9 China and Global Internet Governance

A Tiger by the Tail

Milton L. Mueller

As of June 2010 the Chinese government claimed the country's number of "netizens," or Internet users, had increased to 430 million.[1] That very large number is only 32 percent of China's total population.[2] Already one of the biggest presences on the Internet, and with a long way to go yet, China and the Internet enjoy a complex and seemingly paradoxical relationship. Many Westerners have trouble making sense of the way China's socialist market economy (SME) combines heavy restrictions with vibrant growth, and globalized networking with an insistence on territorial sovereignty. Western observers have long abandoned the notion that the Internet was inherently uncontrollable and that its use would automatically overthrow dictatorships. They are now replacing that simplistic notion with an equally coarse inversion: the image of China as the constructor of an impregnable "Great Firewall," a place of omnipotent surveillance, a population susceptible to well-organized propaganda campaigns, and a source of pervasive and insidious cyber attacks and cyber espionage. It is a new Internet version of the Cold War.

The Internet in the People's Republic of China (PRC) strains and challenges the capacity of the Chinese Communist Party (CCP) to maintain control. And the fact that China needs to be linked to the external world, through the Internet as well as through trade, provides a double challenge. The international environment of Internet governance is freer, is private-sector based, and is more capitalistic than China's rulers would prefer. And, it is subject to U.S. hegemony. If one combines an analysis of the global politics of Internet governance with an understanding of the long-term status of China's reform process, one can understand better which factors facilitate and which place constraints on the party's ability to regulate the Internet. One can even, perhaps, understand how the further development of digital communications might contribute to a transformation of Chinese society.

This chapter outlines a general framework for understanding Internet politics and locating China within it. It then analyzes China's attempt to move against the grain of the current Internet governance regime, promoting sovereignty and intergovernmental institutions in opposition to the new, transnational, and private-sector-based

Internet governance institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Regional Internet Registries (RIRs). The next section describes various interactions and spillover effects, both intended and unintended, between China's attempt to maintain its Great Firewall and the globalized operations that characterize the Internet, focusing in particular on the domain name system (DNS) and routing, and cyber espionage. A concluding section places these issues in a more general discussion of the tensions inherent in the Chinese "socialist market economy."

The Four Quadrants of Internet Politics and China's Place in Them

In another work I have described the politics of Internet governance using a space defined by two axes.[3] This conceptual scheme is predicated on recognizing that the Internet does indeed create a novel form of politics around communication and information policy. The novelty comes from the Internet's transnational scope, its massively increased scale of interaction, its distribution of control, its capacity to facilitate new forms of collective action, and the emergence of new, nonstate-based governance institutions native to the Internet.

The horizontal axis pertains to the status of the territorial nation-state in the governance of the Internet and communications technology generally. The vertical axis identifies the level of hierarchical control one is willing to countenance in the solution of Internet governance problems. Together, these axes form a four-quadrant space, which provides a useful schema for analyzing and classifying the various ideologies and policy systems related to the Internet.

In figure 9.1, the horizontal or nation-state axis locates one's view of the appropriate polity. Those on the right side of this axis prefer the traditional territorial nation-state as the institutional basis for governing the Internet. At the rightmost extreme stand those who would subordinate the Internet to national sovereignty completely—in effect, negating global networking altogether in favor of a bounded, analog telephone-network-like regime. At the left extreme, Internet governance decisions would be made by a globalized polity where national borders, national sovereignty, and national identity play almost no role.

The vertical or networking-hierarchy axis juxtaposes free association (at the top) with command and control (at the bottom). This reflects the degree to which one believes the problems associated with Internet governance should be solved using coercive and hierarchical mechanisms or left to the looser forms of association and disassociation among Internet users and suppliers. At the top of this axis, the shape of Internet governance would be defined by looser forms of *networked governance*; at the bottom, governance emerges from adherence to rules enforced by an authority. Of course, what makes Internet governance especially interesting is that there is no

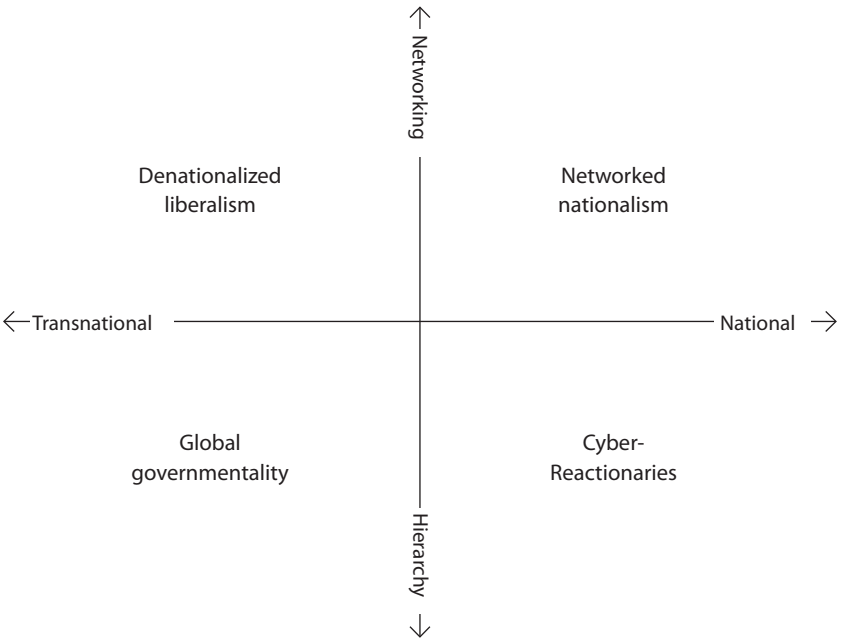


Figure 9.1
The quadrants of Internet politics.

universally recognized authority at the global level; therefore, advocates of hierarchy must also make choices regarding where they stand on the horizontal axis.

These two axes form a political space with four quadrants. In the lower-right quadrant, we have *cyber-conservatives* and outright *cyber-reactionaries*. In essence, these actors regret the rise of the Internet in most respects, and insofar as they tolerate its existence they strive to make it conform to the authority and parameters of the nation-state. Their intent is to realign control over the Internet's operational units and critical resources with the jurisdiction of the nation-state. Insofar as international policy is recognized as necessary, they believe that it should be handled by intergovernmental institutions and kept to the bare minimum required to protect or supplement domestic policy.

In the upper-right quadrant, which I call *networked nationalism*, the nation-state is still the dominant governance institution, but there is greater willingness to embrace the potential of networking and less of an attempt to impose territorial hierarchies on networked actors and network operations. National public policies and regulations are applied to actors within the territorial jurisdiction, but many loopholes and escape valves are left open because of transnational Internet access. States in this quadrant might cope with transnational problems through a mix of transgovernmental networks, delegation to private actors, or formal intergovernmental treaties, but international

institutions remain rooted in states, and any organically evolved Internet institutions would have to be recognized by and subordinated to states. This quadrant is characterized by an acute tension between the boundaries of the national polity and the (transnational) boundaries of networked activity.

The lower-left quadrant encompasses those who advocate *global governmentality*—namely, hierarchical control of the Internet by means of new institutions that transcend the nation-state. These new institutions are most likely to be private-sector based and created to advance business interests, though they could also be multistakeholder and public-private partnerships and even democratic for some version of democracy not rooted in 20th-century nations.

The upper-left quadrant, which I call *denationalized liberalism*, also supports a transnational institutional framework but is less hierarchical in its approach to the need for order. This quadrant combines economic and social liberalism; its adherents recognize individual network participants, not states or corporations, as the fundamental source of legitimate Internet governance and propose to create new institutions around them. Its adherents valorize freedom and propose to rely primarily on peer-production processes, networked governance, and competitive markets to handle the issues of Internet governance. Hierarchical interventions would be limited to the minimum required to secure basic protections against theft, fraud, and coercion.

Within this political space, China (along with Burma, Russia, and other postcommunist nations such as Vietnam) is unambiguously cyber-nationalist. It strives mightily to reorder the Internet by filtering content and by licensing and regulating the providers of Internet services in order to make them conform to national policy. Its philosophy is clear from its own 2010 White Paper:

> The Chinese government believes that the Internet is an important infrastructure facility for the nation. Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security.[4]

Along with the emphasis on sovereignty, equally strong support for hierarchical control exists. Both the telecommunication infrastructure and the services that run on top of it are subject to strict licensing and entry restrictions, as well as outright censorship and repression:

> No organization or individual may produce, duplicate, announce or disseminate information having the following contents: being against the cardinal principles set forth in the Constitution; endangering state security, divulging state secrets, subverting state power and jeopardizing national unification; damaging state honor and interests; instigating ethnic hatred or discrimination and jeopardizing ethnic unity; jeopardizing state religious policy, propagating heretical or superstitious ideas; spreading rumors, disrupting social order and stability; disseminating

obscenity, pornography, gambling, violence, brutality and terror or abetting crime; humiliating or slandering others, trespassing on the lawful rights and interests of others; and other contents forbidden by laws and administrative regulations. These regulations are the legal basis for the protection of Internet information security within the territory of the People's Republic of China. All Chinese citizens, foreign citizens, legal persons and other organizations within the territory of China must obey these provisions.[5]

As a logical extension of its cyber-nationalism, China steadfastly supports a traditional, sovereignty-based communications governance regime in the international arena. It prefers an international regime organized around treaty-based intergovernmental organizations that rely on one-country, one-vote distributions of power. When China uses the word "democratic" in this context, it means one country, one vote. Its point of reference for "democracy" is not the rights and interests of the individual citizen, but is equality among sovereign states: "China believes that UN [United Nations] should be given full scope in international Internet administration and supports the establishment of an authoritative and just international Internet administration organization under the UN system through democratic procedures on a worldwide scale. All countries have equal rights in participating in the administration of the fundamental international resources of the Internet."[6]

Both the domestic and international aspects of China's approach to the Internet underscore the inevitability of its attempt to create a bordered Internet subject to national policy. The Great Firewall of China (GFW) is but one aspect of this; more important than the filtering of external information are the licensing requirements, extensive state ownership, and entry controls that can be imposed upon domestic Internet intermediaries and service providers, as well as the growing identification and surveillance of users and potential for severe, arbitrary punishment that can be imposed on them domestically. This leads to extensive self-regulation and self-censorship.

All these points refer to the Chinese Communist Party's theory of how things *should* be—their preferred state of affairs. That preferred reality, however, is undercut by the realities of the Internet. As Wang Chen, the State Council's chief information officer, put it, "the Internet is a global open-information system." In a speech before the Chinese parliament, he recognized the fact that

> as long as our country's Internet is linked to the global Internet, there will be channels and means for all sorts of harmful foreign information to appear on our domestic Internet. As long as our Internet is open to the public, there will be channels and means for netizens to express all sorts of speech on the Internet. Judging from our country's social development, our country is currently in a period of social transformation, rapid development, and conspicuous contradictions. Unavoidably, actual contradictions and problems in our society are reported on the Internet. Judging from our country's Internet management practices, we are still in the process of exploration and improvement. Many weak links still exist in our work. These problems have weakened our ability to manage the Internet scientifically and effectively.[7]

In addition to those limitations on control, China is constrained by the need for economic development and productive exchanges with the rest of the world. Thus, in its experimentation with combinations of restriction and openness and its sensitivity to its economic interdependence with the developed world, China's approach to the Internet mirrors its strategic approach to openness to foreign investment and trade generally. With its aspiration to become a global leader in high technology, China simply cannot afford to turn its back on the Internet.

China's Predictable Clash with (and Adjustment to) the Current Internet Governance Regime

The current Internet governance regime clashes with China's preferences in two distinct ways. First, the legacy of denationalized liberalism associated with the Internet's early development still powerfully shapes the Internet's operations and the social, economic, and political norms associated with its use. Instead of traditional, intergovernmental institutions there are private-sector-based, transnational forms of governance and a widespread ethic of self-regulation and civil society support for Internet freedom. Second, the privileged role of the United States in the current Internet governance regime, especially its control over ICANN, rankles the Chinese. Although in many respects denationalized liberalism and U.S. preeminence are at odds with each other, it is not surprising that China sees them as related and mutually reinforcing. In China's state-centric view, Internet freedom and the U.S. doctrine of the "free flow of information" are merely tools that a hegemonic America uses to penetrate and subvert other states with its own worldviews and values. China's accusations that Hillary Clinton's "Internet freedom" initiatives are part of a calculated "information imperialism" flow logically from this perspective.[8] The Chinese view is given some credence, since U.S. "Internet freedom" initiatives are in fact rather selectively targeted at U.S. geopolitical rivals China and Iran, as opposed to other equally censorious countries that are allies of the United States.[9]

China and ICANN

To the Chinese state (in common with other cyber-nationalist and cyber-reactionary nation-states), ICANN is highly objectionable for two reasons: first, because of its status as a nonstate actor that supplants or competes with states in the exercise of policy-making and governance responsibilities; and second, because of its unilateral establishment by the United States and its contracts that make it beholden to the U.S. Department of Commerce. Initially, the Chinese also objected to ICANN because, as a private corporation free from intergovernmental diplomacy, the corporation allowed representatives of the government of Taiwan to participate openly and freely in ICANN

activities and sit on its Governmental Advisory Commmittee (GAC). ICANN did not observe the protocols regarding the name affixed to Taiwan and used various other means of treating it as an independent state. Thus, after some early engagement with ICANN, China ceased sending representatives to its meetings in 2001.

During the World Summit on the Information Society (WSIS) from 2002 to 2005, China joined in the attack on ICANN. It made clear its support for a takeover of its functions by an intergovernmental institution such as the International Telecommunication Union (ITU). Adding to these tensions, members of the Chinese-language technical community (not all of whom lived in or were citizens of the PRC) were also frustrated with the slow development of new technical standards enabling the DNS to represent Chinese and other non-Roman scripts. Internationalized Domain Names (IDNs) represented not only a business and political opportunity for the Chinese, but a potential threat as well. U.S. companies such as VeriSign were licensing IDN technology and could use it to enter the Chinese market. The market for registration of Chinese-language domain names is potentially a very large one. If the Chinese government and its favored state enterprises were not in control of the standards for representing Chinese characters in the DNS and if they had no direct participation in the policy processes within ICANN for adding top-level domain names (TLDs) to the DNS root, this opportunity might be threatened.

During the ICANN-China freeze period, China mounted a challenge to ICANN that was less visible but far more radical and significant than the conference diplomacy of WSIS. It created what was, in effect, an alternate DNS root for Chinese-character domain names. China's national alternative to ICANN's global DNS root used the same technical approach pioneered by competing root operator New.Net to ensure that the new domains were globally compatible.[10] Chinese characters would appear as top-level domains inside China. If one of these Chinese-character domains was queried from outside China, the uniquely Chinese names would be rendered compatible with the global Internet by having the name servers add the globally recognized ICANN country code top-level domain, .cn, to the end of them. China created three new top-level domains in this fashion: Zhong guo, Gong si, and Wang luo. These additions were done some time in 2003 but were not widely publicized, and if inquiries were made, they were downplayed as "experimental" by the Chinese. In 2006, however, as ICANN began to develop new policies for the addition of top-level domains, the online version of *People's Daily* openly acknowledged the existence of these new domains and claimed that "[Chinese] Internet users don't have to surf the Web via the servers under the management of the Internet Corporation for Assigned Names and Numbers (ICANN) of the United States."[11]

Due to these preemptive moves, and because of China's realization after WSIS that ICANN was not going to go away, China and ICANN reached a mutual accommodation sometime in 2009. At the June 2009 ICANN meeting, the PRC officially returned

to the GAC, sending a divisional director of the Ministry of Industry and Information Technology (MIIT) to represent it. ICANN also made concessions, agreeing to rename Taiwan as "Chinese Taipei" and (more substantively) to create a "fast track" for the recognition and creation of new "country code top level domains" (ccTLDs) in non-Roman scripts.[12] Unlike ICANN's new generic top-level domain program for ordinary businesses and organizations, these new "ccTLDs" did not have to wait two or three additional years while stringent policies and regulations governing their award and use were developed; nor did they have to pay six-figure application fees or recurring annual fees based on the number of registrations. Indeed, the whole concept of a "country code TLD" was based on an ISO standard assigning two-letter codes using the Roman alphabet to specific geographic territories. Since no such standard existed for the rest of the world's writing scripts, the characterization of these new top-level domains as "country codes" provided political cover for a land grab by national ccTLD monopolies. By giving countries such as China, Russia, and India a privileged and accelerated right to get new top-level domains representing their country names in native scripts, ICANN and the U.S. government were giving the world's states an economically valuable and politically powerful gift in order to keep them happy with the ICANN regime.

China and the Internet Governance Forum

When WSIS failed to bring about a major change in ICANN's status, China acceded to the creation of the Internet Governance Forum (IGF). The IGF is yet another new institution associated with the Internet that fails to conform to cyber-nationalist norms. Although nominally created under UN auspices, it is a multistakeholder environment that mixes governments, civil society, the Internet technical community, and business actors in nonbinding dialogue about Internet issues. All actors are afforded equal status. Within the IGF, China initially took a low profile. Its main accomplishment was to insist that the IGF directly grapple with the issue of U.S. unilateral control over critical Internet resources. On several occasions it has expressed sharp (and valid) criticism of efforts by the United States and its allies in the private sector to avoid confronting those issues in IGF meetings. At one point a frustrated China publicly expressed opposition to the renewal of the IGF after its initial five-year mandate expired because of its avoidance of the WSIS-related issues. That position was later moderated, and now seems to have been replaced with reliance on a longer-term war of attrition that attempts to make the IGF gradually become more intergovernmental and a standard part of the UN bureaucracy.

This war of attrition attained tangible success in late 2010. In the early days of the IGF, no one at the UN headquarters was paying much attention to the IGF or even to

the Internet. This situation has changed. China has taken the lead in shaping the institutional environment for the IGF at the UN. Chinese diplomat Sha Zukang, who represented China during WSIS, became the United Nations' undersecretary-general for economic and social affairs on July 1, 2007. From that platform he has made a series of moves designed to bring the IGF more under the control of the UN system and make it more intergovernmental in character. China has the support of many Arab states and the BRICs in this regard. (Brazil, Russia, India, and China make up the BRICs.) While business interests and the United States thought they were minimizing damage by making the Committee on Science and Technology for Development (CSTD), a near-dormant entity within the UN Economic and Social Council (ECOSOC), responsible for WSIS follow-up, they were later outmaneuvered. The UN resolution renewing IGF was conditioned on a review and "improvement" process that made it more intergovernmental. In setting the parameters of the improvement process, Undersecretary Sha, with the support of other cyber-nationalist states, minimized the role of civil society and business. He also reinstituted the old way of excluding non-state actors from speaking during parts of the public consultations.

These moves actually do more to exclude the United Nations from the broader currents of Internet governance than to assert UN control over Internet governance. Without full and equal-status participation of Internet businesses and users, the United Nations is unlikely to have much influence and the IGF will not be much of a forum. But the changes bring a halt to the multistakeholder innovations and reforms that came from WSIS.

China and the Regional Internet Registries

The Regional Internet Registries (RIRs) manage and set policy for Internet Protocol (IP) address resources. Like ICANN, the RIRs are private, nonprofit corporations that have transnational governance responsibilities. Although they are not under the direct contractual authority of the U.S. Commerce Department, they do rely on ICANN for the initial allocations of large address blocks, which they subdelegate to Internet service providers (ISPs) and organizations in their regions. China has consistently attempted to make IP addresses conform to the governmental, sovereigntist model. Led by the Chinese director of the ITU's Telecommunication Standardization Bureau, Houlin Zhao, it has backed efforts by the ITU to compete with the RIRs.[13] It also supported a more recent attempt by the ITU to propose a parallel system of IPv6 address allocation based on country Internet registries.[14] Within its region, it has acquired addresses through its own National Internet Registry (NIR) rather than allowing ISPs and companies to go directly to the IP addressing authority for its region, the Asia Pacific Network Information Centre (APNIC). The cyber-nationalist pattern is consistent here, too.

International Incidents

The Chinese Communist Party has more direct authority over the domestic institutional environment than it does over the international regime. It has used this authority to create a comprehensive system of blocking/censorship, public-opinion management, and intermediary responsibility that has come to be known colloquially as the Great Firewall of China. Even so, its attempt to maintain and enforce cybernationalism is challenged domestically by four tendencies: the need for Internet operations to be globally coordinated and compatible; the ability of domestic actors to grasp the communicative opportunities of the Internet; the greater transparency fostered by Internet communications; and China's need to maintain trade relationships with the rest of the world.

The China country profile in this volume covers the domestic situation in more detail. This chapter focuses instead on the way China's attempt to maintain cybernationalism has interacted or conflicted with the globalized nature of Internet operations and governance. It describes the way the Chinese state's attempt to tamper with the domain name system to support censorship "spilled out" into the rest of the world. It looks next at a routing misconfiguration incident that created a minipanic in the United States. Then it shows how cyber espionage efforts traced to China are also shaping global attitudes toward Internet governance.

Exporting the Great Firewall?

DNS root servers tell Internet users where to find the information needed to connect to other domains. In March 2010, Internet users outside China found that their access to popular Web sites such as Facebook, YouTube, and Twitter was impaired. The problem, which was known to affect users in Chile and California, was eventually traced to their use of root servers located in China.[15]

The origins of this story go back to the early days of ICANN, when U.S. control of the DNS was becoming a global political issue. Root servers are the starting point for the hierarchical resolution process that makes domain names globally unique and matches IP addresses to domains. Because of the Internet's U.S. origins, all but three of the world's 13 root servers were located in the United States; a few were run by the U.S. military. Many national leaders (assuming they were aware of the problem) viewed this as an unacceptable kind of dependency on a foreign power. Although many of the people who were concerned about this had no idea what a DNS root server actually does, they were quite sure that they wanted one in their country. And there were, in fact, legitimate technical reasons supporting a greater geographical diversification of the root server infrastructure, such as greater resiliency in the face of outages and reduced latency in response times.

A zero-sum solution to this problem would have required taking root servers away from the United States and moving them to other countries. Aside from being a non-starter politically, given U.S. power and the lack of any institutionalized process for designating and removing root server operators, such a measure had the potential to create adjustment and compatibility issues. Therefore, leading DNS experts developed and implemented a technical modification that allowed existing root servers to multiply themselves with "instances" elsewhere in the world.[16] This was a positive-sum solution that used some aspects of the "anycast" service to make an authoritative name-server operator provide access to a single-named server in multiple locations.

China was one of the first countries to set up "mirrored" or "anycasted" root servers. There are now instances of three different root servers located in Beijing. And due to routing agreements among ISPs, it is possible that root-level domain name queries coming from sources outside China might make use of those root server instances in China.

What makes this interdependency interesting is that China relies heavily on domain name blocking to implement the GFW. As a result, its name servers will modify or tamper with responses to queries about where to find the blocked domains. If someone lives outside China and, because of network topography, happens to query a root name server hosted in China, that person's queries will pass through the Great Firewall, potentially subjecting the person to the same censorship imposed on Chinese citizens. Apparently, China's version of the "I" root was not visible to the rest of the world. In early March 2010, however, it seems to have become visible.[17] As a result, Chinese censorship "spilled out" and affected a number of users outside of China. Despite some countermeasures taken by the main root server operators, the problem happened again in June. Like the incident described in the next section, the Chinese impact on the rest of the world's Internet was almost certainly unintentional.

The BGP "Hijack"

U.S.–China Internet relations were inflamed again in November 2010, when the U.S.–China Economic and Security Review Commission (USCESRC) issued its report to Congress.[18] Discussing what was probably an unintentional routing-prefix configuration error that took place in April, the USCESRC stated that "a state-owned Chinese telecommunications firm 'hijacked' massive volumes of Internet traffic. For about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed U.S. and other foreign Internet traffic to travel through Chinese servers."[19]

In technical jargon, this is a problem in the border gateway protocol (BGP) routing protocol, sometimes called "BGP hijacks" or more frequently known as "BGP leaks," in which an ISP announces a route it is not authorized to service and the route

announcement is propagated to other ISPs and begins to affect routing patterns around the world. Inaccurate or unauthorized BGP route announcements happen frequently and are a well-known problem. While the USCESRC report did not explicitly assert that the prefix leak was intentional, the report framed the event as an "interception of Internet traffic" rather than as a routing configuration error. Those hostile overtones were picked up and amplified by the U.S. mass media, which publicized the idea that China had diverted "15 percent of the Internet" to its own country. The "15 percent of the Internet" claim confused Internet traffic volume with Internet route announcements—a completely false equation. Internet technical experts quickly weighed in to correct the understanding of the situation. According to Arbor Networks' Craig Labovitz, "This hijack had limited impact on the Internet routing infrastructure—most of the Internet ignored the hijack for various technical reasons."[20] Labovitz wrote that far from diverting "massive amounts of the Internet's traffic," there was "no statistically significant increase for either [of the two Chinese Internet service providers]. While we did observe modest changes in traffic volumes for carriers within China, the BGP hijack had limited impact on traffic volumes to or from the rest of the world."[21]

Both the incident and the reaction to it underscore the global interdependencies created by the Internet and the dangerous tendency for interstate rivalries to inflame mundane operational problems into military and political tensions. Correctly interpreted, the April 2010 Chinese routing hijack had little if anything to do with China and its geopolitical rivalry with the United States, but instead should be viewed as a spur for instituting more secure routing protocols on the Internet. Greater routing security is something that would benefit both China and the United States—and proper implementation of such a goal would require cooperation between the United States and China especially.

Cyber Espionage and the Blurring Line between State and Nonstate Actors

As China becomes a powerful state on the global scene it will—like other powerful states before it—engage in power and spying games with its rivals. Just as traditional, "meatspace" (i.e., physical) forms of spying and infiltration provide governments with ways to disrupt their enemies' plans or obtain valuable information, so does Internet-based espionage. Evidence in the West suggests that China has been especially active and effective at using cybercrime tactics to monitor and disrupt its enemies.

In early 2009 the Information Warfare Monitor (IWM) released one of the first unclassified reports detailing the activities of a cyber espionage effort.[22] The network, dubbed GhostNet, appeared to have been controlled from commercial Internet accounts located on the island of Hainan, China. A year later, another report from the IWM and the Shadowserver Foundation uncovered more extensive evidence of a China-based computer espionage network targeting India: its diplomatic missions,

government departments, national security and defense groups, Indian academics, and journalists focused on China. The Office of the Tibetan Dalai Lama was also targeted.[23] Leaked State Department cables show that U.S. and German government agencies were becoming concerned about Chinese cyber espionage as early as 2006.[24]

The Google-China incident (covered in more detail in the China country profile in this volume) can be seen as a straightforward clash between China's domestic policy and Internet freedom in that it involved a transnational business founded on the free and indiscriminate dissemination of information demanded by users. It was that, but it was something more as well. Google's sudden questioning of its presence in China was triggered not by ongoing Chinese censorship but by a break-in to its corporate network that Google believed could be attributed to Chinese state-sponsored or state-directed actors. This break-in not only involved the theft of proprietary information but also seemed to target the e-mail accounts of human rights activists.

State Department cables released by Wikileaks provide support for the conclusion not only that China's government was involved in the break-ins, but also that China's government views the Internet in general and Google in particular as state-directed pieces that are being played in its geopolitical power competition with the United States:

> A well-placed contact claims that the Chinese government coordinated the recent intrusions of Google systems. According to our contact, the closely held operations were directed at the Politburo Standing Committee level. . . . Chinese concerns over the recent Google threat to take down the company's Chinese-language search engine google.cn over censorship and hacking allegations were focused on the service's growing popularity among Chinese Internet users and a perception that the USG and Google were working in concert.[25]

Ties between China's leadership and Google rival Baidu are also asserted in the cables. The current dialogue over Chinese cyber espionage may be overlooking the extent to which China is subject to the same tactics from other countries, especially the United States. The State Department cables, for example, warn darkly of "potential linkages of China's top companies with the PRC [state]" and claim that such links "illustrate the government's use of its 'private sector' in support of information warfare objectives."[26] Coming from the United States, it sounds very much like the policeman at Rick's casino in the movie *Casablanca* proclaiming that he is "shocked, shocked to discover that gambling is going on here." The massive U.S. military-industrial complex and the deep, long-term ties between Internet technical experts, cyber security firms, and Defense Department and the Department of Homeland Security's research funding are almost exactly the same as those described in threatening terms in the State Department cables.

An inherent feature of the nation-state system of governance is that concepts of order and security apply first and foremost in the domestic sovereign's jurisdiction. Different, negotiable standards apply to outsiders. Because China believes that it is

both necessary and justified to "manage" the information environment and control political activity, it makes sense that it would use cyber espionage to its fullest capacity to survey its international and domestic environment.

Ongoing Tensions between China's Sovereigntism and the Internet

To decode the paradox of the Chinese Internet we need to return to the dialogue within the international communist movement about the future of socialism. By the 1950s it was clear that true, thoroughgoing socialism—an economy devoid of private property, a price system, or markets—had failed economically and was simply unworkable. Leftist intellectuals contemplated two ways forward, one known as reform and the other as transformation. Reform did not mean, as many Westerners assume it does, a liberalization of economy and society that leads to convergence with the West. The communists referred to that path as *transformation*—the abandonment of communism and a move toward liberal democracy. A *reformed* communism would make socialism economically viable by permitting the existence of enough market forces and trade to deliver growth, while retaining the Leninist approach to centralized political control associated with classical communism. This is clearly the path that China has chosen. The whole point of China's reform process is to benefit from Western technology and from trade with the global market economy *without* converging into the West's liberal democratic governance model. Its opening and reform process was and is intended to deliver continued economic development without fundamental political change. Continued economic growth, they believe, makes political transformation unnecessary.

At least since the early 1990s, China's approach to information and communication technology has played a significant role in facilitating the achievement of these reform objectives. An early discourse among Chinese intellectuals about "informatization" set the stage for this. The CCP viewed information technology as the best way to scale up the control capabilities of the state to keep pace with its growth and greater wealth. In a typically pragmatic Chinese style, which has been described as "touching the stones to cross the river," the Chinese Communist Party has gone through repeated cycles of loosening control to foster development and growth, and then tightening restrictions to ensure that the party stays in control. The first step releases suppressed economic energy and generates growth; the second phase prunes the development so that it conforms to the parameters of the SME and does not threaten the stability and security of the political system.

An observation by the former Beijing bureau chief of the *Financial Times* dispels any notion that the economic development based on these reforms is inherently incompatible with party control:

> If you benchmark the Chinese Communist Party against a definitional checklist authored by Robert Service, the veteran historian of the Soviet Union, the similarities are remarkable. As with

communism in its heyday elsewhere, the party in China has eradicated or emasculated political rivals, eliminated the autonomy of the courts and media, restricted religion and civil society, denigrated rival versions of nationhood, centralized political power, established extensive networks of security police, and dispatched dissidents to labor camps. There is a good reason why the Chinese system is often described as "market-Leninism."[27]

Unfortunately, in the West there is a persistent refusal or inability to grasp and accept the meaning of the SME. Westerners, and especially American politicians and businesses, are constantly mistaking China's *reform* with *transformation*. As a result, they are repeatedly disappointed and angry with China's suppression of individual rights and its limited and fitful openings to foreign investment and free trade. United States policies that attempt to change China are usually based on the premise that the country's leaders are making false steps on the road to embracing liberal democratic norms and models. They are not. Zhao Ziyang and a few other Chinese leaders from the mid-1980s may have flirted with or embraced transformation, but the Tiananmen Square incident settled that issue decisively within China's party.[28] Since then, the CCP mainstream has reaffirmed the notion of the SME and has explicitly rejected convergence. One need not approve of this approach to accept its reality and form one's expectations based on it.

It would make sense, then, that the Chinese state's approach to information and communications technologies (ICTs) in general and the Internet in particular is neither to completely suppress it in order to preserve a brittle and unpopular regime, nor to provide the Internet-based economy and society free rein. It is a constant, iterative attempt to release productive forces and then corral them into supporting the continued control and dominance of the CCP. Rebecca MacKinnon has called this "networked authoritarianism,"[29] although I am not sure it is the best label. The term may attribute too much intentionality to China's approach. What is really going on is an improvised response to the contradictions of the socialist market economy. On one hand, the market economy part of the package thrives on open exchanges with foreigners and robust circulation of information, both of which deliver the economic development and growth needed for the CCP to maintain its legitimacy; the continued political grip of the CCP, on the other hand, requires limiting entry into the market for information services, constant monitoring and surveillance of communications, propaganda activities, repressive capabilities, and accurate targeting of political and social threats.

Note that the attempt to subject the Internet to hierarchical control relies in many respects on the unique capabilities of networked computers, whether it is the use of DNS blocking and deep packet inspection to filter Web and search-engine queries, the mobilization of armies of freelance propagandists to search for and intervene in public discourses critical of the government, the surreptitious use of cyber espionage, or the "identification and record-keeping" activities invoked by Wang Chen. In an information age, the label "networked authoritarianism" is practically redundant—if there is

to be authoritarianism on this scale, how can it *not* be networked? Still, China's online economy and innovative capacity is certainly stunted by these self-limiting applications of ICTs. While China's huge domestic economy makes the growth of major Internet companies inevitable, it is hard to imagine major service innovations or globally competitive online service providers emerging from this environment.

The oscillation between progress and control appears regularly across a number of different economic sectors, including China's approach to telecommunications sector reform.[30] In sum, the experience of China and the Internet is the latest episode in the familiar tale of Chinese reform, which recalls the parable of the man who caught a tiger by the tail. As the tiger gallops and struggles along, the man finds it more and more demanding to maintain his grip. But if he lets go, the tiger will surely turn and destroy him. Unlike the man in the parable, the CCP is, to some extent, strengthened by the tiger's energy—but the tiger keeps getting bigger and bigger. How long this cycle can go on is difficult to know. For those who seek transformation of communist China the trick is to conceptualize how this self-reinforcing cycle works and how it might break down. One thing seems certain: for other governments, especially the United States, neither external intervention nor subversion directed from outside is likely to work. The CCP thrives on exploitation of nationalism and by positioning itself as the people's defender against the humiliations and dominations of foreigners. If anything can make the tiger and the man hanging onto its tail work together in harmony it would be that process.

Notes

1. China Network Information Center, "Internet Fundamental Data," June 30, 2010, http://www.cnnic.cn/en/index/0O/index.htm, accessed January 5, 2011.

2. Ibid.; U.S. CIA, *The World Factbook*, https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html.

3. Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2010).

4. Information Office of the State Council of the People's Republic of China, chapter 5, "The Internet in China," June 8, 2010, http://www.gov.cn/english/2010-06/08/content_1622956.htm.

5. Ibid.

6. Information Office of the State Council of the People's Republic of China, chapter 6, "The Internet in China."

7. Wang Chen, "Development and Administration of Our Country's Internet," delivered on April 29, 2010, before the Standing Committee of the National People's Congress. Unofficial English translation is available at http://www.hrichina.org/public/contents/article?revision%5fid=175119&item%5fid=175084.

8. Christopher Bodeen, "China Slams Clinton's Internet Speech: 'Information Imperialism,'" Associated Press, January 22, 2010, http://www.huffingtonpost.com/2010/01/22/china-slams-clintons-inte_n_432691.html.

9. Sami ben Gharbia, "The Internet Freedom Fallacy and the Arab Digital Activism," Samibengharbia.com, September 17, 2010, http://samibengharbia.com/2010/09/17/the-internet-freedom-fallacy-and-the-arab-digital-activism.

10. For a good discussion of this, see the comments appended to Rebecca MacKinnon, "China's New Domain Names: Lost in Translation," CircleID, February 28, 2006, http://www.circleid.com/posts/chinas_new_domain_names_lost_in_translation/#1905. The blog itself understates the significance of the situation, but the comments on the post and the tests reported there clarify the situation.

11. "China Adds Top-Level Domain Names," *People's Daily* Online, February 28, 2006, http://english.people.com.cn/200602/28/eng20060228_246712.html.

12. A country code is a top-level domain based on the ISO-3166 standard of two-letter codes, such as .cn for China, .fr for France, or .br for Brazil. They were created in the mid-1980s as alternatives to the so-called generic top-level domains (.com, .net, .org, .mil) at the insistence of some non-U.S. Internet developers. Not wanting to put himself in the position of deciding who or what qualified as a "country," Internet pioneer Jon Postel found an existing ISO standard, originally developed for postal uses, which assigned unique two-letter codes to each territory. Most of these territories correspond to nations, but many (e.g., .io for Indian Ocean) did not.

13. Houlin Zhao, "ITU and Internet Governance," input to the seventh meeting of the ITU Council Working Group on WSIS, December 12–14, 2004, Geneva, 30 November 2004. In this WSIS contribution Zhao wrote, "in addition to the current arrangements for allocation of IPv6 address by the RIRs, one could reserve a portion of the large IPv6 space for country-based assignments, that is, assign a block to a country at no cost, and let the country itself manage this kind of address in IPv6."

14. Sureswaran Ramadass, *A Study on the IPv6 Address Allocation and Distribution Methods* (Geneva: International Telecommunication Union, 2009).

15. Earl Zmijewski, "Accidentally Importing Censorship," Renesys Blog, March 30, 2010, http://www.renesys.com/blog/2010/03/fouling-the-global-nest.shtml.

16. Tim Hardie, "Distributing Authoritative Name Servers via Shared Unicast Addresses," RFC 3258, April 2002.

17. Zmijewski, "Accidentally Importing Censorship."

18. U.S.–China Economic and Security Review Commission (USCESRC), *2010 Report to Congress of the U.S.–China Economic and Security Review Commission* at the 11th Congress, Second Session, November 2010.

19. U.S.–China Economic and Security Review Commission, Section 2, *2010 Report to Congress of the U.S.–China Economic and Security Review Commission*, November 2010, http://www.uscc.gov/annual_report/2010/annual_report_full_10.pdf.

20. Craig Labovitz, "China Hijacks 15% of Internet Traffic?" Arbor Networks Security to the Core Blog, November 19, 2010, http://asert.arbornetworks.com/2010/11/china-hijacks-15-of-internet-traffic.

21. Craig Labovitz, "Additional Discussion of the April China BGP Hijack Incident," Arbor Networks Security to the Core Blog, November 22, 2010, http://asert.arbornetworks.com/2010/11/additional-discussion-of-the-april-china-bgp-hijack-incident.

22. Information Warfare Monitor, *Tracking Ghostnet: Investigating a Cyber-espionage Network*, March 29, 2009, http://www.tracking-ghost.net.

23. Information Warfare Monitor and the Shadowserver Foundation, *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, April 6, 2010, http://shadows-in-the-cloud.net.

24. The German Federal Office for the Protection of the Constitution (BfV) delivered a briefing on its analysis of the cyber threat posed by the People's Republic of China (PRC), which appears to mirror conclusions drawn by the U.S. intelligence community. The BfV surmises that the intention of PRC actors is espionage, and the primary attack vector used in their malicious activity is socially engineered e-mail messages containing malware attachments and/or embedded links to hostile Web sites. From October 2006 to October 2007, 500 such e-mail operations were conducted against a wide range of German organizations, and the attacks appear to be increasing in scope and sophistication. See Wikileaks cable at "A Selection from the Cache of Diplomatic Dispatches," *New York Times*, November 28, 2010, http://www.nytimes.com/interactive/2010/11/28/world/20101128-cables-viewer.html#report/. Once on the site, click on "China" to get to the cable.

25. "US Embassy Cables: Google Hacking 'Directed by Chinese Politburo Itself,'" Latest China (The Guardian online China News), December 4, 2010, http://latestchina.com/article/?rid=24361.

26. "WikiLeaks Cables Reveal Fears over Chinese Cyber Warfare," Latest China (The Guardian online China News), December 4, 2010, http://latestchina.com/article/?rid=24367.

27. Richard McGregor, "Five Myths about the Chinese Communist Party—Market-Leninism Lives," *Foreign Policy* (online), January/February 2011, http://www.foreignpolicy.com/articles/2011/01/02/5_myths_about_the_chinese_communist_party.

28. Willy Wo-Lap Lam, *The Era of Zhao Ziyang: Power Struggle in China, 1986–88* (Hong Kong: A.B. Books and Stationery, 1989).

29. Rebecca MacKinnon, "China's Internet White Paper: Networked Authoritarianism in Action," RConversation Blog, June 15, 2010, http://rconversation.blogs.com/rconversation/2010/06/chinas-internet-white-paper-networked-authoritarianism.html.

30. Milton Mueller and Zixiang Tan, *China in the Information Age: Telecommunications and the Dilemmas of Reform* (Westport, CT: Praeger, 1996); and Irene S. Wu, *From Iron Fist to Invisible Hand: The Uneven Path of Telecommunications Reform in China* (Stanford, CA: Stanford University Press, 2009).

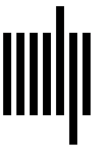
Access Contested

Security, Identity, and Resistance in Asian Cyberspace

Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain

Citation:

Access Contested: Security, Identity, and Resistance in Asian Cyberspace
Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain
DOI: 10.7551/mitpress/9780262016780.001.0001
ISBN (electronic): 9780262298919
Publisher: The MIT Press
Published: 2011



The MIT Press

The online edition of this work is available from IDRC and at http://www.access-contested.net.

International Development Research Centre
PO Box 8500, Ottawa, ON K1G 3H9, Canada
info@idrc.ca / www.idrc.ca <http://www.idrc.ca>
ISBN 978-1-55250-507-6 (IDRC e-book)

This book was set in Stone Sans and Stone Serif by Toppan Best-set Premedia Limited. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Access contested : security, identity, and resistance in Asian cyberspace / edited by Ronald Deibert . . . [et al.].
p. cm. — (Information revolution and global politics)
Includes bibliographical references and index.
ISBN 978-0-262-01678-0 (hardcover : alk. paper) — ISBN 978-0-262-51680-8 (pbk. : alk. paper)
1. Cyberspace—Government policy—Asia. 2. Computer security—Asia. 3. Computers—Access control—Asia. 4. Internet—Government policy—Asia. 5. Internet—Censorship—Asia. I. Deibert, Ronald.
HM851.A253 2011
303.48′33095—dc23

2011031273

10 9 8 7 6 5 4 3 2 1