A GOVERNANCE SWITCHBOARD: SCALABILITY ISSUES IN INTERNATIONAL CYBER POLICYMAKING

CHRISTOPHER BRONK

Baker Institute for Public Policy, Rice University

MARCH, 2012

CYBERDIALOGUE2012

WHAT IS STEWARDSHIP IN CYBERSPACE?

Canada Centre for Global Security Studies

MUNK SCHOOL OF GLOBAL AFFAIRS

UNIVERSITY OF TORONTO

—In some places it is easier to have a good Internet connection than to have effective domestic sovereignty.[1]

WHICH IP? TECHNOLOGY OUTPACING GOVERNANCE

Twenty years ago, only a million computers were connected to the Internet, while today, perhaps as many as 2 billion people on the planet enjoy its use.[2] What was once primarily a tool for scholarly communications has quickly become the key infrastructure for communicating at a distance. At the core of this growth is the remarkable scalability of Internet Protocol (IP). Whether YouTube videos and Twitter microblog posts or telephone calls and sensitive military communications, IP is the technological backbone of digital connectivity on planet Earth.

IP grants a standard for data communication that scales to almost every computing device on the planet.[3] Because of this technology, and some exceptions notwithstanding,[4] the last twenty years have been a period in which a message can be transmitted from one computer to another anywhere, in large part because the set of instructions for delivery have been open, understandable, and relatively easy to implement. The economic transformation ushered in by this connectivity is well underway,[5] but its salient issues regarding politics, and more for the purposes of this paper, international politics, are still emerging. This is a newly constructed techno-informational space, often called "cyber" because there is something that clearly goes beyond just the delivery and receipt of data by IP.

CYBER, POLITICS, AND SOVEREIGNTY

The beginning of this decade may well mark a point of change in how political leaders regard the Internet and the larger related conceptual item we call cyberspace. True, there have been those who have successfully managed Internet connectivity through political turbulence—government response to internal disturbances in Burma (2007) and Iran (2009) as exemplars—but development of state instruments to control Internet-delivered discourse is a fairly new development. While it is easy to veer towards hyperbolic thinking on the political impact of the Internet and cyberspace, we have reached a point at which policy-makers should probably realize that these constructs have

1 Krasner, Stephen, "Abiding Sovereignty," *International Political Science Review*, 22, no. 3 (2000): 247.

2 Central Intelligence Agency, *World Fact Book*, https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html, accessed 18 January 2012.

3 While electricity to power computers may be delivered at 120 or 220 cycles, on direct or alternating current, the mechanism by which data are transmitted or received between them is now generally the same.

4 Consider national-level Internet content filtering activities of the People's Republic of China, for instance.

5 See Erik Brynjolfsson and Brian Kahin, *Understanding the Digital Economy* (Cambridge, MA: MIT Press, 2000) and Hal Varian, Joseph Farrell, and Carl Shapiro, *The Economics of Information Technology* (Cambridge, UK: Cambridge University Press, 2004).

very real ramifications for domestic and international political power. But what is cyber? Nye's definition is useful:

> Cyber is a prefix standing for computer and electromagnetic spectrum- related activities. The cyber domain includes the Internet of networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications. Cyberspace has a physical infrastructure layer that follows the economic laws of rival resources and the political laws of sovereign jurisdiction and control. This aspect of the Internet is not a traditional "commons." It also has a virtual or informational layer with increasing economic returns to scale and political practices that make jurisdictional control difficult.[6]

With cyber's rise in importance on policy agendas, questions arise about the nature of this highly unusual construct—a globally interconnected, interoperable digital communications system. Sovereign and commercial interests are evolving to cope with that rise. Cyber policymaking is shaped by those interests, as well as other norms. At a conference in 2009, a Chinese government official, Liu Zhengrong, deputy director general of the State Council Information Office's Internet Affairs Bureau, made several references to "Our Internet."[7] But of whose Internet was he speaking? China's? The world's? His prepared remarks left that somewhat unclear.[8]

What will become of this globally interconnected, man-made space, distinct from all others? Now, like the land, seas, air, and space, cyber is considered a domain of operations by the US Department of Defense. The world's major powers may carve up cyber in accordance with their own sovereign interests, rendering it balkanized.[9] Furthermore, the economic concerns of industries and their own capacity to mobilize government resources points to fissures in cyber's global interconnectedness. The debate on proposed US federal legislation contained within the Stop Online Piracy Act (SOPA) and the PROTECT IP Act (PIPA) appeared to request statute that would block off portions of cyber to protect some interests, but that could damage the business models of others while potentially damaging the capacity to maintain integrity of data delivery across the Internet. Despite the global standards for interconnectivity, the balkanization of cyber for political reasons over the next decade seems a real possibility and we must consider what that fragmentation will mean.

Division of global cyber spaces is a real possibility. Perhaps as with the Cold War, wherein the world was divided into ideological spheres—the West, the Eastern Bloc, and the rest—there could be formidable walls erected and a subnetting of cyber.

We can reflect on this. In 1990, there were few states (North Korea, Iraq and Iran, labeled an Axis of Evil a decade later) that did not want to sign on to the new world order. The world's governments would be democracies and their economies would be open markets. The Internet

6 Nye, Joseph, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Winter (2011): 19-20.

7 Liu Zhengrong, Plenary Session: How Do We Build International Cybersecurity Consensus? First Worldwide Cybersecurity Summit, Dallas, Texas, 4 May 2010.

8 This does not mean, however, that scholarship has not forged ahead on what the Internet means inside China. A useful survey of thinking on Internet life in China may be found in Guobin Yang, "Technology and Its Contents: Issues in the Study of the Chinese Internet," *The Journal of Asian Studies*, 70, no. 4 (2011): 1043-1050.

9 Furthermore, this balkanization can be either technological or political. On the former, take for instance the case of social network use, in particular Google's Orkut service. A fairly straightforward competitor to Facebook, Orkut is very popular in both Brazil and India, although apparently not for any significant political reason. It is so popular in Brazil that Google moved the division to Belo Horizonte in 2008. See David Ingenito, "Democracy in the Twenty-first Century: Social Media and Politics – Global Village or Cyber-Balkans," MA Thesis, University of Southern California, May 2011.

was an ancillary item (or perhaps the key one) in the great wave of globalization that washed across the planet in the 1990s. However, its development outpaced the capacity of sovereign entities to understand and utilize it. A growing fear of cyber stems from the political forces marshalled by social media and the damaging ramifications of cyber attack. It is this fear that drives the development of monitoring and security technologies as well as calls for policy at every level from local to global on protecting, preserving, and taming cyber.

WHAT ISSUE?

Over the last decade, a grand convergence has taken place in telecommunications. US telecom firms increasingly earn revenues not for completing telephone calls but rather for delivering data. Communication may take place across a multiplicity of formats—email, desktop videoconference, instant messenger, social network, microblog—so there exists no end of ways to pass messages and engage others, more or less in real time. This capacity for connection is important in the postindustrial economies.[10] Cyber is vitally important.[11] We can only ponder the cost of a significant global outage of our complex, Internet-enabled systems for a significant period of time. The good news is that, like most worst-case scenarios, a global outage is incredibly unlikely. Cyber appears resilient.

Despite this resilience, cyber is highly prone to disruption. The hacker group Anonymous cheerleads for its activist agenda deployed through cyber-attack tools downloaded from the Internet that require a relatively low degree of technical expertise to use. The easy-to-use attack tools require only targets with unremedied vulnerability. There is a world of unpatched, poorly configured, and badly designed IT that political hacktivists or cyber criminals can exploit to meet their objectives. The relatively unskilled are able to locate vulnerabilities in systems far more effectively than those charged with securing systems can.

Because of the relative ease in locating and exploiting vulnerability, a basic asymmetry of cyber comes into relief: the offence, the attacker, he who wishes to compromise a system, holds the upper hand.[12] Included in this asymmetry are systems in which significant resources are expended for the system's own protection.[13] This asymmetry extends beyond systems used merely to store, transmit, and process data. Now vulnerable are data processing systems employed to manage real physical machinery. *Prima facie* evidence of this issue appears to exist in the actions produced by the Stuxnet worm – we have been told that Stuxnet compromised the process control computer systems of the Iranian nuclear enrichment facility at Natanz some time in 2010.[14]

Although Stuxnet presents a redefining incident in the discourse on cyber (as do the

10 My graduate students in organizational information security place their own data connectivity somewhere below electricity and water in their hierarchy of needs, but generally above hot water.

11 We consider a world in which cyber systems include "those whose interruption could cause 'a mass casualty event'; 'the interruption of life-sustaining services'; 'mass evacuations'; or 'catastrophic economic damage to the United States.'" "A Cyber Risk to the US," *The Washington Post*, 13 February 2012, A16.

12 This issue is the topic of ongoing conversation between the author and the National Academies' Herbert Lin.

13 The compromise of US Central Command's secret-level computer network in the incident known as Buckshot Yankee by the Department of Defense offers additional reinforcement of this hypothesis. See William Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September-October (2010): 97-108.

14 John Markoff, "Malware Aimed at Iran Hit Five Sites, Report Says," *The New York Times*, 11 February 2011, 15.

social-media-mediated revolutions across the Arab world in 2011), it remains an outlier. General consensus is that problems in cyber are growing. Cyber crime—outright electronic theft and fraud—is an issue but it is also conflated with piracy of copyrighted works. Cyber espionage undertaken against states is a real concern, but those wagging the finger are often representatives of the very same governments that have developed sophisticated cyber espionage capabilities. There are plenty of items to be concerned about and that call for remedy and prescription, but the interaction between technology and policy communities appears disjointed and limited in efficacy.

WHY NO POLICY ANSWERS?

Any shortage of international agencies willing to take on cyber issues appears to have evaporated some time ago. In the last few years, international organizations (IOs) that report, analyze, or otherwise show interest in cyber have grown to include: the Organization for Security and Cooperation in Europe; the International Telecommunications Union; the Group of Twenty Finance Ministers and Central Bank Governors (G20); the World Intellectual Property Organization; the North Atlantic Treaty Organization; the European Union; and the Organization for Economic Cooperation and Development. It would appear that just about any IO has some cyber concern.

This breadth of interest has also mushroomed at the nation state level. The United States is perhaps the nation most deeply invested in cyber, practically as well as in its historiography. Cyber is largely an outgrowth of the interaction between Department of Defense-sponsored research and the Silicon Valley innovation ecosystem. In the 1990s, a decidedly *laissez-faire* approach to cyber was national policy. Taxation, regulation, and other state interventions were eschewed for the power of market forces and technical innovation. Capital poured into cyber and when too much capital fed it, the speculative bubble burst and money chased more tangible assets.

Today, however, government avoidance of involvement in dialog on cyber vulnerabilities and the drive for their remedy seems highly unlikely. And there is still a problem of knowing where technology may serve as an answer versus where policy is the appropriate response. We have a responsibility problem, to paraphrase Herbert Lin, of technologists and policy-makers not knowing who is in the position to lead. [15]

But in the United States at least, industry will ultimately lead. So while international discussion circulates around issues of censorship of political speech or the commensurability of cyber attack to use of physical military force (which adherents of DOD doctrine call kinetic), the latest set of cyber dividing lines in political discourse have been between business interests. In cyber, diplomacy between states is augmented or supplemented by state-firm diplomacy of multi-national corporations. [16]

For this reason it is unwise to engage in conjecture on some form of stewardship for cyberspace without considering the alignment of US business interests regarding the advance of the Stop Online Privacy Act (SOPA) and Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) through the US House of Representatives and

15 Herbert Lin, ISODARCO Conference, Andalo, Italy, 3 January 2012.

16 Jade Miller, "Soft Power and State-Firm Diplomacy: Congress and IT Corporate Activity in China," *International Studies Perspectives*, 10, no. 3 (August 2009): 285-302; 18.

Senate, respectively. Ostensibly forwarded as a new mechanism to protect intellectual property—which might mean anything from news articles and pop songs to engineering blueprints and corporate pricing strategy—SOPA and PIPA bitterly divided firms producing music and film, represented by the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) and major US Internet firms, principally Google, Facebook, and Twitter.[17]

There was an interesting meta-narrative in the nasty row between Hollywood and Silicon Valley. Pro-PIPA and SOPA rhetoric embraced the idea that the bills were designed to cope with the problem that US industrial competitiveness was being undercut by international scofflaws—that is, China— that engaged in sophisticated industrial espionage against leading technology firms, including the developers of advanced weapons systems. Criticism of the bills declared them wanton acts of censorship designed to remove large portions of the Internet from public view, much like the actions of the Chinese government to block speech deemed objectionable to the leadership of China's Communist Party.

In the end, the bills were pulled from a vote and China was roundly vilified by both sides. Coincidentally, the US government convinced its ally New Zealand to arrest online file repository Megaupload's founder Kim Dotcom (born Kim Schmitz in the Federal Republic of Germany) on 20 January 2012 under indictments filed in the Eastern District of Virginia a couple weeks earlier.[18] This was an important action. Setting aside the issue of government's capacity for protecting copyright of artistic works available in digital form, which, depending on opinion, is either an exercise in futility or a vital response to the greatest aggregate theft in the history of mankind, the Dotcom arrest showed that government could act to bring an arrest across international jurisdiction. On 27 November 2011, I suggested, in preference to the highly contentious legislation: "a simpler, better idea: Locate the funds to hire 50 additional FBI cyber agents able to serve as legal attachés in foreign countries, prosecuting the most egregious IP violators under current law."[19] Dotcom was called an egregious violator by the Department of Justice (DOJ) and handled accordingly, under existing law.

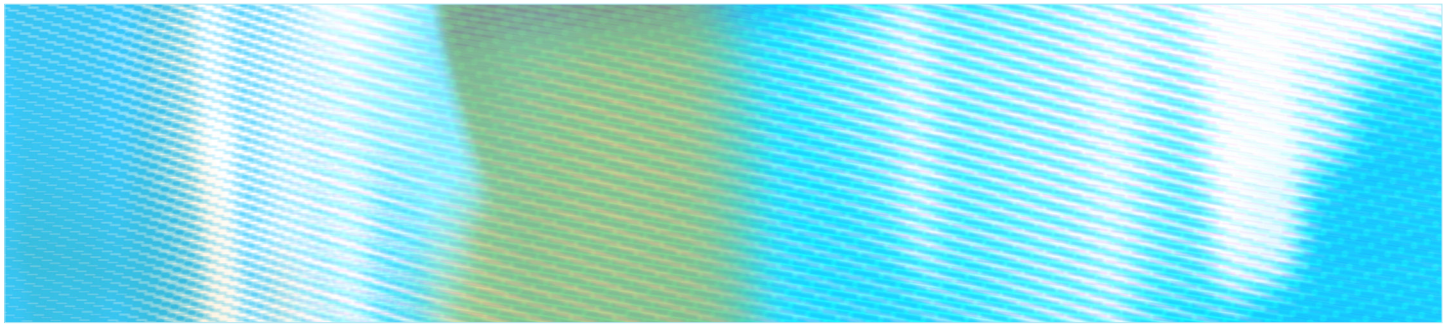
Naturally, some thought Dotcom was unfairly singled out, and that the charges against him carried an excessive set of potential penalties. But Dotcom was also convicted in his home country of both insider trading and embezzlement. The DOJ clearly picked a man to go after who could hardly be considered a pillar of business ethics, and it may well convict him in the same court that heard cases against Al Qaeda confederates Zacarias Moussaoui, Ahmed Omar Abu Ali, and John Walker Lindh.[20] We students of international cyber-politik are left to wonder if the defeat of PIPA and SOPA and the prosecution of Kim Dotcom were the best thing for the future of cyberspace. But this presumes that we know what is best for its future.

17 See Ryan Nakashima, "SOPA Protest Part of Growing Silicon Valley-Hollywood Beef," *San Jose Mercury News*, 18 January 2012, http://www.mercurynews.com/nation-world/ci_19767280

18 See "Justice Department Charges Leaders of Megaupload with Widespread Online Copyright Infringement," U.S. Department of Justice, 19 January 2012, http://www.justice.gov/opa/pr/2012/January/12-crm-074.html.

19 Chris Bronk, "The Wrong Way to Stop Online Piracy," *The Houston Chronicle*, 27 November 2011, B8.

20 As well as National Football League quarterback Michael Vick in the Bad Newz Kennels dog-fighting case.



NOTHING OLD, SOMETHING NEW?

Considering the issue of cyber and international power relations, Mary Joyce urges us to consider getting beyond cyberoptimism and -pessimism.[21] A recent panel, which included the Defense Advanced Research Projects Agency's Rand Waltzman and Ushahidi's Patrick Meier, brought home that message. Waltzman recalled Operation Valhalla, a firefight between a US Special Forces unit and a Jaish al-Mahdi (JaM) squad in which several of the Mahdi fighters were killed, and how

> roughly an hour after leaving the site of the firefight, someone had moved the bodies and removed the guns of the JaM fighters back at their compound so that it no longer looked as if they had fallen while firing weapons. They now looked as if they had fallen while at prayer. Someone had photographed the bodies in these new poses and the images had been uploaded to the web, along with a press release explaining that American soldiers had entered a mosque and killed men peacefully at prayer.[22]

Waltzman found numerous cases for grave concern over how cyber could threaten the United States, its interests, and military forces, across a spectrum of doctrinal space from Information Operations to Computer Network Attack.

Meier, conversely, could recall the massive volunteer response of technologists and translators in the Boston area to build the Ushahidi Haiti Platform that the US Coast Guard and Marine Corps employed in their rapid response to the 12 January 2010 earthquake that struck Haiti.[23] Ushahidi's service, and not just the technology, overcame both linguistic and distance barriers to enable the actions of those directly involved in saving lives. To borrow from Mary Joyce, we see a dose of cyber-pessimism and one of cyber-optimism.[24]

This range of views reminds us of prior liberalist and realist thinking about cyber and how international discourse is constructed around its politics.[25] We will likely see the development of international institutions or regimes to enforce standards and norms in areas that, to some degree, overlap. To break apart the issue set into manageable pieces, we may want to consider three issue areas: technical, information, and security. While this represents a simplification, perhaps the trio I outline here is a heuristic worth considering.

21 Mary Joyce, personal correspondence, 13 July 2011.

22 Cori Dauber, "The Truth Is Out There: Responding to Insurgent Disinformation and Deception Operations," *Military Review*, January-February (2009): 13-14.

23 Nathan Morrow, Nancy Mock, Adam Papendieck, and Nicholas Kocmich, *Independent Evaluation of the Ushahidi Haiti Project*, Development Information Systems International, 8 April 2011.

24 Mary Joyce, personal correspondence, 13 July 2011.

25 For discussion of this, see Mary McEvoy Manjikian, "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik," *International Studies Quarterly* 54 (2010): 381-401.

On *technical issues*, there are clearly defined organizations and gatherings that consider how the international connectivity of networks, including the Internet, should be undertaken. The Internet Engineering Task Force (IETF) has, since its inception in 1986, engaged in consensus-building efforts to establish the technical agreements that become standards and protocols, the building blocks of interconnectivity. IETF approaches issues by Request for Comment (RFC), and those comments become the work product of Working Groups (WG). In managing the progress of a WG, its chair is reminded, "that the overall purpose of the group is to make progress towards reaching a rough consensus in realizing the working group's goals and objectives."[26] But, generally speaking, IETF activity aims to hammer out technical agreement, something that may be akin to the management of a guild's activities.[27]

Information issues are far more complicated with regard to governance. While a relatively small set of actors may find rough consensus for packet delivery standards, the same is not true for the unfettered delivery of messages, ideas, and content. There are international laws and regimes on information control, but there is enormous breadth here and cyber, with its global reach, complicates matters enormously. Where IETF WGs are fairly homogenous sets of people, discourse on information issues takes place in a heterogeneous system. There are many stakeholders in freedom and control of information. The SOPA-PIPA debate was an international issue that involved US companies (on both sides), trade and professional associations, legislators, academics, think tanks, and ultimately, the president of the United States. Clearly, discourse on information issues takes place in a broader, more largely populated, heterogeneous space than discourse on technical issues.

And then there are *security issues*. Setting aside the securitization of the Internet and cyber, something that a number of scholars have handled well,[28] there is the problem that sovereign political actors now care a great deal more about cyber issues than they did just a few years ago. Anyone who has even briefly considered the Wikileaks State Department cable breach, Stuxnet, or the relationship of the Internet to the Arab Awakening should see how cyber is a rising issue. In his testimony to the US Senate Intelligence Committee, FBI director Robert Mueller acknowledged that stopping terrorists was still the top priority for his agency, but also that, "down the road, the cyber threat will be the number one threat to the country."[29] This insecurity will drive the allocation of resources and geopolitical strategy in the United States – a country representing "43 percent of the global total [of defense spending], six times its nearest rival China."[30] Such activity will securitize cyber more completely. Cyberwarfare will no doubt continue to develop, progressing from Estonia and Georgia through Stuxnet to some greater place.

26 RFC 2418, p. 10. RFC 2418 goes to some length to describe what rough consensus is, falling somewhere between majority agreement and 99 percent agreement.

27 Paul Twomey, Securing the Cyber Commons, remarks, 27 March 2011.

28 See Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53 (2009): 1155-1175.

29 J. Nicholas Hoover, "Cyber Attacks Becoming Top Terror Threat, FBI Says," *Information Week*, 1 February 2012, http://www.informationweek.com/news/government/security/232600046

30 "World Military Spending Reached $1.6 Trillion in 2010, Biggest Increase in South America, Fall in Europe According to New SIPRI Data," SIPRI, http://www.sipri.org/media/pressreleases/2011/milex.

A PATH FORWARD

So in assessing what policy should do about these three interrelated issue sets, it is necessary to evaluate the health of cyber. Is cyber sick? Will global digital interconnection end? Are the salad days of the Internet behind us? To even begin to formulate answers for those questions, we must accept the newness of all that we lump together as cyber, from cell-phone merchants in West Africa to integrated information warfare campaigns. Cyber is huge, deep, and vast – in its broadest interpretations it encompasses all data, both transmission and at rest, that has ever been digitized. Its enormity is overwhelming and growing all the while, although in the data deluge a ratio of signal to noise would probably skew mostly to noise (and many, many copies of items that are similar or the same). Nonetheless, there are questions that policy-makers need to answer now. Unfortunately, there is a divergence of answers to those questions and even a divergence in questions and facts.[31]

There are many questions we should consider when we assess cyber's health. Each of them requires careful examination by scholars and practitioners of both information technology and public policy. There is a need to see these questions through the more narrow lens of those who are concerned with cyber security as well as the wider one held by students of information politics. This is why sorting out cyber is difficult.

There remain many unknowns in cyber, and theories of international relations and foreign policy are a long way from providing a satisfying understanding of them. A metapolitical philosophy of cyber and politics would be a desirable end.[32] But ends are not what we have in store in this rapidly developing area of human interaction. Policy guidance will likely remain highly tactical and inserted where time permits. The bigger issues, such as when disagreement or even conflict in cyber may necessitate a martial response involving the use of force, will be debated and likely sorted out only after the fact.

31 According to David Weinberger's recent reflection on the creation of facts supporting arguments on almost any viewpoint, in this age of petabytes and petabytes of information published to the web, we may even be entitled to our own facts. (David Weinberger, closing keynote address, Tech@State: Real-Time Awareness, George Washington University, 3 February 2012.

32 Perhaps through the intellectual process of interplay between understanding and explaining we may see the interdependent variables of cyber and politics. See Martin Hollis and Steve Smith, *Explaining and Understanding International Relations* (Oxford UK: Oxford University Press, 1990).

Ultimately, the governance problem for cyber involves connecting the right actors with one another at the right time to produce the best desired result for the cyber ecosystem as most now enjoy it. Of course it would be naïve to assume that there are not interests — sovereign, corporate, or issue-specific — that will come into conflict with one another. What will likely be needed is a deepening of institutions to cope with these issues as they globalize. The Internet Governance Forum (IGF) is such an institution, though it carries with it the legacy of debates on cyberspace, particularly on IT and development/digital divide issues. Others will be involved, covering everything from telecommunications and radio spectrum issues to collective security arrangements and global trade regimes. These institutions will serve even more deeply as a *governance switchboard*, making the connection between the heterogeneous actors for whom cyber matters, when it is needed. There won't be one IO for cyber, but rather a set of them interacting with one another.

A decade ago, with the collapse of the "dot.com" bubble, we learned that not all political and economic outcomes regarding cyber would be pareto-optimal. Today, we must consider whether cyber is becoming zero-sum in nature, pure winners and losers. Because of the continuing march of cyber innovation—in power relationships, technological development, and social interaction—it is likely that cyber's future is somewhere between these two theoretical poles. In cyber, finite resources such as bandwidth, computing cycles, and well-educated computer engineers, will comingle with the products of crowd sourcing and the confounding economics of Coase's Penguin.[33]

Grand failure in cyber has yet to occur, technologically, socially, or economically, however, all sorts of little failures happen every day. We are left to wonder if cyber is headed to failure on a global scale or if it has developed enough mechanisms for self-correction, somehow akin to how *Wikipedia*'s editors are able to swiftly track down and eliminate vandalism that violates its emphases on neutrality and verification.[34] It will be these institutions that embody the spirit that will be cyber's most important steward. What remains to be seen is whether the model of peer-production scales to a concept of peer-governance. It is those institutions that can be lashed together to govern as peers that will give cyber the chance to endure as a global commons for the interchange of data, information, and knowledge.

Christopher Bronk is the Baker Institute fellow in information technology policy. He previously served as a career diplomat with the U.S. Department of State on assignments both overseas and in Washington, D.C. Since arriving at Rice, Bronk has divided his attention among a number of areas, including information security, technology for immigration management, broadband policy, Web 2.0 governance and the militarization of cyberspace. He teaches on the intersection of computing and politics in Rice's George R. Brown School of Engineering.

33 Yochai Benkler, "Coase's Penguin, or Linux and The Nature of the Firm," *The Yale Law Journal* 112, no. 3 (2002): 369-446.

34 For comparisons on peer governance issues and Wikipedia see Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2011).