecological Systems," *Science* 325 (24 July 2009): 419–22.

20. A view of "state responsibility" is elaborated in the Russian draft for a "Convention on International Information Security," presented to the Second International Meeting of High-Level Officials Responsible for Security Matters, Ekaterinburg, Russia, 22 September 2011, http://2012.infoforum.ru/2012/files/konvencia-mib-en.doc. A problem with any plan that assigns responsibility to states for the cyber behaviors of their residents is that many states lack cyber security awareness, capacity, and computer forensic capabilities. This problem and the role for technologically advanced nations to help less-advanced ones build such capacity are recognized in the US International Strategy for Cyberspace and the UN General Assembly Resolution "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures," A/Res/64/211, 17 March 2010, http://www.citizenlab.org/cybernorms/ares64211.pdf.

21. Chris Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 32–61.

22. Bus, "Societal Dependencies and Trust," 21.

23. Stein Schjølberg, "Wanted: a United Nations Cyberspace Treaty," in Andrew Nagorski, ed., *Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway* (New York: EastWest Institute, 2010), 11.

24. Ellen Nakashima and William Wan, "In China, Business Travelers Take Extreme Precautions to Avoid Cyber-Espionage," *Washington Post*, 26 September 2011, http://www.washingtonpost.com/world/national-security/in-china-business-travelers-take-extreme-precautions-to-avoid-cyber-espionage/2011/09/20/gIQAM6cR0K_story.html. See also Joel Brenner, *America the Vulnerable* (New York: Penguin Press, 2011), 61ff.

25. UN General Assembly Resolution 64/211: "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures," http://www.citizenlab.org/cybernorms/ares64211.pdf.

26. UN General Assembly Resolution 65/201: "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," http://www.unidir.org/pdf/activites/pdf5-act483.pdf.

27. Touré et al., *Quest for Cyber Peace*, 16.

28. Ibid., 25.

29. Foreign Secretary William Hague, "Security and Freedom in the Cyber Age—Seeking the Rules of the Road," speech to the Munich Security Conference, 4 February 2011, http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=544853682.

30. According to the well-known Metcalfe's law, the value of a network is proportional to the number of cross connections among its N users, that is N2. The growth (or decline) in value with each user who joins (leaves) the network is proportional to 2N. The more extreme Leek's law equates network value with the number of distinct audiences that can be formed from the number of users, i.e., the number of subsets less the null set of N or 2N – 1. So the value of the network would incredibly double (or be halved) with each user joining (or leaving). A more reasonable evaluation, especially for large networks, assumes differential use by those in the network. Consistent with power laws (long-tail phenomena), usage is assumed to decline exponentially with delay in joining the network. Usage or transactions over the N users describes a hyperbole, with the first joiners the heaviest users. The cumulative benefit, hence value of the network, is then proportional to the area under the curve or natural log of N (lnN). The increase (decrease) in network value with each person joining (leaving) is significantly less than estimated by Metcalfe's law, and the change is decreasing rather than increasing. Thus, if the network provider's cost of acquiring an additional user is fixed, a point of diminishing returns on value will be reached.

31. My thanks to Phillip Hallam-Baker for discussion of this point.

32. Ekaterinburg draft. (see note 20).

33. Michael Bohm, "Putin Chasing Imaginary American Ghosts," *Moscow Times*, 9 February 2012, http://www.themoscowtimes.com/opinion/article/putin-chasing-imaginary-american-ghosts/452802.htmlhttp://www.themoscowtimes.com/opinion/article/putin-chasing-imaginary-american-ghosts/452802.html.

34. See UN General Assembly Resolution 64/211: "Creation of a global culture of cyber-security and taking stock of national efforts to protect critical information infrastructures," adopted 17 March 2010.

35. Ronald Deibert and Rafal Rohozinski, "Contesting Cyberspace and the Coming Crisis of Authority," in Deibert et al., *Access Contested*, 21–41.

36. Brenner, *America the Vulnerable*, 239–44; and Brenner, personal communication, 2010.

37. Apps, "Disagreements on Cyber Risk East-West 'Cold War.'"

38. Bus, "Societal Dependencies and Trust," 24.