Internet Governance and National Security

Panayotis A. Yannakogeorgos

The debate over network protocols illustrates how standards can be politics by other means.

—Janet Abbate, *Inventing the Internet* (1999)

The organizing ethos of the Internet founders was that of a boundless space enabling everyone to connect with everything, everywhere. This governing principle did not reflect laws or national borders. Indeed, everyone was equal. A brave new world emerged where the meek are powerful enough to challenge the strong. Perhaps the best articulation of these sentiments is found in "A Declaration of Independence of Cyberspace." Addressing world governments and corporations online, John Perry Barlow proclaimed, "Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here."[1] Romanticized anarchic visions of the Internet came to be synonymized with cyberspace writ large. The dynamics of stakeholders involved with the inputs and processes that govern this global telecommunications experiment were not taken into account by the utopian vision that came to frame the policy questions of the early twenty-first century. Juxtapose this view with that of some Internet stakeholders who view the project as a "rational regime of access and flow of information, acknowledging that the network is not some renewable natural resource but a man-made structure that exists only owing to decades of infrastructure building at great cost to great companies, entities that believe they ultimately are entitled to a say."[2]

Dr. Pano Yannakogeorgos is a research professor of cyber policy and global affairs at the Air Force Research Institute of Air University. His research interests include the intersection of cyberspace and global security, cyber norms, cyber arms control, violent nonstate actors, and Balkan and Eastern Mediterranean studies. He formerly held appointments as senior program coordinator at the Rutgers University Division of Global Affairs and was an adviser to the UN Security Council. He holds PhD and MS degrees in global affairs from Rutgers University and an ALB degree in philosophy from Harvard University.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Internet Governance and National Security	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Institute,Strategic Studies Quarterly,155 N. Twining St., Bldg. 693,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**24**	

The sole purpose of cyberspace is to create effects in the real world, and the US high-tech sector leads the world in innovating and developing hardware, software, and content services.[3] American companies provide technologies that allow more and better digital information to flow across borders, thereby enhancing socioeconomic development worldwide. When markets and Internet connections are open, America's information technology (IT) companies shape the world and prosper. Leveraging the benefits of the Internet cannot occur, however, if confidence in networked digital information and communications technologies is lacking. In cyberspace, security is the cornerstone of the confidence that leads to openness and prosperity. While the most potent manifestation of cyberspace, the Internet, works seamlessly, the protocols and standards that allow computers to interoperate are what have permitted this technological wonder to catalyze innovation and prosperity globally. The power of the current Internet governance model strengthens the global power of the American example and facilitates democratization and development abroad by permitting the free flow of information to create economic growth and global innovation.[4] Today, this Internet is at risk from infrastructure and protocol design, development, and standardization by corporate entities of nondemocratic states.

Cyber security discussions largely focus on the conflict created by headline-grabbing exploits of ad hoc hacker networks or nation-state-inspired corporate espionage.[5] Malicious actors add to the conflict and are indeed exploiting vulnerabilities in information systems. But there is a different side of cyber conflict that presents a perhaps graver national security challenge: that is the "friendly" side of cyber conquest, as Martin Libicki once termed it.[6] The friendly side of cyber conquest of the Internet entails dominance of the technical and public policy issues that govern how the Internet operates. Current US cyber security strategies do not adequately address the increasing activity of authoritarian states and their corporations within the technical bodies responsible for developing the protocols and standards on which current and next-generation digital networks function.

Internet governance can be defined as a wide field including infrastructure, standardization, legal, sociocultural, economic, and development issues. But the issues related to governance of critical Internet resources and their impact on US national security are often overlooked. Foreign efforts to alter the technical management of the Internet and the design of technical standards may undermine US national interests in the

long term. This article discusses the US national security policy context and presents the concept of friendly conquest and the multistakeholder format of Internet governance which allows for the free flow of information. There are many global challenges to the status quo, including the rise of alternative computer networks in cyberspace, that beg for recommendations to address those challenges.

Internet Governance and US National Cyber Strategy

Technical standards and protocols do not elicit the same attention as more visible threats to national cyber security. In a human capital and resource-constrained environment, attention has focused on crime, espionage, and other forms of cyber conflict rather than on the issues related to governance of critical Internet resources, development of technical standards, and design of new telecommunications equipment. In a domain that is already confusing to policy wonks, the complexity of Internet governance makes it even harder for policymakers to commit resources to a field that has no analogy in the physical world. In the nuclear age, there was no debate as to whether one could redesign the physical properties of uranium and apply them universally to eliminate the element's potential for weaponization. The underlying language of nuclear conflict was constrained by the laws of physics (e.g., nuclear fission, gravity). Physical limits in cyberspace exist as well by constraining information flows to the laws of physics—the wave-particle duality of radiation which, when modulated with bits, creates an information flow. However, the "logic" elements of cyber that permit information to flow across networks and appear within applications to create effects in the real world are bound only by the limits of human innovation. This affects the character of cyberspace. Its current form is free and open, but that does not necessarily mean it always will be. Understanding the strategic-level issues of Internet governance are thus just as critical as understanding the impact of vulnerabilities that attackers may exploit to cause incidents of national security concern. In the national security context, the technical management of the Internet matters because it may allow authoritarian states to exert power and influence over the underlying infrastructure. In the global security context, maintaining the values of free-flowing information within Internet governance bodies will continue to foster innovation and economic prosperity in both developed and developing states.

Several current national strategies articulate nationwide responses to cyber threats.[7] They tend to focus on catastrophic national security incidents rather than on the battles within the organizations that set technical standards or manage the day-to-day operation of the Internet. The White House does highlight the importance of current multistakeholder forums for design and standardization of the technical standards via "collaborative development of consensus-based international standards for information and communication technology . . . a key part of preserving openness and interoperability, growing our digital economies, and moving our societies forward."[8] Furthermore, the challenges we face in international standards-setting bodies are recognized in that "in designing the next generation of these systems, we must advance the common interest by supporting the soundest technical standards and governance structures, rather than those that will simply enhance national prestige or political control."[9] However, these issues are drowned out by more-sensational, hypothetical situations of a cyber doomsday.

Security demands that the language of the Internet—the underlying technical standards and protocols—continue to sustain free-flowing information. If "code is law" in cyberspace, as some posit,[10] then the standards and protocols are the fabric of cyber reality that give code meaning. In policy circles, cyberspace is already considered the "invisible domain." Technical standards and protocols are thus, "invisible" squared. However, these protocols define the character of the Internet and its underlying critical infrastructures. As noted elsewhere, "The underlying protocols to which software and hardware design conforms represent a more embedded and more invisible form of level architecture to constrain behavior, establish public policy. . . . [I]n this sense protocols have political agency—not a disembodied agency but one derived from protocol designers and implementers."[11] In the past it was the United States that led the world in the development of protocols and standards. As a result, the values of freedom were embedded in the Internet's design and character, which incubated innovation that continues to spur socioeconomic development globally.

Within the DoD context, a single, connected, open Internet is critical to assuring its missions by facilitating collaboration within the agency and with its mission partners. Today, the department lists in its *Strategy for Operating in Cyberspace* its concerns about "external threat actors, insider threats, supply chain vulnerabilities, and threats to DoD's operational ability."[12] Other elements from the DoD's *Information Enterprise Strategic*

Plan that articulate concerns with Internet governance and advocate for "DoD equities at international technical and governance meetings" should be added to the list.[13] However, the sheer political nature of the documents does not adequately address broader US foreign policy goals within global Internet governance bodies as much as intended. Thus, DoD computer scientists and engineers risk taking the backseat in an area where they once pioneered. Creating the Internet and maintaining the technical edge are two very different problems.

The Friendly Side of Cyber Conflict

Looming battles in Internet standards and governance bodies will determine the future character of the Internet. The advanced deployment of IPv6 in Russia and China and development of new standards by near-peer-competitor countries are creating new technical standards and deploying them into the global marketplace, thus enabling friendly cyber conflict.

Friendly conquest occurs when a noncore operator of a system enters into partnership with a core operator in exchange for access to a desired information system. Cyber theorist Martin Libicki notes,

> One who controls a system may let others access it so that they may enjoy its content, services and connections. With time, if such access is useful . . . users may find themselves not only growing dependent on it, but [also] deepening their dependence on it by adopting standards and protocols for their own systems and making investments in order to better use the content, services or connections they enjoy.[14]

The core partner in such a coalition emerges to dominate noncore members who have come to depend on the service offered, though not without some vulnerability to the core partner's network. Fears exist "that the full dependence that pervades one's internal systems may leave one open for manipulation. . . . The source of such vulnerability could range from one partner's general knowledge of how the infrastructure is secure, to privileged access to the infrastructure that can permit an attack to be bootstrapped more easily."[15]

Libicki operates with relational mechanisms to explain how coalitions leading to friendly conquest occur. Friendly conquest in cyberspace can be surmised as the willing participation of X in Y's information system. X willingly enters into a coalition with Y in cyberspace. Y's friendly

conquest of X occurs when X becomes dependent on Y's system. This is not to say that X merely entering the coalition will cause the conquest. X's perceived need for access to Y's cyberspace (or inability to construct its own) causes it to willingly enter into a coalition with Y. X adopts Y's standards and protocols making up the information system architecture of Y's cyberspace in a way that allows it to interoperate within X's cyberspace. X adopts Y's cyberspace architecture and thus the necessary condition for Y's friendly conquest. It is a facilitating condition for X's hostile conquest. X might begin to use the standards and protocols of Y's cyberspace as a model for its own cyberspace. Since Y is an expert in its own standards and protocols, X's modeling of these standards in its own systems is another vulnerability, which can facilitate X's hostile conquest by Y. X does not have to be a friend. It can be a neutral or a possible future enemy of Y. There is utility in Y opening its cyberspace to X only if Y sees some benefit to itself, although Libicki does argue that Y will open its cyberspace regardless. Once friendly conquest is accomplished, Libicki argues, it can facilitate hostile conquest in cyberspace. Friendly conquest of X by Y may thus facilitate hostile conquest in cyberspace conducted by Y against X.

The Internet and its underlying technical infrastructure is a potent manifestation of how the United States, as core operator of an information system, extended friendly dominance over allies and adversaries alike through creation of the technology and setting the rules for its operation. The Internet relies on products designed and operated by US-based entities such as the Domain Name System (DNS) and Internet Corporation for Assigned Names and Numbers (ICANN), Microsoft, and Cisco. Users around the world, such as Google and Facebook, have come to rely on services offered over this platform. The dominant position that US-based entities currently have is not permanent. The Estonian-developed Skype is indicative that services may be non-US in origin. Yet, even when an Internet-based service is created by foreign entities, most of the information flowing through the said application passes through hardware in the United States. When vulnerabilities are perceived, other nations may try to exit our information system to preserve their cyber sovereignty and expand their influence by attracting customers toward their own indigenous systems and away from the Internet.[16] Thus, our strategic advantage in cyberspace is not timeless and is being contested in varying degrees by near-peer competitors. Hence, we should understand their current

responses to US technological dominance to refine our cyber strategy within the context of friendly cyber conquest.

US Air Force doctrine recognizes one aspect of friendly conquest: supply-side infrastructure vulnerabilities. "Many of the COTS [commercial off the shelf] technologies (hardware and software) the Air Force purchases are developed, manufactured, or have components manufactured by foreign countries. These manufacturers, vendors, service providers, and developers can be influenced by adversaries to provide altered products that have built-in vulnerabilities, such as modified chips."[17] Friendly conquest goes beyond adversaries merely being able to infiltrate the supply chain and create backdoors on servers of national security significance before they enter the United States.[18] The threat also comes from the emergence of new technologies in which the United States is not the core operator but may become dependent. With the focus on malicious cyber attacks, not enough attention is being paid to the soft underbelly of the cyber world—the technologies and standards that have allowed cyberspace to emerge from the electromagnetic spectrum.

China is making a great leap forward in terms of sowing the seeds for global friendly conquest in cyberspace. As reported by the US-China Economic and Security Review Commission, "If current trends continue, China (combined with proxy interests) will effectively become the principal market driver in many sectors, including telecom, on the basis of consumption, production, and innovation."[19] US reliance on China as a manufacturer of computer chips and other information and communications technology (ICT) hardware has allowed viruses and backdoors in equipment used by US-based entities, including the military. Extraordinarily low-priced Chinese-made computer hardware is a lucrative buy in Asia and the developing world.[20] Furthermore, Chinese entities, such as Huawei, are on the leading edge of developing the standards of next-generation mobile 4G LTE networks.[21]

One example of how efforts at friendly conquest can backfire and make the United States vulnerable to cyber attack was demonstrated in Microsoft's experience with China. In 2003, China received access to the source code for Microsoft Windows in a partnership with Microsoft to cooperate on the discovery and resolution of Windows security issues. The China Information Technology Security Certification Center (CNITSEC) Source Code Review Lab, described as "the only national certification center in China to adopt the international GB/T 18336, the ISO 15408 standard

to test, evaluate and certify information security products, systems and Web services," was the focal point of this collaboration.[22] Undeterred by International Organization of Standards (ISO) criteria, and unanticipated by many experts in the field, Chinese computer scientists reverse-engineered the code. This allowed them to develop malicious code, including viruses, Trojan horses, and backdoors, that exploited software vulnerabilities in the operating system. These efforts resulted in the shutting down of the US Pacific Command Headquarters after a Chinese-based attack.[23] Chinese entities are also making great strides in developing core information systems upon which others will come to rely. Virtual reality (VR) technologies are one example of an emerging tool that could become as ubiquitous for social and commercial interactions as the Internet is today. Globally, people are increasingly using VR technology fused with the Internet to socially interact.[24] Experts have noted that

> any country that succeeds in dominating the VR market may also set the technical standards for the rest of the world, and may also own and operate the VR servers that give them unique access to information about future global financial transactions, transportation, shipping, and business communications that may rely on virtual worlds. . . .
>
> Global commerce is expected to "come to rely heavily on VR." Banking, transportation control, communications are all types of global commerce occurring in a virtual reality.[25]

While current strategies do address the supply-chain risks posed by foreign manufacturing, the trend of China taking the lead in the protocols that will come to underlie VR and other technologies, as well as standard setting within international bodies, is a challenge that current cyber strategies insufficiently address. This may be due in part to the cultural differences in the relations between US-headquartered multinational corporations (MNC) and the US government (USG) versus the MNCs in foreign countries that at times have very close relations to their own governments.

Multistakeholders and Internet Governance

Business entities such as multinational corporations contribute to the formation of policies regulating international communications formally within the International Telecommunications Union (ITU) and informally through the personal contributions of their employees within the ICANN, the Internet Engineering Task Force (IETF), and other organizations.

Within the United States, telecommunications service providers (dating back to the era of electrical telegraph systems) were never part of a state-owned monopoly. This was not the case in the rest of the world.[26] British Telecom and Deutche Telekom, for example, were state-owned entities before being privatized in the 1990s. Granted, although there is no direct state control within the United States, telecommunications companies are regulated by the state. In international telecommunications negotiations, a state and its ICT firms have a symbiotic relationship.[27] This has been the case since the International Telegraph Union, predecessor of the International Telecommunications Union, began meeting in the mid nineteenth century to regulate telegraphy policies.[28] Thus, the view in the developing world is that "at present, it is . . . U.S. law which applies globally by default as most monopoly Internet companies are U.S.-based."[29]

If trade is a political activity, then firms are political actors. States can utilize firms to distribute or reward power to meet their own political objectives.[30] Since states and firms both cause effects on the behavior of the other, a dynamic bidirectional interaction exists between the state and the MNC.

Important policy tools that affect the behavior of MNCs include export controls, protectionism, and strategic trade policy. Export controls tend to have a political purpose since, as one expert notes, "they are designed to prevent rival states from gaining access to key resources and technologies," or to punish a state.[31] Firms manufacturing strategic goods rely on governments to adopt trade policies that will support the firm's competitive stance in the global market,[32] but states do place restrictions on what may be exported, even if it is to the detriment of a firm's competitiveness in foreign markets.[33] In the United States, the federal government lost the so-called encryption wars of the 1990s, when private industry protested policies prohibiting the export of strong encryption software for strategic reasons.[34]

In an effort to prevent criminals from communicating using unbreakable codes, some firms implement law enforcement intercept (LEI) mechanisms so national security agencies can monitor suspected criminal and terrorist communications.[35] US firms and persons associated with them, who develop, maintain, and revise the core standards and technological infrastructures, are stigmatized by such allegations which depict a rogue national security apparatus and private sector in collusion capturing all of the world's data. This does not reflect the fact that, unlike in authoritarian states, careful compliance with US laws designed to protect user privacy maintains a separation between government and the private sector.[36] Media

preferring headline-grabbing allegations decrease global trust in the American private sector and validate the narratives that the Internet governance mechanisms must be internationalized. Thus, the close relationship between governments and firms in the area of strategic trade policy affects both how firms operate and how governments counteract the misuse of cyberspace.[37]

The global perception that the US government has de facto control of critical Internet resources is largely shaped by other nations' experiences of the close relationship between telecommunications companies and their national governments. Uniquely, the US government has never owned or operated any telecommunications companies. As the rest of the world shifted to the US privatized telecom model, prior experience of government control of the sector did not leave their cognitive balance. Today these experiences cast a shadow of suspicion over the special agreement between the ICANN and the US Department of Commerce.

Critical Internet Resources and Infrastructure

Technical management of the Domain Name System, invented by the DoD and governed by it in its formative years, was assumed by the Department of Commerce in 1998 and subsequently evolved into its current nongovernmental multistakeholder model.[38] The description here will not delve into the tactical- and operational-level functioning of each organization that has a role in Internet governance.[39] It will instead offer a brief recap of the underlying technology and the organizations that have a role in setting the standards which allow for technical functioning of the Internet. It is thus the purpose of this section to provide an account of Internet governance as a source of national security concern. With discussions focusing on malicious activities, there has been little consideration to the implications of the peaceful work of designing and maintaining the Internet and the implications these activities have on US interests.

Critical Internet resources (CIR) "in the context of Internet governance usually refers to Internet unique logical resources rather than physical infrastructural components or virtual resources not exclusive to the Internet. CIRs must provide a technical requirement of global uniqueness requiring some central coordination: Internet address, DNS, Autonomous System Numbers."[40] Unlike the popular conception of a limitless Internet, the underlying address space is limited. Indeed, IP address space has nearly run out. Foreseeing this Internet protocol, engineers developed IPv6, which among other improvements increased the total number of potential

IP addresses from 4,294,967,296 in IPv4 to 2^{128} in IPv6. It is recognized today that "deploying IPv6 is the only perennial way to ease pressure on the public IPv4 address pool."[41] As the world begins a transition from using IPv4 to IPv6 as the dominant communications protocol for the global Internet, the United States is not leading its deployment. Russia currently enjoys the greatest deployment in terms of market penetration, and China enjoys the greatest deployment in sheer numbers.[42] The consequences of delayed deployment are related to both Internet governance and the more traditional security threats. On the latter point the National Institute for Standards notes that the "prevention of unauthorized access to IPv6 networks will likely be more difficult in the early years of IPv6 deployments."[43] Thus, competitor nations that have more experience in national-level deployments of IPv6 have greater technical understanding of its real-world operations. The Air Force NIPRNet will not be entirely enabled for IPv6 until 2014. Even then, it has been noted that the plan is to use both IPv4 and IPv6 in parallel for the next 10–15 years.[44] As deployment of IPv6 as the backbone of the Internet continues, Russia and China may have the perceived legitimacy as IPv6 leads and take advantage of that opportunity to shift control of these scarce address spaces from the ICANN toward the control of an intergovernmental body, such as the United Nations.

The ICANN and the Current Internet Governance Structure

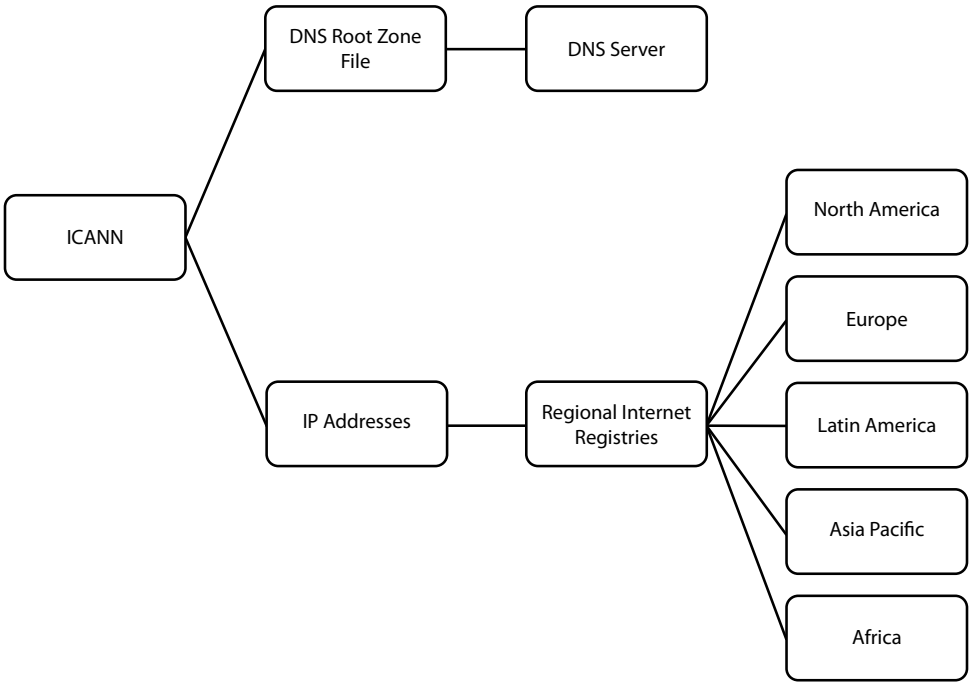
Because cyberspace is a man-made domain, infrastructure and standardization are critically important. Global bodies of computer scientists and engineers create the standards and rules on which the Internet—the most potent manifestation of cyberspace—operates. Indeed, many of these global bodies began as DISA, DARPA, or other USG programs that were privatized in the mid 1990s. Thus, the development of the next-generation Internet does not have the United States as the prime mover.[45] Instead, standards and processes are being developed by Russian, Chinese, and other foreign scientists and engineers. Today's machines speak a form of the English language to each other. If US scientific excellence continues its degenerative path, future networks may come to rely on machines speaking foreign languages. Furthermore, governance of the DNS and IP address allocation is being challenged to migrate from the current multistakeholder approach to an intergovernmental mechanism within the ITU. This is the friendly side of cyber conflict.

The DNS allows people to use Uniform Resource Locators (URL) to communicate with other machines on the Internet. Instead of having to type in the IP address of a website—a string of numbers—a person can type a natural language URL, such as www.af.mil, into a web browser to connect with the desired corresponding IP address. This makes the web user-friendly, and to the common user, might as well be the work of a wizard that allows information to be piped onto someone's computer. However, IP addresses are scarce, especially in IPv4. The processes for assigning scarce IP addresses and allowing the Internet to serve as a global platform are complex, both technically and, increasingly, politically.

The allocation of IPv4 address space to various registries is provided by ICANN via the Internet Assigned Numbers Authority (IANA).[46] Globally routable IP addresses reside in DNS databases on root zone databases that allow for the translation of URLs into IP addresses.[47] (see figure next page). The top-level domain names, such as .com or .org, are maintained and updated by the ICANN, which was once under the Department of Commerce (DoC). Now operating under a memorandum of understanding with the DoC, the ICANN continues to be the sole source of IP address allocation to specific DNSs and regional Internet registries to assure a uniform Internet experience for all. By governing and maintaining the DNS central root zone databases and backing them up on DNS servers worldwide, the ICANN assures that if a domain name is available, someone can buy it and link it with an IP address to create an online presence.[48]

Internet Engineering Task Force: Stewards of TCP/IP

Internationally standardized communications protocol stack, called Transmission Control Protocol and Internet Protocol (TCP/IP), allows for the flow of data packets and information across computer networks, including the Internet. TCP/IP is standardized by the International Organization of Standards for the Open Systems Interconnection (OSI) model as the basis of Internet networking. A brief description of how information is sent across networks is necessary to better understand the significance of TCP/IP. Data packets are the basic units of network traffic. They are the standard means of dividing information into smaller units when sending it over a network. A significant component of computer networks is the IP header, which contains information pertaining to the source and destination addresses. Machines require these strings of numbers to connect with other computers on the Internet or other networks.[49] All



networked hardware must have a valid IP address to function on a network. Data packets are recreated by the receiving machine based on information within a header of each packet that tells the receiving computer how to recreate information from the packet data. Without internationally standardized protocols such as TCP/IP, there would be no assurance that packets could be read by a receiving machine.[50]

The most esoteric of all critical Internet resources are the autonomous system numbers (ASN). These numbers are used by network providers at "peering points" to allow information to flow from, say, Verizon to ATT, among other uses. Border gateway protocols are one aspect of ASNs.

Internet policy debates have proven the ineffectualness of multilateralism as the United States strives to lead and others fail to follow. American technological innovation in the development and maintenance of the Internet's backbone is unquestioned. But global efforts to promote regulatory reform, such as including institutions of global governance like the ITU as entities responsible for overseeing the ICANN, are a tense political issue closely linked with the national cyber security concerns of democratic and autocratic regimes alike. In sum, American "leadership" as first among equals has led to a succession of dead ends. We are witnessing

countermoves by friends and competitors alike that may gain momentum during the 2012 World Conference on International Telecommunication.[51]

Global Challenges to the Status Quo

Global information flowing through open elements of cyberspace, such as the Internet, is regulated by national and regional bodies coordinating their policies internationally. Standards that have been created for elements of cyberspace have required lengthy processes at various bodies, such as the International Organization for Standardization and ITU, to assure sufficient technical and political cooperation among nation-states. While US-based entities have traditionally set the standards for Internet technology, China-based entities, such as the ZTE Corporation, are increasingly taking on roles within the ITU to draft important international standards that will shape the world's next-generation networks. This is not a recent development. As early as 2004, Chinese personnel working in senior ITU Telecommunication Standardization Sector positions began to discuss using the transition to IPv6 as a way to correct a perceived imbalance in address allocation between the United States and the developing world: "The early allocation of IPv4 addresses resulted in geographic imbalances and an excessive possession of the address space by early adopters. This situation was recognized and addressed by the Regional Internet Registries (RIR). . . . Some developing countries have raised issues regarding IP address allocation. It is important to ensure that similar concerns do not arise with respect to IPv6."[52] This is indicative of a desire by some states to perhaps shift the governance of IPv6 address allocation into a global institution such as the ITU.

From the perspective of maintaining US national interests, the current multistakeholder framework governing critical Internet resources continues to be a good mechanism for regulating the day-to-day technical operations of the Internet. However, momentum related to Internet governance within the United Nations is gaining within political forums. Led by Russian and Chinese initiatives, competitors and partners alike have been working toward internationalizing the Internet's technical governance. China and Russia, along with India, South Africa, and Brazil, have led initiatives against US dominance of the ICANN. These efforts have been in the works for nearly a decade.[53] As the DoD ARPANET experiment emerged to become a significant component of global socioeconomic development and governments increasingly came to realize its importance,

the momentum for internationalizing its backbone, the ICANN, became greater. Recall that these pushes for internationalization are due in part to the perception of US government control over ICANN via the DoC and NTIA, shaped by the history of special relationships between state telecommunication corporations existing in other countries.

The (Potential) Tyranny of the ITU over Critical Internet Resources

One battleground for debates over internationalizing the ICANN was observed during preparations for the World Summit for the Information Society (WSIS),[54] when significant opposition to the current Internet governance began to emerge.[55] For instance, in March 2004 during a UN-hosted Global Forum on Internet Governance.[56] Brazilian delegate Maria Luiza Viotti claimed that Internet governance needed reform, since it is not inclusive of developing countries and instead appears to be under the ownership of one group of countries or stakeholders.[57] Lyndall Shope-Mafole, chair of South Africa's National Commission, spoke on similar lines, arguing that the legitimacy of the ICANN's processes, rather than its functioning, was of most concern for developing countries.[58] Thus, after rigorous talks, delegates concluded on the basis of concerns from the developing world that the ICANN required further reform. Throughout the WSIS process, and continuing in other forums discussing Internet governance and global cyber security, Brazil has continued to be a vocal proponent against the US position in the ICANN. In 2011, India joined South Africa and Brazil in proposing to "operationalize the Tunis mandate" by

> bearing in mind the need for a transparent, democratic, and multilateral mechanism that enables all stakeholders to participate in their respective roles, to address the many cross-cutting international public policy issues that require attention and are not adequately addressed by current mechanisms and the need for enhanced cooperation to enable governments, on an equal footing, to carry out their roles and responsibilities in international public policy issues pertaining to the Internet, India proposes the establishment of a new institutional mechanism in the United Nations for global Internet related policies, to be called the United Nations Committee for Internet-Related Policies (CIRP).[59]

The CIRP idea has gained momentum within the developing world as a counter to the current technical management of the Internet. Indeed, it echoes closely Chinese concerns voiced by the China Organizational

Name Administration Center (CONAC) that "the U.S. government has the sovereign power to control the Internet resources. We therefore suggest making the computer security plan available for comment by all multistakeholders, for maintaining the security of cyber space is not a mission only for the U.S. government, and it cannot be accomplished by any single nation."[60]

From Russia, then prime minister Vladimir Putin stated,

> The International Telecommunication Union is one of the oldest international organisations; it's twice as old as the United Nations. Russia was one of its co-founders and intends to be an active member. We are thankful to you for the ideas that you have proposed for discussion. One of them is establishing international control over the Internet using the monitoring and supervisory capabilities of the International Telecommunication Union (ITU).[61]

Thus, the United States faces a significant challenge within the ITU from autocratic regimes leading the developing world to move control of critical Internet resources toward a multilateral body. The underlying danger is a shift away from an Internet whose defining characteristic is the free flow of information toward a model in which the political agendas of nondemocracies attempt to exert control over the flow of information. Hence, the United States and like-minded nations must surge diplomatically to ensure the character of the Internet remains free from the political control of a multilateral institution.

This diplomatic struggle for control of the Internet has also been occurring within various other forums, like the UN Commission on Science and Technology for Development. Suggestions being made on the issue include:

> Establishment of an ad hoc working group under the Commission on Science and Technology for Development with a view to the development of an institutional design and road map to enhance cooperation on Internet-related public policy issues with the support of the Secretary-General . . .
>
> Creation of a more permanent committee on international public policy issues pertaining to the Internet within the United Nations system, possibly modeled on the Committee on Information, Communications and Computer Policy of the Organization for Economic Cooperation and Development . . .
>
> And more concretely, global policy questions should be addressed by an entity with global representation, such as the United Nations, and regional questions by entities with regional representation, such as the Council of Europe . . . [and] the participation of relevant organizations in discussions on Internet governance at the quadrennial ITU Plenipotentiary Conference, and the public review process and Governmental Advisory Committee of ICANN. [62]

With the upcoming World Conference on Telecommunications in December 2012, such statements indicate that these ideas will resurface as part of the ITU effort to revise International Telecommunications Regulations (ITR) to include governance of next-generation critical Internet resources within the ITU's mandate and assume a greater role in Internet governance.[63]

Making Internet governance open to intergovernmental processes could put US national security at risk, given the potential for less-than-responsible state actors to take the current privatized laissez-faire approach to governing the Internet and have nation-states and their corporate entities take control of governing critical Internet resources. This would not ensure DoD equities are protected in an environment where critical decisions on underlying technical standards and Internet operation would be left to national governments that are competing with the United States.

Shadow "DNS" Rising

As described above, the critical Internet resources that allow for universally resolvable URLs and global Internet communications are possible due to the root system that is managed by the ICANN and protocols designed, developed, and debated within the IETF (among other organizations). Although this allows for a free and open Internet to function, the standards and protocols that the ICANN uses to maintain the domain name registries can be used by individuals, ad hoc networks, and nation-states to design and deploy an alternative DNS system that can either be independent of or "ride on top" of the Internet. A corporate LAN, such as ".company–name" for internal company use, is an example of the first. When a group wishes to ride over the global DNS root but incorporate its own pseudo top-level domain, core operators of the pseudo domains can use specific software resources to resolve domains that are globally accessible within their alternative DNS system. American audiences can experience what it is like to enter an alternative DNS universe via the Onion router (TOR) network. Downloading the Onion router package and navigating to websites one would prefer to visit anonymously (the typical use of TOR), one may point the TOR browser to websites on the ".onion" domain and mingle where the cyber underworld has started shifting the management of its business operations these days to avoid law enforcement and to add another layer of protection to their personas.[64]

Should significant usage of such shadow Internets occur, this could lead to the loss of confidence and utility of the Internet itself. The greatest risk

comes when nation-states develop and deploy their own alternate domain-naming systems for internal use, thereby separating themselves from the global Internet. This is different from controlling access points and actually develops country-level intranets that may or may not be connected to the global Internet.[65] The discussion herein focuses on Russia and China as far as their successes in deploying potentially new intranets for in-country use. Other countries, such as Iran, are following suit.

US involvement in *openly* promoting and organizing "digital activists" by issuing up to $30 million in grant funding to increase open access to the Internet, support digital activists, and push back against Internet repression wherever it occurs in the fight for free flows of information, generates international friction that is counterproductive to promoting international cooperation on cyber security issues."[66] The "Internet Freedom Agenda" is one example of this phenomenon.[67] Such technology effectively allows citizen-activists to hack past government digital sentries to spread forbidden information. Other tools allow activists to don digital disguises and organize themselves into social movements designed to topple regimes. The result has been the emergence of alternative national networks that essentially create alternate domain name systems for in-country use, allowing for censorship of content and stifling the productivity of the current Internet topology. China is one country that has implemented this on a national scale, and Iran is closely following suit.[68] Others are sure to follow these attempts. The rise of a splintered Internet will certainly change the character of the current Internet, with negative consequences for freedom and prosperity worldwide. Those who wish the Internet to remain free and open will benefit, and draw a sharp, moral contrast with those wishing to control the master switch. Thus, maintaining the current Internet governance model, while addressing legitimate concerns of friends and allies, will help assure the Internet continues to serve as a robust platform for human economic development.

Conclusion

Failure to pay attention to our vulnerabilities from Internet governance and friendly conquest may provide our adversaries with a strategic advantage in cyber conflict. Our own cyber-attack efforts will also become complicated as networks that are not based on protocols and standards developed by US-based entities are deployed by our competitors. To aid

how we conceive of cyberspace, as well as adjust to change within the cyber environment, there must be a broad dialogue on these issues. Despite the Internet's historic roots within the Department of Defense, there has not been a well-organized effort to influence the development of technical standards and policies affecting Internet governance. Currently, the DoD has remained in a reactive mode, coordinating and commenting on the various global norms and standards being considered within the USG processes related to Internet governance. Because of this approach, the DoD and the USAF may be perceived as not having the legal expertise or technical reputation in Internet governance. The DoD, and the US Air Force in particular, should exercise leadership and take a more active role in the development of information technology infrastructure standards as it once did. Furthermore, it should more carefully document its role and provide metrics on its participation and position with Internet governance bodies. The Air Force should play a leading role within the DoD and the whole of government by explicitly focusing on a broader concept of friendly conquest that implicitly exists in policies, strategies, and doctrines. The 2012 World Telecommunications Conference in December 2012 may be the right place to commence this effort.

As the hardware and software on which the global Internet is based evolve and non-US entities begin to invent new hardware, standards, and protocols, potentially taking market share away from US entities, the US position as core cyber infrastructure operator will diminish. The United States currently enjoys technological dominance through its position of developer and core provider of Internet services made possible by the ICANN and the top-level Domain Name System. But our national cyber security strategies do not adequately address threats that may stem from other countries developing the protocols, standards, and technologies on which the next generation of networks will be based. The Air Force has a key role to play given the wealth of technical excellence that resides within its community of scientists and engineers. It cannot act alone, however, and the DoD will need to focus some of its already limited cyber resources toward Internet governance. Not doing so risks allowing foreign-designed technical standards and protocols to form the backbone of next-generation IT and potentially puts DoD operations at risk by reversing what is now an Internet characterized by the free flow of information on which the DoD depends. The USAF remains the leading

US military service impacting cyberspace, and thus its actions or inactions in Internet governance debates matter. SSQ

Notes

1. John Perry Barlow, "A Declaration of Independence of Cyberspace," published online 8 February 1996.

2. Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (New York: Alfred A. Knopf, 2010), 290.

3. Granted, for the most part, manufacturing does not occur within the United States, which presents the national security risk of supply-chain vulnerabilities. This is a subset of friendly conquest but remains beyond the scope of the argument here.

4. American values are a core national interest. *National Security Strategy* (Washington: The White House, May 2010), 35.

5. See, for example, Bryan Krekel, Patton Adam, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Washington: US-China Economic and Security Review Commission, 27 March 2012); and Dmitri Alperovitch, *Revealed: Operation Shady RAT* (Santa Clara, CA: McAfee White Paper, 2011), http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

6. Martin Libicki, *Conquest in Cyberspace* (New York: Cambridge University Press, 2007).

7. The *National Strategy to Secure Cyberspace* (*NSSC*) (Washington: The White House, February 2003); John Rollins and Anna C. Henning, *Comprehensive National Cybersecurity Initiative* (*CNCI*) (Washington: Congressional Research Service, 10 March 2009; declassified in March 2010); the *International Strategy for Cyberspace* (Washington: The White House, May 2011); and the *Department of Defense Strategy for Operating in Cyberspace* (Washington: DoD, July 2011) are to date the leading relevant directives on cyber security. Although the White House completed a cyberspace policy review in 2009, the primary suggestions in the review amount to existing policy recommendations already in the *NSSC* and declassified *CNCI*. After the White House *Cyberspace Policy Review*, several initiatives were either launched or announced by departments and agencies of the US government. Declassification of the *CNCI* enabled the timely development of a framework for international partnerships consistent with a common cyber security policy. In 2011, the White House released the *International Strategy for Cyberspace*. Subtitled, *Prosperity, Security, and Openness in a Networked World*, the document falls short of providing the solutions necessary to live up to its name. The simple fact is, without security there can be no prosperity or openness.

8. *International Strategy for Cyberspace*, 12.

9. Ibid., 15.

10. Lawrence Lessing, "Code is Law," in *Code: And Other Laws of Cyberspace, Version 2.0* (New York: Basic Books, 2006), 11–10.

11. Laura DeNardis, *Protocol Politics: The Globalization of Internet Governance* (Cambridge: MIT Press 2009), 11.

12. Cyrus Farivar, "Security Researcher Unearths Plans for Iran's Halal Internet," *Ars Technica*, 17 April 2012, http://arstechnica.com/tech-policy/2012/04/iran-publishes-request-for-information-for-halal-internet-project/.

13. *Department of Defense Information Enterprise Strategic Plan 2010–2012* (Washington: DoD, May 2010), 10, http://dodcio.defense.gov/Portals/0/Documents/DodIESP-r16.pdf. Examples con-

tained in the plan include the Internet Engineering Task Force, ICANN, Internet Governance Forum, Réseaux IP Européens, and American Registry for Internet Numbers/North American Network Operators' Group.

14. Libicki, *Conquest in Cyberspace*, 12.

15. Ibid., 137.

16. The global positioning system (GPS) is one example where control of both the software and hardware is being contested. Although access to GPS is available without a fee for the basic service, friends and competitors alike have realized their dependence on this US system makes them vulnerable. Russia is modernizing its GPS system, and the European Union and China are developing independent GPS systems of their own. The long time cycle from intent to implementation of these new systems is due to the immense financial costs of deploying a space network. Cyber time cycles may be shorter, given the lower costs associated with deploying a national computer network compared with multiple high-tech satellites launched into space. For a more complete discussion of alternate GPS systems, see Lt Col Scott W. Beidleman, *GPS versus Galileo: Balancing for Position in Space* (Maxwell AFB, AL: Air University Press, 2006).

17. Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations*, 2010, 4.

18. Bruce Rayner, "Ferreting out the Fakes," *Electronic Engineering Times*, 15 August 2011, 24. See also John Markoff, "Computer Gear may Pose Trojan Horse Threat to Pentagon," *New York Times*, 10 May 2008, 12.

19. *The National Security Implication of Investments and Products from the People's Republic of China in the Telecommunications Sector*, U.S.-China Economic and Security Review Commission Staff Report, January 2011, 7, http://www.uscc.gov/RFP/2011/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf.

20. LCDR A. Anand, "Threats to India's Information Environment," in *Information Technology: The Future Warfare Weapon* (New Delhi: Ocean Books Pvt. Ltd., 2000), 56–62.

21. "Huawei Conducts World's First Commercial Network LTE Category 4 Trial," *Cellular News*, 9 May 2012, http://www.cellular-news.com/story/54329.php.

22. "China Information Technology Security Certification Center Source Code Review Lab Opened," *Microsoft News Center*, 26 September 2003, http://www.microsoft.com/presspass/press/2003/sep03/09-26gspchpr.mspx.

23. Barrington M. Barrett Jr., "Information Warfare: China's Response to U.S. Technological Advantages," *International Journal of Intelligence and Counterintelligence* 18, no. 4 (2005): 682–706.

24. Ibid.

25. Clay Wilson, *Avatars, Virtual Reality Technology, and the U.S. Military: Emerging Policy Issues* (Washington: Congressional Research Service, April 2008), 4, 12.

26. Anton A. Huurdeman, *The Worldwide History of Telecommunications* (Hoboken, NJ: John Wiley & Sons, 2003), 91–146, 153–85. See also Jill Hills, "International Market Structure and the ITU," in *Telecommunications and Empire* (Champaign: University of Illinois Press, 2007), 91–116.

27. Edward Comor, "Communication Technology and International Capitalism: The Case of DBS and US Foreign Policy," in *The Global Political Economy of Communication: Hegemony, Telecommunication and the Information Economy*, ed. Comor (New York: St Martin's Press, 1994), 83–102.

28. Jill Hills, *The Struggle for Control of Global Communications: The Formative Century* (Champaign: University of Illinois Press, 2002.)

29. Parminder Jeet Singh, "India's Proposal Will Help Take the Web out of U.S. Control," *Hindu Online*, 17 May 2012, http://www.thehindu.com/opinion/op-ed/article3426292.ece.

30. Debora L. Spar, "National Policies and Domestic Politics," in *The Oxford Handbook of International Business*, ed. Alan M. Rugman (New York: Oxford University Press, 2008), 207.

31. Ibid., 209.

32. Ibid., 212.

33. Standard export restrictions are meant to prevent access, whereas sanctions or embargoes aim to act as punitive measures. Sanctions appear to have the greatest effects on firms. For example, firms in State I which imports from State A will be at a loss if State A subjects State I to a sanctions regime. However, firms that export from State A to State I will also be at a loss since they will suffer from a decline in sales and face the possibility of ties being severed with State I in the long term. Thus, as Spar notes, MNCs must remain aware of political developments within the countries in which they operate so as to not find themselves prohibited from accessing a market due to sanctions. Thus, export controls are one mechanism that can affect the behavior of firms and economies.

34. Richard C. Barth and Clint N. Smith, "International Regulation of Encryption: Technology Will Drive Policy," in *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, eds. Brian Kahin and Charles Nesson (Cambridge: MIT Press 1998), 283–99.

35. James Bamford, *The Shadow Factor: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York: Doubleday, 2009). See also Claude Crépeau and Alain Slakmon, "Simple Backdoors for RSA Key Generation," in *CT-RSA'03: Proceedings of the 2003 RSA conference on the Cryptographers'* Track (Berlin: Springer-Verlag, 2003), 403–16; and Benjamin J. Romano, "Microsoft Device Helps Police Pluck Evidence from Cyberscene of Crime," *Seattle Times*, 29 April 2008, http://seattletimes.nwsource.com/html/microsoft/2004379751_msftlaw29.html.

36. See Foreign Intelligence Surveillance Act, Electronic Communications and Privacy Act, and Communications Assistance for Law Enforcement Act.

37. The crux of the argument made by those holding the opinion that states' sovereignty is at bay is that "the multinational corporation has broken free from its home economy and has become a powerful independent force determining both international and political affairs. [While] others [who] reject this argue that the multinational corporation remains a creature of its home economy." It follows that by the MNC breaking free from its home economy, the sovereignty and autonomy of states is compromised. Those that disagree with the above claim argue that the MNC has not become fully independent from the home country but remains "a creature of the home country." Robert Gilpin, *Global Political Economy: Understanding the International Economic Order* (Princeton, NJ: Princeton University Press, 2001), 278.

38. Department of Commerce, *Management of Internet Names and Addresses,* 63 *Fed. Reg.* 31741 (1998).

39. Harold Kwalwasser, "Internet Governance," in *Cyber Power and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington: NDU Press, 2009), 491–524.

40. DeNardis, *Protocol Politics*, 11.

41. See, for example, M. Ford et al., "Issues with IP Address Sharing," Internet Engineering Task Force, Request for Comments: 6269, June 2011, http://www.hjp.at/doc/rfc/rfc6269.html.

42. Ingrid Marson, "China launches largest IPv6 network," *CNET News*, 29 December 2004, http://news.cnet.com/China-launches-largest-IPv6-network/2100-1025_3-5506914.html.

43. Sheila Frankel et al., *Guidelines for the Secure Deployment of IPv6* (Gaithersburg, MD: National Institute of Standards, December 2010).

44. Katherine Kebisek, "AFNIC prepares Air Force for IPv6 transition" Air Force Space Command, 4 April 2011, http://www.afspc.af.mil/news1/story.asp?id=123249968.

45. Indeed, one should recall that the World Wide Web, the commercial adaptation of the DARPAnet project, was a CERN (European Organization for Nuclear Research) initiative.

46. This agreement was renewed on 2 July 2012. See http://www.icann.org/en/news/announcements/announcement-2-09jul12-en.htm.

47. Robert E. Molyneux, *The Internet under the Hood: An Introduction to Network Technologies for Information Professionals* (Westport, CT: Libraries Unlimited, 2003), 86.

48. ICANN, "Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority," 1 March 2000, http://www.icann.org/en/general/ietf-icann-mou-01mar00.htm.

49. Elihu Zimet and Edward Skoudis, "A Graphical Introduction to the Structural Elements of Cyberspace," in *Cyber Power and National Security*, 91–112. See also Molyneux, *Internet under the Hood*, 85–86.

50. Molyneux, *Internet under the Hood*, 27.

51. The Internet governance debates have a history of about a decade and certainly will continue past 2012. The next phase of the World Summit for the Information Society will occur in 2015.

52. H. Zhao, "ITU and Internet Governance—Input to the 7th meeting of the ITU Council Working Group on WSIS, 12–14 December 2004," http:// www.itu.int/ITU-T/tsb-director/itut-wsis/files/zhao-netgov02.doc.

53. For a comprehensive discussion of the dynamics of Internet politics as they relate to the perceptions by foreign countries that ICANN control is a cyber security for all, see Panayotis A. Yannakogeorgos, "Cyberspace: The New Frontier and the Same Old Multilateralism," in *Global Norms, American Sponsorship, and the Emerging Pattern of World Politics*, ed. Simon Reich (New York: Palgrave, 2010).

54. The World Summit on the Information Society (WSIS) and its spin-off, the Internet Governance Forum (IGF), are the main venues where governments and all interested stakeholders debate the issues, determine the objectives, and determine principles surrounding the structure of the global information society. The first and second phases of the summit resulted in the *Geneva Declaration of Principles* and the *Tunis Plan of Action*, respectively.

55. The ITU is the main entity tasked with organizing the WSIS. The High-Level Summit Organizing Committee was formed to "coordinate the efforts of the United Nations family in the preparation, organization and holding of WSIS." It was made up of a representative of the UN secretary-general and the executive heads of relevant UN specialized agencies. Other UN entities were included as observers. The ITU secretary-general served as the chair of this committee. One of its important functions was to "ensure that the contributions of the actors participating in the various conferences were comprehensively merged with the contributions from preparatory committees and regional meetings in a consensus document that would serve as the basis for the *Declaration of Principles* and *Plan of Action* of the WSIS."

56. "UN ICT Task Force Global Forum on Internet Governance to be Held in March," UN press release, Paris, 13 February 2004, http://portal.unesco.org/ci/en/ev.php-URL_ID=14347&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html.

57. "Global Internet Governance System is Working But Needs to Be More Inclusive, UN Forum on Internet Governance Told," UN press release, 26 March 2004, http://www.un.org/News/Press/docs/2004/pi1568.doc.htm.

58. Ibid.

59. "Statement by Mr. Dushyant Singh, Member of Parliament, on Agenda Item 16—Information and Communication Technologies for Development, at the 66th Session of the United Nations General

Assembly on October 26, 2011," http://content.ibnlive.in.com/article/21-May-2012documents/full-text-indias-un-proposal-to-control-the-internet-259971-53.html.

60. Yang Yu, Chinese response to "Further Notice of Inquiry on the Internet Assigned Numbers Authority Functions," China Organizational Name Administration Center (CONAC), http://www.ntia.doc.gov/files/ntia/conac_response_to_fnoi.pdf. CONAC is a nonprofit organization established in 2008. With the authorization of the State Commission Office for Public Sector Reform (SCPSR) and the Ministry of Industry and Information Technology (MIIT), CONAC runs the registry for ".政务.cn" (Government Affairs) and ".公益.cn" (Public Interest). CONAC also actively participates in the global Internet community.

61. "Prime Minister Vladimir Putin meets with Secretary General of the International Telecommunication Union Hamadoun Toure," *Working Day*, 15 June 2011, http://premier.gov.ru/eng/events/news/15601/.

62. UN General Assembly, "Enhanced Cooperation on Public Policy Issues Pertaining to the Internet," Report of the Secretary-General, http://unctad.org/meetings/en/SessionalDocuments/a66d77_en.pdf.

63. Signed by 178 countries, the ITR is a global treaty applied around the world.

64. Disclaimer: This is for informational use only. Any action undertaken by the reader of this article on the .onion domain is at his/her own risk, and this author is not liable for any harm caused by or to the reader.

65. This is different from what Chris Demchak points to in "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 32–61, where the focus on sovereignty of the Internet is on access points of incoming Tier 1 ISP connections into the country and maintaining government control of those.

66. US Department of State, "Internet Freedom Fact Sheet," 15 February 2011, http://www.state.gov/r/pa/prs/ps/2011/02/156623.htm.

67. Spencer Ackerman, "Does Obama's 'Net Freedom Agenda' Hurt the U.S.?" *Wired*, 28 January 2011, http://www.wired.com/dangerroom/2011/01/does-obamas-internet-freedom-agenda-hurt-the-u-s-without-helping-dissidents/.

68. Ye Tian et al., "China's Internet: Topology Mapping and Geolocating," http://cis.poly.edu/~ratan/topologymappingchinainternetshort.pdf.