China

China maintains one of the most pervasive and sophisticated regimes of Internet filtering and information control in the world. The community of Chinese Internet users continues to grow, while the state simultaneously increases its capacity to restrict content that might threaten social stability or state control through tight regulations on domestic media, delegated liability for online content providers, just-in-time filtering, and "cleanup" campaigns.

RESULTS AT A GLANCE

Filtering	No Evidence of Filtering	Suspected Filtering	Selective Filtering	Substantial Filtering	Pervasive Filtering
Political					•
Social				•	
Conflict and security					•
Internet tools				•	

OTHER FACTORS

	Low	Medium	High	Not Applicable
Transparency	•			
Consistency			•	

KEY INDICATORS	
GDP per capita, PPP (constant 2005 international dollars)	6,200
Life expectancy at birth, total (years)	73
Literacy rate, adult total (percent of people age 15+)	93.7
Human Ddevelopment Index (out of 169)	89
Rule of Law (out of 5)	2.2
Voice and Accountability (out of 5)	0.8
Democracy Index (out of 167)	136 (Authoritarian regime)
Digital Opportunity Index (out of 181)	77
Internet penetration rate (percentage of population)	28.9

Source by indicator: World Bank 2009, World Bank 2008a, World Bank 2008b, UNDP 2010, World Bank Worldwide Governance Indicators 2009, Economist Intelligence Unit 2010, ITU 2007, ITU 2009. See Introduction to the Country Profiles, pp. 222–223.

Background

The People's Republic of China (PRC) is a one-party state ruled by the Chinese Communist Party (CCP). Since the opening of its economy under the leadership of Deng Xiaoping in the 1980s, the country has undergone drastic changes. These changes are especially apparent in the information communication technology (ICT) sector, which has become a subject of considerable significance within PRC policy and discourse.[1] With the total number of Chinese netizens surpassing 450 million at the end of 2010, the Internet has become increasingly embedded in Chinese society and progressively more central to the flow of information within and across Chinese borders.[2]

Although recent and current administrations have emphasized the importance of Internet development, Chinese policymakers are also wary of the potentially crippling effects that these changes could have on the CCP's ability to contain sensitive or threatening information.[3] As changing dynamics in China's relationship with the international community present new opportunities for increased dialogue, the CCP has focused significant energy on developing new ways of maintaining close regulation of the information accessed and disseminated within the PRC.

Since 2008, several milestones in China's development, domestic politics, and foreign relations have presented new challenges to the PRC government, and authorities have responded by launching rigorous campaigns to contain communications, monitor and control citizens' activities, and outweigh public criticism through proactive counterinformation campaigns.

On March 10, 2008, the anniversary of the 1959 Tibetan Uprising, protests erupted in the Tibetan capital of Lhasa, calling for improved human rights conditions, religious freedom, and, in some cases, political independence.[4] Shortly thereafter, with the international community's eyes on China during the lead-up to the Beijing Olympics, unprecedented protests broke out among Tibetan communities throughout China and around the world.[5] The Chinese government responded by initiating violent crackdowns in the Tibet Autonomous Region, clamping down on domestic and foreign media, and systematically blocking online content pertaining to the incident.[6]

As the Olympics drew nearer, China faced increasing international pressure to lessen censorship and honor its commitment to allow foreign media to report freely during the games. The official policy on foreign media restrictions during the Olympics, issued in 2006, considerably loosened control over foreign journalists, allowing them to travel and conduct interviews throughout China without registration or the official consent of local authorities.[7] However, while these new regulations represented an unprecedented level of freedom for foreign journalists working in China, the government continued to exercise strict control over domestic media, tightly limiting the availability of unbiased Chinese-language news.[8] Furthermore, though the PRC government had initially agreed to provide unfiltered Internet access to journalists during the Olympics, this promise was significantly compromised and redefined as pertaining only to "games-related" Web sites.[9] Numerous political and human-rights-focused Web sites remained blocked throughout the games. Following the Olympics, the new regulations on foreign media reporting in China remained temporarily in place. However, events of the coming year led to a series of tightened restrictions and intensified controls.

The year 2009 was a critical one in the trajectory of China's Internet restrictions and censorship. In April 2009 the State Council Information Office issued its first "National Human Rights Action Plan of China," which, in addition to numerous other commitments, promised that "the state will take effective measures to develop the press and publications industry and ensure that all channels are unblocked to guarantee citizens' right to be heard."[10] However, throughout the year China continued to tighten censorship and increase control over public media and discussion, showing little potential for progress toward this goal. In preparation for numerous important milestones, including the 60th anniversary of the PRC's founding, the 50th anniversary of the Tibetan Uprising and retreat of the Dalai Lama to India (and one year since the 2008 protests in Tibet organized on the same date), the 20th anniversary of the Tiananmen Massacre, and the tenth anniversary of the Falun Gong spiritual movement being outlawed, the ruling party began the year carefully poised to tighten restrictions surrounding these sensitive dates.[11]

In July 2009, violent clashes broke out in Urumqi, the capital of the western province of Xinjiang. The protests, which appeared to have started peacefully, began as a

result of discontent among Uighur citizens following the murder of several Uighur workers in a Guangdong toy factory.[12] Though it is unclear what sparked the violence, conflict quickly erupted between Han and Uighur residents, leading to at least 197 deaths and more than 1,600 injuries.[13]

The Urumqi riots, China's most serious case of civil unrest in decades, led to severe and calculated clampdowns on local and national media and telecommunication networks. Unlike the case of the Tibetan protests of 2008, the Chinese government allowed—and even encouraged—foreign media coverage of the Xinjiang riots. However, journalists were confined to the city of Urumqi and permitted to cover violence instigated by Uighur citizens only. They were forbidden from reporting on the aftermath of the incidents, including the widespread and systematic interrogations and arrests of Uighurs, as well as the unexplained disappearance of dozens of detained suspects.[14] There were also cases of Chinese journalists being verbally and physically harassed while attempting to cover the news objectively.[15] Even more extreme, however, were the government's actions regarding Internet and telephone communications. The riots in Urumqi led immediately to drastic tightening of Internet censorship nationwide, including the blocking of Facebook, Twitter, and other social media sites, as well as a complete cutoff of all Internet and telephone access within the province of Xinjiang.[16]

Officials justified the Internet blocks as safety precautions, claiming, "We cut Internet connection in some areas of Urumqi in order to quench the riot quickly and prevent violence from spreading to other places."[17] They further asserted that the central government believed that World Uighur Congress Leader, Rebiya Kadeer, had "used the Internet and other means of communication to mastermind the riot," necessitating greater restrictions on the Internet to avoid further collaboration between separatist forces.[18] Although telephone communication and access to 31 state-sponsored Web sites were slowly restored, Xinjiang's Internet access remained effectively severed for ten months following the July 2009 riots.[19]

In January 2010, Google made a bold move by announcing it would no longer comply with the legal requirements of content filtering imposed on companies operating within the PRC.[20] Following a series of cyber attacks that targeted Google's infrastructure and the e-mail accounts of several Chinese human rights activists, Google publicly stated that it would seek to discuss the establishment of an unfiltered search engine in China, or else officially close down China-based Google.cn.[21] The attacks, which also hit a number of other Silicon Valley technology firms, led to responses from the central government that were largely dismissive of Google's accusations. Official reactions condemned the move as "financially driven," because of Google's inability to surpass Baidu.com as the number-one search engine in China.[22] Minister of the State Council Information Office Wang Chen defended China's censorship policies, maintaining that "properly guiding Internet opinion is a major measure for

protecting Internet information security,"[23] and showed no signs that the government would be willing to negotiate with Google.

In March 2010, after a series of strained negotiations between Google and Chinese authorities, the company finally made good on its threat to stop filtering content, stating that it would redirect all traffic from Google.cn to its unfiltered Chinese-language site, Google.com.hk, based in Hong Kong. Later that month, there were numerous reports that the government had blocked both Google.cn and Google.com.hk, though blockings appeared to be somewhat sporadic.[24] In June 2010, Google's senior vice president, corporate development officer, and chief legal officer, David Drummond, said, "It's clear from conversations we have had with Chinese government officials that they find the redirect unacceptable."[25] To renew its ICP license and continue serving Chinese audiences (while still refusing to censor search results), Google altered its approach to include a link to the Hong Kong site on the Google.cn home page, rather than automatically redirecting users. Google's ICP license was successfully renewed on June 30.

The overall effect of Google's decision to take a public stance on Internet censorship and cease compliance with PRC censorship policies has been widely discussed among both the Chinese and international communities. Whether or not the company's actions serve to improve the overall online environment and Internet freedom for Chinese citizens is not entirely clear. However, Google's actions have directed widespread international attention to the censorship practices of the PRC government; heightened global awareness of issues surrounding targeted malware attacks, Internet controls, and human rights; and placed the actions of the Chinese authorities and their manipulation of cyberspace in the international spotlight.

Chinese leaders consider China to be one of the largest developing countries in the world—one that is following its own model of development, which suits its own national conditions and is shaped by its unique history, social system, and culture. Chinese leaders place great emphasis on equality and mutual respect for sovereignty in foreign relations and are particularly sensitive to criticisms of the Chinese state and its handling of its internal affairs.

In 2010, U.S. Secretary of State Hillary Clinton criticized the country for threatening the free flow of information. In her January speech on Internet freedom, Clinton remarked, "On their own, new technologies do not take sides in the struggle for freedom and progress, but the United States does. We stand for a single Internet where all of humanity has equal access to knowledge and ideas. And we recognize that the world's information infrastructure will become what we and others make of it."[26]

In response, an op-ed in the state-run *Global Times* accused the United States of using the notion of an unrestricted Internet as a disguised imposition of its values on other cultures—in other words, information imperialism. The op-ed argued that "countries disadvantaged by the unequal and undemocratic information flow have to

protect their national interest, and take steps toward this. This is essential for their political stability as well as normal conduct of economic and social life. These facts about the difficulties of developing nations, though understood by politicians like Clinton, are not communicated to the people of Western countries. Instead, those politicians publicize and pursue their claims purely from a Western standpoint."[27] On the Chinese Foreign Ministry Web site, spokesperson Ma Zhaoxu officially stated, "We urge the US to respect facts and stop attacking China under the excuse of the so-called freedom of Internet."[28]

Internet in China

Like many of its neighbors in Asia, China has sought to balance the benefits that technological growth can bring to socioeconomic development with the potential risks to the government's control over media and information dissemination. Despite the rapid spread of Internet access throughout its vast population, China also has one of the largest and most sophisticated Internet filtering systems in the world.

Although access to the Internet in China is low relative to much of the world, it is growing rapidly and expanding into previously inaccessible regions. Despite a penetration rate of only 28.9 percent, the country's population means it has the most Internet users in the world.[29] The growth rate of China's user base has exceeded 20 percent for each year since 2006, reaching a peak of 53.3 percent in 2007.[30] Because the population has also grown since 2001, Internet users have increased more than tenfold—from 33 million to 388 million users by 2009.[31]

The majority of users access the Internet at home, although Internet cafés remain a means of access for an estimated one-third of users.[32] Broadband remains the most popular means of connectivity, with 103 million broadband users by 2009.[33]

Despite this large and growing population of users, Internet access is not evenly distributed. Most significant is the urban/rural divide, although this gap has closed in recent years as a result of initiatives to expand rural access.[34] As of January 2011, the China Internet Network Information Center reports that the number of urban Internet users was more than three times greater than the number of rural users.[35]

Other disparities in Internet access in China persist. The gender gap increased to more than 10 percent by 2010, with males making up 55.8 percent of users.[36] There is a significant age gap in access—almost 60 percent of users are under age 30, although the proportion of older users has increased.[37]

One area where China has seen tremendous growth and which offers the potential to alleviate the rural/urban imbalance is the mobile sector. Following the 2008 restructuring of China's telecom industry, the mobile services on offer expanded significantly. The number of mobile phones in use in China has multiplied almost tenfold in a decade, with an estimated one billion phones and a 73.5 percent penetration rate by

2010.[38] Mobile phones are a means of accessing the Internet for more than 300 million mobile users,[39] with over 10 percent of users accessing the Internet solely through their mobile phone.[40]

China's Internet users access a variety of resources online, including social networking, instant messaging, video sharing, and blogs. Search engines remain the primary use of the Internet, with 81.9 percent of users using these services.[41] Despite their dominance of the search-engine market throughout much of the world, Google is a distant second in China. China-based Baidu dominates the search-engine market with 75 percent market share compared to Google's 19 percent, particularly following Google's spat with CCP leadership over censorship and cyber attacks.[42] The use of instant messaging on mobile devices has grown, especially in regions with limited connectivity options.[43] Other services have also expanded. More than 3 million users use microblogging services,[44] and the country has the largest population of Voice over Internet Protocol (VoIP) users in the world.[45]

Access to the Internet in China is controlled by the Ministry of Industry and Information Technology (MIIT) and is provided by eight state-licensed Internet service providers (ISPs). The MIIT's mandate includes regulating telecommunications, Internet, and broadband as well as supervising IT development.[46] The telecommunications industry is dominated by a small group of state-owned companies. China Telecom Group is the largest telecommunications company in the country, controlling 70 percent of the local market.[47] China Telecom and the second-largest ISP, China Unicom, combined serve more than 20 percent of the world's total broadband users.[48] With six international backbone links, China's international bandwidth has grown consistently and now exceeds 1 million Mbps.[49]

A major restructuring of the telecom industry in China took place in 2008, with the six state-owned companies merged into three networks, greatly increasing the capacity of large firms to expand into wireless services.[50] By January 2009, the MIIT had issued 3G licenses to China Unicom and China Telecom using EVDO and WCDMA standards, as well as to China Mobile using the unproven TD-SCDMA standard unique to China.[51]

The expansion of Internet access has created a vibrant and dynamic online community throughout the country that has had a significant impact on public discourse, while also drawing the attention of government officials. Online discussion has frequently elevated local incidents to national prominence, with Web portals and forums dropping "information bombs" that have led to the tarnished reputations and dismissal of senior officials.[52] In an unpublished investigative report obtained by David Bandurski of the China Media Project, the vice president of People's Daily Online said that two-thirds of the few hundred secret internal reports that CCP top leaders give priority and action to are from the Internet Office of the State Council Information Office.[53]

The online community has broadened the capacity for collective action on a variety of fronts. Notable among these are so-called "human flesh search engines," which are massive online collective research projects. They have focused on conducting crowd-sourced investigations into a variety of incidents, from finding missing relatives to exposing corruption of government officials, although they have also strayed into questionable acts of vigilantism.[54] Discussion forums and blogs also offer new opportunities for organization and dissemination of information. Charter 08, a prodemocracy manifesto whose signatories included 2010 Nobel Peace Prize winner Liu Xiaobo, was circulated by e-mail and other means and had gathered 10,000 signatures by 2010.[55] However, these discussion forums are not the exclusive domain of those critical of government. The "Fifty Cent Party," named for the price individuals are rumored to be paid per post, is organized by the government to steer online discussion of sensitive topics.[56]

A variety of different Internet filtering mechanisms have been implemented. One such effort, the Green Dam Youth Escort project, was a far-reaching and ultimately unsuccessful attempt to implement filtering at the level of the user's computer. The project originally called for all new computers sold in China to come preinstalled with the Green Dam software to filter harmful online text and images to prevent them from being viewed by children.[57] However, ONI and Stop Badware researchers conducted an initial technical assessment of the software that found that Green Dam's filtering not only is ineffective at blocking pornographic content as a whole, but also includes unpredictable and disruptive blocking of political and religious content normally associated with the Great Firewall of China.[58] Following the findings, the MIIT delayed implementation and made installation of the software optional.[59] Despite the apparent failure of this initiative, a similar filtering package called Blue Dam was mandated for installation by all ISPs by September 2009.[60] This system included a graphic-filtering system, administration-management system, and Internet-behavior manager aimed at blocking content deemed inappropriate.[61]

Blog service providers also face requirements to ensure that there is no inappropriate content on their sites. These providers must install filters that prevent postings of thousands of keyword combinations, delete or conceal posts with sensitive comments, and cancel the accounts of bloggers deemed to have posted too many troublesome posts.[62] This discretion on the part of service providers has led to uneven patterns of filtering. A study of Chinese blog service providers demonstrated that there is substantial variation in censorship methods, the amount of content censored, and providers' transparency about deleting content.[63] Similar findings were reached in a Citizen Lab study of four popular search engines in China, which found significant variations in the level of transparency about filtering, actual content censored, and methods used, suggesting that there is no comprehensive system for determining censored content.[64]

China's dynamic system of Internet control is demonstrated by the rise of "just-in-time" filtering during key events. The 2009 violent protests between Uighur and Han residents of Urumqi saw Internet access in the Xinjiang autonomous region cut after videos and images of the protests spread online.[65] The 2010 awarding of the Nobel Peace Prize to activist Liu Xiaobo led to the blocking of sensitive keywords in search engines, blogging sites, and SMS text messages.[66] Notable anniversaries of sensitive events are a frequent target of filtering, including the 60th anniversary of the founding of the PRC,[67] the 20th anniversary of Tiananmen,[68] and the first anniversary of the 2008 Tibetan protests.[69] Such filtering has not been limited to domestic events—key Internet portals Sina.com and Netease.com blocked keyword searches of "Egypt" during that country's unrest in early 2011.[70]

The combination of rigorous technical filtering mechanisms and content providers' self-policing can often lead to self-censorship, with users unwilling to risk posting controversial content. Organizations like the China Internet Illegal Information Reporting Center (CIIRC), ostensibly a civil society organization, encourage the reporting of "illegal and harmful information" and send information about illegal content to the Ministry of Public Security.[71] As a result, commercial Web sites can elect to prevent the posting of controversial material rather than risk negative consequences later.[72] The pervasiveness of filtering at Internet cafés, a common method of access for many, means cafés are generally avoided for discussing sensitive topics online.[73] Further, many users have long assumed surveillance of communication tools like TOM-Skype,[74] thus discouraging their use.[75]

Legal and Regulatory Frameworks

The legal and regulatory frameworks that underpin China's Internet landscape are shaped by the PRC's desire to develop the Internet as a driver of the national economy while maintaining "state security and social harmony, state sovereignty and dignity, and the basic interests of the people."[76]

According to the June 2010 White Paper on Internet Policy, "The government has a basic policy regarding the Internet: active use, scientific development, law-based administration and ensured security. The Chinese government has from the outset abided by law-based administration of the Internet, and endeavored to create a healthy and harmonious Internet environment, and build an Internet that is more reliable, useful, and conducive to economic and social development."[77]

Regulations prohibit citizens from disseminating or accessing online content deemed subversive or harmful by the state. Laws and regulations that control online content distribute criminal and financial liability, licensing and registration requirements, and self-monitoring instructions to people at every stage of access—from the ISP to the Internet content provider to the end user.

Through Internet information service (IIS) providers and ISPs, the state regulates available online content and monitors Internet users. As laid out in Article 20 of the Measures for Managing Internet Information Services, IIS providers are directly responsible for content published on their services.[78] Specifically, IIS providers are prohibited from producing, reproducing, releasing, or disseminating information that falls under nine categories forbidden by the state, as laid out in Article 15 of the measures. Forbidden information ranges from content that undermines state security, social order, and national unity (such as information inciting ethnic hatred) to pornography. Internet information service providers who violate these measures or fail to monitor their Web sites and report violations can face fines, shutdown, criminal liability, and license revocation.[79] Commercial IIS providers must be licensed, while noncommercial IIS providers must report on their operations for official records. Electronic bulletin board services (including chat forums) are subject to similar regulations under the Rules on the Management of Internet Electronic Bulletin Services.[80]

Internet news information services have to abide by regulations laid out in the 2005 Provisions on the Administration of Internet News Information Services. The provision provides a complex regulatory scheme—only news originating from state-supervised news outlets can be posted online. Government-licensed and authorized news agencies are limited to covering specific subjects approved by the state, but they can at least conduct original reporting on "current events news information," defined as "reporting and commentary relating to politics, economics, military affairs, foreign affairs, and social and public affairs, as well as reporting and commentary relating to fast-breaking social events."[81] Web sites that are nongovernmental entities, or otherwise not licensed news agencies, are restricted from performing any journalistic function other than reprinting content from central news outlets or media under the direct control of provincial governments.[82]

Under Article 19 of this provision, there are 11 content categories that Internet news organizations are prohibited from posting or transmitting. These restrictions are similar to those regulating bulletin board services and IIS providers. Beyond formal controls such as policies, instructions, and defamation liability, the government also utilizes informal mechanisms to discipline media, ranging from editorial responsibility for content to economic incentives, intimidation, and other forms of pressure.[83]

The government has used this framework to bring social media in line with Internet content regulations. Under the January 1, 2008, "Provisions on the Management of Internet Audio and Video Programming Services,"[84] issued by the State Administration of Radio, Film, and Television (SARFT) and MIIT, Internet audiovisual program service providers that produce original content are required to obtain a broadcast production license and Internet news information services licenses regulated by the MIIT. Similarly, video service providers are also prohibited from allowing any individuals without a special license to upload content pertaining to "current events."[85] Audiovisual

programs are further prevented from presenting content that pertains to all but one of the prohibitions listed under the 2005 provisions.[86] The Provision on Internet AV Programming Services was strengthened on March 30, 2009, with the addition of 21 additional types of content that Internet audiovisual service providers were required to edit or delete. These content categories range from sexually provocative or pornographic content; to content that promotes "a negative or decadent outlook, world view, or value system, or deliberate exaggeration of the ignorance and backwardness of ethic groups or social ills"; to content that calls "for religious extremism, provocation of conflict between religions, religious sects, or between believers and nonbelievers, hurting the feelings of the public," among others.[87] Within these updated rules, Internet AV program service providers are also mandated to "improve their program content administration systems by hiring well-qualified service personnel to review and filter content" so that content does not violate existing and new rules.[88]

With the explosion of an active blogosphere in China, the government implemented the Convention on Blog Service Discipline[89] in 2007, which was signed by blog service providers including the People's Daily Online, Sina, Sohu, Netease, Tencent, TOM, MSN China, and Qianlon.[90] According to the convention, blog service providers should "abide by state laws, regulations and policies, safeguard the legitimate blog users and the public interest." Blog providers must also have an end-user agreement with terms of service for the blogger to abstain from disseminating rumors or false information and to delete postings considered bad or illegal. The blog provider has to encourage real-name registration, supervise and manage content, and remove illegal content or cease blog services.[91]

Similarly, end users are also subject to content controls such as those as laid out in the rules of the National People's Congress (NPC) Standing Committee on Safeguarding Internet Security.[92] Violators of these rules can incur fines, content removal, and criminal liability. For example, on October 28, 2010, Twitter user Cheng Jianping was arrested for disturbing social order and sent to a labor camp for retweeting a sarcastic comment about the anti-Japanese protests in China, suggesting that the protesters attack the Japan pavilion at the Shanghai Expo.[93] In January 2011, blogger Lin Chenglong was arrested for spreading obscene material in his blog where he wrote about his experiences with prostitutes and posted obscene photos.[94] In 2010, Zhao Lianhai, an activist for families who suffered from the Chinese milk scandal and started the "Home for Kidney Stone Babies Web site" (http://jieshibaobao.com), had his Web site blocked and shut down. He was consequently charged with inciting social disorder and sentenced to two and a half years' imprisonment.[95] Seventy-seven netizens were reported imprisoned in 2009.[96]

In 2010, the Chinese government amended the 1988 Law on Guarding State Secrets (State Secrets Law) to require all ICT companies operating within the country to comply with measures to protect state secrets. "State secrets" are defined as matters of national security interests in the realm of political, economic, defense, and foreign

affairs.[97] The revised law was passed in April, on the heels of the Google-China conflict, and took effect in October. Under Article 28 of the law, Internet and other public information network operators and service providers are required to cooperate with the state in investigating leaked secrets when the information involving the secret has been published on the Internet or other public information networks. In such cases, companies are required to cease transmission of the information immediately, and maintain and disclose records to public security organs, state security organs, or relevant departments that guard state secrets.[98] According to a Beijing-based lawyer, "Such regulation will leave users with no secrets at all, since the service providers have no means to resist the police."[99] In the past, the law has been invoked to target journalists, activists, and dissidents, like journalist Shi Tao, who sent an e-mail from his personal Yahoo! account to a prodemocracy group based in the United States, summarizing a government-issued directive on how to manage the 15th anniversary of the 1989 Tiananmen Square crackdown. He was subsequently arrested and imprisoned when Yahoo! disclosed his identity to authorities.[100]

Beyond legal restrictions to control Internet use, the state has also launched campaigns to clean up Internet use. These campaigns may be organized around a specific issue area (such as online gambling) during key politically sensitive events (such as the lead-up to the 17th Party Congress in 2007).[101] In 2010, Chinese authorities launched campaigns against online gambling and pornography and Web sites promoting or selling illegal drugs. In December 2009, authorities initiated an antipornography campaign that shut down more than 60,000 Web sites, deleted over 350 million pornographic and lewd online articles, pictures, and videos, and rounded up 4,965 suspects by the end of the year. Of these suspects, 1,332 were found criminally liable, and 58 were jailed for five or more years.[102] In the same year, the state launched a campaign against Web sites promoting or selling illegal drugs as a part of a nationwide effort to stamp out the production and distribution of counterfeit drugs or drugs that violated intellectual property rights.[103] As a result, 290 Web sites were shut down. Similarly, a February 2010 campaign against online gambling led to 3,430 suspects rounded up and 670 online gambling Web sites shut down.[104]

Surveillance

The PRC continues to refine Internet surveillance mechanisms to monitor users' activities. The Golden Shield project—a digital surveillance network with almost complete coverage across public security units nationwide—is the pillar of China's surveillance regime.[105] Its use of identification cards with scannable computer chips and photos further allows the state to effectively police citizens. Since 2006, local governments have been developing "Safe City" surveillance and communications networks that connect police stations through video surveillance, security cameras, and back-end

data management facilities to specific locations including Internet cafés, financial centers, and entertainment areas. In recent years, the state has begun exploring real-name registration as a monitoring tool. Private companies, too, are often complicit in the state's surveillance regime.

Real-name registration (through ID cards) in Internet cafés illustrates how filtering and monitoring/surveillance are complementary processes that allow the state to manage the Internet. This is reflected in a recent speech, "Concerning the Development and Administration of Our Country's Internet," delivered to the Standing Committee of the National People's Congress on April 29, 2010.[106] The speaker claimed that in order to strengthen the basic management and security of the Internet, the state would have to implement the real-name system and improve the efficiency in handling harmful online information.[107]

In June 2010, the Chinese government released a white paper on Internet policy that insisted, "The Chinese government attaches great importance to protecting the safe flow of Internet information, actively guides people to manage Web sites in accordance with the law and use the Internet in a wholesome and correct way."[108] Following the release of the white paper, the government began to take active steps in strengthening security through the implementation of real-name registration across the country, including in Internet cafés.[109]

Because real-name registration removes the anonymity that allows citizens to make public comments without fear of state sanctions, it can lead to self-censorship among users.[110] Real-name registration policies also allow the state to track each user's Internet activities. In the summer of 2010, Internet users across cities in China were required to swipe their second-generation identity cards through an ID scanner in order to gain online access at Internet cafés.[111] In September 2010, real-name registration was expanded into the area of mobile phones so users are now required to show their identity card to purchase a SIM card.[112]

Prior to the white paper and the April 2010 speech, real-name registration had already been implemented on some Web sites. For instance, a few leading Web portals in China already require users to register their real names to post on message or bulletin boards. Sina requires users to register real names as well as identity cards in order to post comments on their site.[113] Since 2005, users of student-run university discussion forums have been required to register with their real identifying information before posting messages online.[114] In May 2010, the Chinese state was actively exploring ways to have all Internet users register their real names prior to posting on discussion forums or chat rooms.[115]

In December 2009, the China Internet Network Information Center (CNNIC), which operates under MIIT and is responsible for Internet affairs and China's domain name registry, announced that only businesses or organizations would be eligible for registering domain names ending in .cn.[116] The CNNIC stated that this control would

eliminate abuse of .cn domain names by criminals. Because self-employed workers had been affected by the new rules, by February 2010 the CNNIC announced that they would allow individuals to register once again, but only if applicants registered for the domain with their government ID cards in person and attached a photograph to each application[117]—effectively ending anonymity in Web site registration. In opposition to the new reporting requirements, domain name registrar Go Daddy suspended registration for the .cn domain.[118]

Although there have been demonstrations against real-name registration on campus bulletin boards,[119] other efforts have embraced real-name registration on the grounds that it can empower citizens. A campaign launched by activist blogger Ai Aiwei on Twitter argued, "The fact that we try to cover our identity that we are so afraid of what we said has empowered the authoritarian state. We need to speak in public with transparency and demand the government to do the same. If we do not encourage such act and continue to live in fear, such fear would be exaggerated and we could not make any change."[120] In just a day, hundreds of Internet users had joined the campaign.[121]

Technically, Internet laws and regulations provide protection for individual privacy. However, state regulations require private actors to cooperate not only in monitoring and filtering online content but also in keeping records of personal user information and activities to be handed to authorities upon request.

Under the Measures for the Management of E-mail Services, e-mail service providers are required to keep personal information and e-mail addresses of users and can disclose such information with users' consent or when authorized for national security reasons or criminal investigations according to procedures stipulated by law.[122] Similarly, IIS providers, ISPs, and electronic bulletin board service providers are required to record users' information and activities. Internet service providers are obliged to record the addresses or domain names their users have accessed, while IISs are required to record the content of the information, the date such information was released, and the address or the domain name that hosted such information. Bulletin board service providers have to keep records of the contents, time of publication, and Web site names or addresses of the information published on their services, as well as user information.[123] All these services are required to store records for 60 days and provide records to authorities upon demand.[124]

Internet cafés, too, are heavily regulated and are required to install filtering software and record patron information and complete session logs for up to 60 days.[125] In August 2010, the Chinese government ordered that the installation of surveillance software in Internet cafés across Tibet be completed by the end of the month.[126]

Companies such as the China Mobile Communications Corporation (China's largest mobile phone company), Tencent, and Skype also monitor and store information about user activities. In a discussion on targeted advertising at the 2008 World Economy Forum, the CEO of China Mobile Communications Corporation, Wang

Jianzhou, announced that the company had access to the personal data of its users—including the user's exact whereabouts—which were given to the authorities on demand.[127] China's most popular instant messenger, QQ (owned by Tencent), was found to have installed a keyword-blocking program in their client software that monitored and recorded users' online communication. This information was given to authorities if required.[128]

In 2008, researcher Nart Villeneuve discovered that TOM-Skype, the Chinese-marketed version of Skype, had stored more than a million user records in seven types of log files stored on publicly accessible servers, including IP addresses, user names, and time-and-date stamps.[129] For call information logs dating from August 2007, the user name and phone number of the recipient were also logged, while content filter logs dating from August 2008 also contained full texts of chat messages (which themselves contained sensitive information such as e-mail addresses, passwords, and bank card numbers). With the information contained in the log files, it would be possible to conduct politically motivated surveillance by using simple social-networking tools to identify the relationships between users.[130]

Cyber Attacks

A growing number of countries, organizations, and companies have reported cyber attacks appearing to originate in China. These reports have ranged from instances of targeted malware attacks against human rights groups, distributed denial of service (DDoS) attacks against government Web sites, and high-profile attempts to compromise Google's e-mail system. While assessing attribution and motivation behind such attacks is perennially difficult, there is growing concern about the security risk posed by cyber attacks originating in China.

In January 2010, Google announced it would no longer censor search results on Google China (http://google.cn) following cyber attacks on its infrastructure.[131] Google claimed that the e-mail accounts of a number of human rights activists connected with China were compromised by the attack, which had also targeted dozens of other Silicon Valley firms.[132] Later reports suggested that the attackers had gained access to the password system controlling the access of millions of users of Google's services.[133] U.S. State Department cables leaked through Wikileaks implicated a senior member of China's government in this attack.[134] An MIIT spokesman denied the Chinese government's involvement, suggesting that in fact China was the world's primary victim of cyber attacks.[135] A compromise solution between Google and the government of China was eventually reached under which users in China were offered a link to Google's unfiltered Chinese-language search services based in Hong Kong.[136]

Google was not the only source to report attacks on human rights and civil society organizations working on issues related to China. Malicious e-mails purporting to

originate from the group Human Rights in China were sent to numerous other organizations that, if opened and executed, would install malware connected to a command-and-control server located in China.[137] In a similar incident, staff at the Committee to Protect Journalists received falsified e-mail invitations to the Nobel Peace Prize awards ceremony of Chinese dissident Liu Xiabo containing malware designed to contact servers in Bengbu, China.[138] These reports followed 2009's *Tracking GhostNet* report by the Information Warfare Monitor, which identified an extensive cyber espionage network that compromised thousands of computers, including some at the private office of the Dalai Lama and several Tibetan nongovernmental organizations (NGOs), which contacted command-and-control servers located in China.[139]

Other organizations that do work in China have also reported malware infection. Journalists and other staff of media organizations have been targeted with malware attacks that made contact with servers in China. The Foreign Correspondents' Club of China warned fellow journalists to be cautious following an e-mail-based malware attack targeting media organizations.[140] Further investigation found a sophisticated malware campaign that compromised users' computers and attempted to make contact with servers at a university in Taiwan.[141] The increase in malware attacks targeting foreign journalists occurred before the 60th anniversary of the founding of the People's Republic of China, a sensitive political event that saw an increase in security precautions.[142]

Cyber attacks attributed to sources in China have been identified by a variety of different states. Reports from Australia,[143] Japan,[144] Pakistan,[145] South Korea,[146] the United Kingdom,[147] and the United States[148] all point to the rise of cyber attacks originating from China. However, attribution of these incidents remains an ongoing challenge. While many of the targets of these attacks may reflect strategic interests for China's government, the country also represents the largest single population of Internet users and thus the greatest potential source of cyber-attack instigators.

ONI Testing Results

In 2010, the OpenNet Initiative conducted testing on a single Chinese ISP, CNLink Networks. The testing results confirm that China maintains an advanced Internet filtering system at the backbone level that is capable of blocking content through a variety of methods, such as IP blocking, DNS tampering, and keyword filtering (TCP resets).

Filtering in China is implemented at the backbone level through a method known as keyword-based filtering, or TCP resets. This blocking method is unique to China and works in part by inspecting the content of IP packets to determine if specific, sensitive keywords are present. These keywords relate to historical events, banned groups, and other topics considered sensitive or controversial by the Chinese government. A

keyword detected in either the header or the content of a message triggers the blocking mechanism and sends reset packets to both the source and destination IP addresses to disrupt and break the Internet user's connection.

The OpenNet Initiative found a lesser extent of Internet protocol (IP) blocking. Consistent with past ONI findings, transparency in Internet filtering remains low. There is no publicly available list of banned sites or mechanisms for users to petition to have a blocked site reviewed. When users attempt to access a blocked site, they receive a network timeout error page that does not indicate if or why the site has been blocked—it can appear to be the result of routine network errors.

Results indicate that the Chinese government continues to concentrate on blocking content that could potentially undermine the authority of the CCP as well as its control over social stability. It was found that CNLink Networks was extensively filtering Web sites critical of the ruling party. These sites include foreign and international media reporting on China in both foreign and local languages, such as Boxun (http://boxun.com), Ming Pao (http://www.mingpao.com), the Epoch Times (http://epochtimes.com), BBC Asia Pacific (http://news.bbc.co.uk/2/hi/asia-pacific), the Chinese-language BBC Zhongwen (http://news.bbc.co.uk/chinese/simp/hi/default.stm), Voice of America (http://voanews.com), and Radio Free Asia (both the English- and local-language versions of the site: http://rfa.org, http://rfa.org/mandarin, http://rfa.org/uyghur, and http://rfa.org/tibetan). Web sites belonging to human rights groups critical of the Chinese state are also extensively filtered, including those belonging to Human Rights in China (http://hrichina.org), Amnesty International (http://web.amnesty.org, http://amnesty.org.hk), Human Rights Watch (http://hrw.org, and http://www.hrw.org/chinese), and the China Labour Bulletin (http://clb.org.hk).

The filtering program of CNLink Networks also heavily emphasized Web sites focusing on politically sensitive issues related to China's national stability such as Uyghur, Tibetan, and Mongolian separatism and rights protection. Although these issues are all sensitive for the Chinese government, CNLink Networks filtered significantly more Web sites with content related to Tibet than the Uyghur minority or Mongolia. Among the Web sites blocked were http://savetibet.org, http://tibetanyouthcongress.org, http://friendsoftibet.org, http://www.uyghuramerican.org, and http://innermongolia.org. Falun Gong Web sites were also extensively filtered.

Web sites that challenge the reunification policy of the PRC—such as those calling for the formal independence of Taiwan—remain filtered, such as sites of the Taipei Economic and Cultural Office in New York (http://www.taipei.org), New Taiwan, Ilha Formosa, Taiwan Organization in the United States (http://taiwandc.org), and the main portal of the Taiwanese government (http://gov.tw). Web sites pertaining to politically sensitive events are also targeted, such as content related to Tiananmen Square (e.g., http://64memo.com, http://tiananmenvigil.org, and http://en.wikipedia.org/wiki/Tiananmen_Square_protests_of_1989).

While Web sites that challenge the political authority of the ruling party are the primary target of filtering on CNLink Networks, the ISP also blocks content that the government deems may harm the social fabric. Pornographic Web sites are heavily targeted, as well as online gambling (such as http://888casino.com and http://partypoker.com). This is consistent with the 2010 state crackdown on pornographic[149] and online gambling[150] content.

In contrast to previous ONI findings, testing results showed that China blocks access to major social media platforms such as Facebook, Twitter, and Blogspot. At the time of testing, other social media Web sites such as http://wordpress.com, http://wordpress.org, and http://flickr.com were accessible, though Wordpress blogs critical of the state or touching on political sensitive were blocked (such as http://chinaview.wordpress.com and http://seapa.wordpress.com). Web sites for circumvention tools were also found blocked, including http://gardennetworks.com, https://dongtaiwang.com, http://wujie.net, and http://peacefire.org.

Conclusion

Although the Chinese government views the Internet as a key engine of economic growth and an important platform for social and public services, it also sees the need to control the Internet to protect its domestic interests. With the largest number of Internet users in the world, the expanding scope of online content presents a major challenge for the Chinese government, which is intent on maintaining social order and stability in a context of rapid development and social transformation. Increasing contradictions arise out of these processes.[151] State authorities resist international criticism by pointing to China's developing country status and vulnerability to potential disorder.

The Chinese government maintains a strict and extensive approach to controlling the flow of information through a robust legal system that delegates filtering and monitoring responsibilities to domestic online service providers. Its content-control regulations impose self-censorship on users, which is reinforced by information campaigns and just-in-time filtering during sensitive moments. The mix of rapid development and a growing online population will remain persistent challenges to China's efforts at information control, and the state will continue to react with new measures for denying and shaping the flow of information in the country.

Notes

1. Will Foster, Milton Mueller, and Zixiang Tan, "China's New Internet Regulations: Two Steps Forward, One Step Back," *Communications of the ACM* 40, no. 12 (1997), http://portal.acm.org/citation.cfm?id=265565.

2. China Internet Network Information Center, *27th Statistical Survey Report on Internet Development in China* [in Chinese], January 19, 2011, http://research.cnnic.cn/html/1295338825d2556.html.

3. China Information Industry Trade Association—Information Security Subcommittee, *China Information Security Industry Development White Paper, 2005–2010* [in Chinese], http://www.itsec.gov.cn/sh/1341.htm.

4. Human Rights Watch, "China: Investigate Crackdown before Torch Relay's Passage through Tibet," March 24, 2008, http://www.hrw.org/en/news/2008/03/23/china-investigate-crackdown-torch-relay-s-passage-through-tibet.

5. Michael Bristow, "Tibet Anti-China Protests Spread," BBC News, March 17, 2008, http://news.bbc.co.uk/2/hi/asia-pacific/7300274.stm.

6. Human Rights Watch, "China: Investigate Crackdown before Torch Relay's Passage through Tibet."

7. Ministry of Foreign Affairs of the People's Republic of China, "Regulations on Reporting Activities by Foreign Journalists during the Beijing Olympic Games and the Preparatory Period," December 1, 2006, http://un.fmprc.gov.cn/eng/zxxx/t282169.htm.

8. OpenNet Initiative, "Country Profile: China," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010), 449–487.

9. David Batty, "Media Face Web Censorship at Beijing Olympics," *The Guardian*, July 30, 2008, http://www.guardian.co.uk/world/2008/jul/30/china.olympicgames2008.

10. Information Office of the State Council of the People's Republic of China, *National Human Rights Action Plan of China (2009–2010)*, 2009, http://news.xinhuanet.com/english/2009-04/13/content_11177126.htm.

11. David Gelles, Joseph Menn, and Richard Waters, "Websites Blocked Ahead of Tiananmen Anniversary," *Financial Times*, June 3, 2009, http://www.ft.com/cms/s/0/e8b88790-4fc6-11de-a692-00144feabdc0.html#axzz1C9ZMGAcs; "There May Be Rising Mass Incidents in China in 2009 [in Chinese]," NF Daily, January 26, 2009, http://opinion.nfdaily.cn/content/2009-01/26/content_4867542.htm; Stan Schroeder, "China Blocks Twitter (and Almost Everything Else)," Mashable, June 2, 2009, http://mashable.com/2009/06/02/china-blocks-twitter-and-almost-everything-else.

12. Human Rights Watch, *We Are Afraid to Even Look for Them: Enforced Disappearances in the Wake of Xinjiang's Protests*, October 22, 2009, http://www.hrw.org/en/reports/2009/10/22/we-are-afraid-even-look-them.

13. Ibid.

14. Ibid.

15. UNESCO Bangkok, "China: Journalists Protest Savage Attacks on Colleagues," September 22, 2009, http://www.unescobkk.org/information/news-display/article/china-journalists-protest-savage-attacks-on-colleagues; Hong Kong Journalists Association, "Our Declaration for the Protest March on Liaison Office on 13 September, 2009," September 13, 2009, http://www.hkja.org.hk/site/portal/Site.aspx?id=A1-812&lang=en-US.

16. OpenNet Initiative Blog, "China Shuts Down Internet in Xinjiang Region after Riots," July 6, 2009, http://opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots.

17. Quoted in "Official: Internet Cut in Xinjiang to Prevent Riot from Spreading," Xinhua News Agency, July 7, 2009, http://news.xinhuanet.com/english/2009-07/07/content_11666802.htm.

18. Ibid.

19. "Accept the Delegation of Some Representatives of Xinjiang, the Media" [in Chinese], China News Service, March 7, 2010, http://www.chinanews.com/shipin/313/2010/0307/76.html.

20. "Google 'May Pull Out of China after Gmail Cyber Attack,'" BBC News, January 13, 2010, http://news.bbc.co.uk/2/hi/8455712.stm.

21. Ibid.

22. Chris Buckley and Lucy Hornby, "China Defends Censorship after Google Threat," Reuters, January 14, 2010, http://www.reuters.com/article/2010/01/14/us-china-usa-google-idUSTRE60C1TR20100114.

23. Ibid.

24. Kenneth Tan, "The Google.cn/Google.com.hk Lockdown Has Begun: ALL Search Queries Now End in a Connection Reset," Shanghaiist, March 30, 2010, http://shanghaiist.com/2010/03/30/the_googlecn_googlecomhk_lockdown_h.php.

25. Google, "An Update on China," June 28, 2010, http://googleblog.blogspot.com/2010/06/update-on-china.html.

26. Hillary Rodham Clinton, "Remarks on Internet Freedom," U.S. Department of State, January 21, 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm.

27. "The Real Stake in 'Free Flow of Information,'" *Global Times*, January 22, 2010, http://opinion.globaltimes.cn/editorial/2010-01/500324.html.

28. Ma Zhaoxu, "Foreign Ministry Spokesperson Ma Zhaoxu's Remarks on China-Related Speech by US Secretary of State on 'Internet Freedom,'" Ministry of Foreign Affairs of the People's Republic of China, January 22, 2010, http://www.fmprc.gov.cn/eng/xwfw/s2510/t653351.htm.

29. International Telecommunication Union (ITU), "Internet Indicators: Subscribers, Users and Broadband Subscribers," 2009 Figures, http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

30. Paul Budde Communication Pty., Ltd., "China—Key Statistics, Telecom Market, Regulatory Overview and Forecasts," July 7, 2010.

31. ITU, "Internet Indicators: Subscribers, Users and Broadband Subscribers"; China Internet Network Information Center, *27th Statistical Survey Report on Internet Development in China*.

32. China Internet Network Information Center, *27th Statistical Survey Report on Internet Development in China*.

33. ITU, "Internet Indicators: Subscribers, Users and Broadband Subscribers."

34. Paul Budde Communication Pty., Ltd., "China—Key Statistics, Telecom Market, Regulatory Overview and Forecasts."

35. Ibid.

36. China Internet Network Information Center, *27th Statistical Survey Report on Internet Development in China*.

37. Ibid.

38. Paul Budde Communication Pty., Ltd., "China—Key Statistics, Telecom Market, Regulatory Overview and Forecasts."

39. China Internet Network Information Center, *27th Statistical Survey Report on Internet Development in China*.

40. China Internet Network Information Center, *Statistical Report on Internet Development in China*, July 2010, http://www.cnnic.net.cn/uploadfiles/pdf/2010/8/24/93145.pdf.

41. China Internet Network Information Center, *27th Statistical Survey Report on Internet Development in China*.

42. "Search Engine Baidu Slams Google in China," AFP, January 20, 2011, http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=10700822.

43. China Internet Network Information Center, *27th Statistical Survey Report on Internet Development in China*.

44. Ibid.

45. Paul Budde Communication Pty., Ltd., "China—Key Statistics, Telecom Market, Regulatory Overview and Forecasts."

46. "Highlights of China's Institutional Restructuring Plan," *People's Daily*, March 16, 2008, http://english.peopledaily.com.cn/90001/90776/90785/6374104.html.

47. China Telecom USA, "Access China with CN2: The Internet for Business," http://www.chinatelecomusa.com/files/Chinausa_WP_FinalWeb.pdf.

48. Telegeography, "Broadband Provider Rankings: The Rise and Rise of China," July 28, 2010, http://www.telegeography.com/cu/article.php?article_id=33858.

49. China Internet Network Information Center, *27th Statistical Survey Report on Internet Development in China*.

50. Paul Budde Communication Pty., Ltd., "China—Key Statistics, Telecom Market, Regulatory Overview and Forecasts."

51. Sumner Lemon, "After Years of Delays, China Finally Issues 3G Licenses," *PC World*, January 7, 2009, http://www.pcworld.com/businesscenter/article/156612/after_years_of_delays_china_finally_issues_3g_licenses.html.

52. Alice Xin Liu, "Hu Yong Interview: The Digital Age, Orwell's 'Newspeak' and Chinese Media," Danwei, April 16, 2009, http://www.danwei.org/media/hu_yong_interview.php.

53. David Bandurski, "China's Guerrilla War for the Web," *Far Eastern Economic Review*, July 2008, http://testfeer.wsj-asia.com/essays/2008/august/chinas-guerrilla-war-for-the-web.

54. Ryan McLaughlin, "Human Flesh Search Engines—Crowd-Sourcing 'Justice,'" January 28, 2009, http://www.ryan-mclaughlin.com/blog/the-tech-dynasty/human-flesh-search-engines-crowd-sourcing-justice.

55. Vaclav Havel, Vaclav Maly, and Dana Nemcova, "A Nobel Prize for a Chinese Dissident," *New York Times*, September 20, 2010, http://www.nytimes.com/2010/09/21/opinion/21iht-edhavel.html?_r=2.

56. John Garnaut, "China's Plan to Use Internet for Propaganda," *The Age*, July 14, 2010, http://www.theage.com.au/technology/technology-news/chinas-plan-to-use-internet-for-propaganda-20100713-109hc.html.

57. OpenNet Initiative, "China's Green Dam: The Implications of Government Control Encroaching on the Home PC," June 12, 2009, http://opennet.net/sites/opennet.net/files/GreenDam_bulletin.pdf.

58. Ibid.

59. Loretta Chao and Jason Dean, "Chinese Delay Plan for Censor Software," *Wall Street Journal*, July 1, 2009, http://online.wsj.com/article/SB124636491863372821.html.

60. Oiwan Lam, "China: Blue Dam Activated," Global Voices Advocacy, September 13, 2009, http://advocacy.globalvoicesonline.org/2009/09/13/china-blue-dam-activated.

61. Ibid.

62. Stephanie Wang and Robert Faris, "Welcome to the Machine," *Index on Censorship* 37, no. 2 (2008): 106–111.

63. Rebecca MacKinnon, "China's Censorship 2.0: How Companies Censor Bloggers," *First Monday* 14, no. 2 (2009), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089.

64. Nart Villeneuve, "Search Monitor Project: Toward a Measure of Transparency," Citizen Lab Occasional Paper, June 2008, http://www.nartv.org/mirror/searchmonitor.pdf.

65. OpenNet Initiative Blog, "China Shuts Down Internet in Xinjian Region after Riots," July 6, 2009, http://opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots.

66. Steven Jiang, "China Blanks Nobel Peace Prize Searchers," CNN, "October 8, 2010, http://edition.cnn.com/2010/WORLD/asiapcf/10/08/china.internet/?hpt=C1.

67. Committee to Protect Journalists, "National Day Triggers Censorship, Cyber Attacks in China," September 22, 2009, http://cpj.org/2009/09/national-day-triggers-censorship-cyber-attacks-in.php.

68. Tania Branigan, "China Blocks Twitter, Flickr and Hotmail Ahead of Tiananmen Anniversary," *The Guardian*, June 2, 2009, http://www.guardian.co.uk/technology/2009/jun/02/twitter-china.

69. Foreign Correspondents' Club of China, "China Should Allow Access to Tibetan Areas," March 9, 2009, http://www.fccchina.org/2009/03/09/china-should-allow-access-to-tibetan-areas.

70. Edward Wong and David Barboza, "Wary of Egypt Unrest, China Censors Web," *New York Times*, January 31, 2011, http://www.nytimes.com/2011/02/01/world/asia/01beijing.html.

71. China Internet Illegal Information Reporting Center, http://ciirc.china.cn.

72. Li Dan, "The Internet and Chinese Civil Society," *China Rights Forum,* no. 2 (2010): 96–104.

73. Rebecca MacKinnon, "China's Internet Censorship and Controls: The Context of Google's Approach in China," *China Rights Forum*, no. 2 (2010): 70–81.

74. Nart Villeneuve, *Breaching Trust: An Analysis of Surveillance and Security Practices on China's TOM-Skype Platform*, Information Warfare Monitor/ONI Asia, http://www.nartv.org/mirror/breachingtrust.pdf.

75. MacKinnon, "China's Internet Censorship and Controls."

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

77. Ibid.

78. Measures for Managing Internet Information Services, Article 20 [in Chinese], issued by the State Council on September 25, 2000, effective October 1, 2000. Unofficial English translation is available at http://www.chinaculture.org/gb/en_aboutchina/2003-09/24/content_23369.htm.

79. Ibid.

80. Rules on the Management of Internet Electronic Bulletin Services [in Chinese], passed by the Fourth Ministry Affairs Meeting of the Ministry of Information Industry on October 8, 2000. Unofficial English translation is available at mesharpe.metapress.com/index/4T7361047374J2U0.pdf.

81. Provisions on the Administration of News Information Services, Article 2 [in Chinese], issued by the Ministry of Information Industry and the State Council Information Office on September 25, 2005, http://www.isc.org.cn/20020417/ca315779.htm. Unofficial English translation is available at http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

82. Provisions on the Administration of News Information Services, Article 11 [in Chinese], issued by the Ministry of Information Industry and the State Council Information Office on September 25, 2005, http://www.isc.org.cn/20020417/ca315779.htm. Unofficial English translation is available at http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

83. Benjamin Liebman, "Watchdog or Demagogue? The Media in the Chinese Legal System," *Columbia Law Review,* January 2005: 41.

84. "Provisions on the Administration of News Information Services" [in Chinese], issued by the Ministry of Information Industry and the State Council Information Office on September 25, 2005, http://www.cecc.gov/pages/virtualAcad/index.php?showsingle-24396.

85. Ibid.

86. Ibid.

87. "Section 2, SARFT Notice for Strengthening the Administration of Internet Audio and Video Programming Content" [in Chinese] issued on March 30, 2009. Unofficial translation is available at http://www.sarft.gov.cn/articles/2009/03/30/20090330171107690049.html; "New Rules Imposed on Internet Video Content," Danwei, April 1, 2009, http://www.danwei.org/media_regulation/new_rules_imposed_on_internet.php.

88. "Section 3, SARFT Notice for Strengthening the Adminstration of Internet Audio and Video Programming Content."

89. Internet Society of China, "Internet Society of China Released 'Self-discipline Convention Blog Service' to Promote Orderly Development of Blog Service" [in Chinese], August 21, 2008, http://www.isc.org.cn/ShowArticle.php?id=7955.

90. Ibid.

91. Ibid.

92. For example, see "Rules of the NPC Standing Committee on Safeguarding Internet Security" [in Chinese], issued by the NPC Standing Committee on December 28, 2000. Unofficial English translation is available at http://www.guangshunda.com/en/Message.html.

93. Reporters Without Borders, "Woman Sentenced to a Year's Forced Labor over One Ironic Tweet," November 24, 2010, http://en.rsf.org/china-woman-sentenced-to-a-year-s-forced-24-11-2010,38886.html.

94. "Man Arrested for Obscene Blog," *China Times,* January 6, 2011, http://china.globaltimes.cn/society/2011-01/609726.html.

95. Bo Gu, "'I'm Innocent,' Roars Chinese Dad at Sentencing," NBC News, November 10, 2010, http://behindthewall.msnbc.msn.com/_nv/more/section/archive?date=2010/11.

96. Reporters Without Borders, "China," http://en.rsf.org/report-china,57.html.

97. Ibid.

98. "Law of the People's Republic of China on Guarding State Secrets," adopted at the Third Meeting of the Standing Committee of the Seventh National People's Congress on September 5, 1988, and revised at the 14th Session of the Standing Committee of the 11th National People's Congress on April 29, 2010, http://www.npc.gov.cn/npc/xinwen/2010-04/29/content_1571588.htm. Unofficial English translation is available at http://www.hrichina.org/public/PDFs/PressReleases/20101001-StateSecretsLaw-EN.pdf.

99. Quoted in Gillian Wong, "China Set to Tighten State Secrets Law Forcing Internet Firms to Inform on Users," *Washington Post*, April 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/04/27/AR2010042704503.html.

100. Human Rights in China, "HRIC Case Highlight: Shi Tao and Yahoo," http://www.hrichina.org/public/highlight; Human Rights in China, "Examples of Cases Involving Charges Related to State Secrets from 2007 to Present," July 24, 2009, http://hrichina.org/public/contents/press?revision_id=170447&item_id=170446.

101. In the lead-up to the 17th party congress in 2007, an official announcement from the General Administration of Press and Publications indicated that it would clamp down on "illegal news coverage" and "false news" in order to create a healthy and harmonious environment for the congress. A crackdown on political news reporting, commentary, and Internet discussion followed. Media outlets were given instructions on what they could write about, while ISPs and individual Web sites disabled chat rooms and forums. See Peter Ford, "Why China Shut Down 18,401 Web Sites," *Christian Science Monitor*, September 25, 2007, http://www.csmonitor.com/2007/0925/p01s06-woap.html?page=1.

102. "China Shuts Over 60,000 Porn Websites This Year," Reuters, December 30, 2010, http://www.reuters.com/article/2010/12/30/china-internet-idUSTOE6BT01T20101230.

103. "China Cracks Down on Illegal Online Drug Selling," *People's Daily,* November 25, 2010, http://english.people.com.cn/90001/90782/90872/7210365.html; "290 Websites Closed for Illicit Drug Promotion," *People's Daily*, November 17, 2010, http://english.peopledaily.com.cn/90001/90776/7202638.html.

104. "China Cracks Down on Online Gambling, Arrests 3,430," Xinhua News Agency, June 8, 2010, http://www.chinadaily.com.cn/bizchina/2010-06/08/content_9948601.htm.

105. "National Development and Reform Commission Issues National Approval for the 'Golden Shield' Construction Project at Management Conference" [in Chinese], Ministry of Public Security, November 17, 2006. For more discussion of the Golden Shield Project, see Greg Walton, "China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China, a Rights and Democracy Report," International Centre for Human Rights and Democratic Development, October 2001, http://www.dd-rd.ca/site/_PDF/publications/globalization/CGS_ENG.PDF.

106. 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.

107. Ibid.

108. Information Office of the State Council of the People's Republic of China, *The Internet in China*.

109. "Top Ten: Please Show Your ID," *China Daily*, December 10, 2010, http://www2.chinadaily.com.cn/china/2010-12/10/content_11684998.htm.

110. Ibid.

111. Ibid.

112. "Real-name Registration Required for Mobile Users in China," Xinhua News Agency, September 1, 2010, http://news.xinhuanet.com/english2010/video/2010-09/01/c_13473049.htm.

113. See registration form at http://login.sina.com.cn/cgi/register/reg_sso_comment.php?entry=comment.

114. Philip P. Pan, "Chinese Crack Down on Student Web Sites," *Washington Post*, March 24, 2005, http://www.washingtonpost.com/wp-dyn/articles/A61334-2005Mar23.html.

115. Peter Foster, "China to Force Internet Users to Register Real Names," *The Telegraph*, May 5, 2010, http://www.telegraph.co.uk/news/worldnews/asia/china/7681709/China-to-force-internet-users-to-register-real-names.html.

116. China Internet Network Information Center, "The Notification about Further Enhancement of Auditing Domain Name Registration Information," December 14, 2009, http://www.cnnic.net.cn/html/Dir/2009/12/12/5750.htm.

117. MacKinnon, "China's Internet Censorship and Controls."

118. Chloe Albanesius, "Go Daddy Cuts Off Chinese Domain-Name Registration," *PC Magazine*, March 24, 2010, http://www.pcmag.com/article2/0,2817,2361779,00.asp.

119. Philip P. Pan, "Chinese Crack Down on Student Web Sites."

120. Oiwan Lam, "China: Radical Real Name Registration Campaign," *Global Voices*, June 15, 2010, http://advocacy.globalvoicesonline.org/2010/06/15/china-radical-real-name-registration-campaign.

121. Ibid.

122. Measures for the Management of E-mail Services, Article 3 [in Chinese], issued by the Ministry of Information Industry on November 7, 2005, effective March 30, 2006.

123. Rules on the Management of Internet Electronic Bulletin Services, Articles 14 and 15 [in Chinese], issued by the Ministry of Information Industry on October 7, 2000. Unofficial English translation is available at http://mesharpe.metapress.com/media/3g267jyuyj4urbm4ek0j/contributions/4/t/7/3/4t7361047374j2u0_html/fulltext.html.

124. Measures for Managing Internet Information Services, Article 14 [in Chinese], issued by the State Council on September 25, 2000, effective October 1, 2000. Unofficial English translation is available at http://www.chinaculture.org/gb/en_aboutchina/2003-09/24/content_23369.htm.

125. Regulations on the Administration of Business Sites Providing Internet Services, Articles 19, 21, and 23 [in Chinese], issued by the State Council on September 29, 2002, effective November 15, 2002.

126. "China Tightens Internet Censorship in Tibet," *Tibetan Review,* August 5, 2010, http://www.tibetanreview.net/news.php?id=6834.

127. "China's Mobile Network: A Big Brother Surveillance Tool?" ABC News, January 28, 2008, http://www.abc.net.au/news/stories/2008/01/28/2147712.htm.

128. Matthew Robertson and Michelle Yu, "In Chinese Internet Rumble, User Rights Not the Focus," *The Epoch Times*, http://www.theepochtimes.com/n2/content/view/45580.

129. Villeneuve, *Breaching Trust*.

130. Ibid.

131. Google, "A New Approach to China," January 12, 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

132. Andrew Jacobs and Miguel Helft, "Google, Citing Attack, Threatens to Exit China," *New York Times*, January 12, 2010, http://www.nytimes.com/2010/01/13/world/asia/13beijing.html.

133. John Markoff, "Cyberattack on Google Said to Hit Password System," *New York Times*, April 19, 2010, http://www.nytimes.com/2010/04/20/technology/20google.html.

134. James Glanz and John Markoff, "Vast Hacking by a China Fearful of the Web," *New York Times*, December 4, 2010, http://www.nytimes.com/2010/12/05/world/asia/05wikileaks-china.html; Patrick Sawer, "Top Chinese Officials Ordered Attack on Google, Wikileaks Cables Claim," *The Telegraph*, December 4, 2010, http://www.telegraph.co.uk/news/worldnews/wikileaks/8181619/Top-Chinese-officials-ordered-attack-on-Google-Wikileaks-cables-claim.html.

135. Tania Branigan, "China Denies Involvement in Cyber Attacks on Google," *The Guardian*, January 25, 2010, http://www.guardian.co.uk/technology/2010/jan/25/china-denies-cyber-attacks-google.

136. Google, "An Update on China."

137. Nart Villeneuve, "Human Rights and Malware Attacks," Nart Villeneuve: Malware Explorer, July 29, 2010, http://www.nartv.org/2010/07/29/human-rights-and-malware-attacks.

138. Danny O'Brien, "That Nobel Invite? Mr. Malware Sent It," Committee to Protect Journalists, November 10, 2010, http://www.cpj.org/internet/2010/11/that-nobel-invite-mr-malware-sent-it.php.

139. "Tracking GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor, March 29, 2009, http://www.tracking-ghost.net.

140. "Warning on Fake Emails Targeting News Assistants," Foreign Correspondents' Club of China, September 21, 2009, http://www.fccchina.org/2009/09/21/warning-on-fake-emails-targeting-news-assistants.

141. Nart Villeneuve and Greg Walton, "Targeted Malware Attack on Foreign Correspondents Based in China," Nart Villeneuve: Malware Explorer, September 29, 2009, http://www.nartv.org/2009/09/28/targeted-malware-attack-on-foreign-correspondent%E2%80%99s-based-in-china.

142. "National Day Triggers Censorship, Cyber Attacks in China," Committee to Protect Journalists, September 22, 2009, http://cpj.org/2009/09/national-day-triggers-censorship-cyber-attacks-in.php.

143. Brett Winterford, "Optus Customers Hit by China DDoS Attack," *SC Magazine*, April 15, 2010, http://www.securecomputing.net.au/News/172229,optus-customers-hit-by-china-ddos-attack.aspx; Asher Moses, "Chinese Cyber Attackers Hit Optus," *Sydney Morning Herald*, April 15, 2010, http://www.smh.com.au/technology/security/chinese-cyber-attackers-hit-optus-20100415-sgm8.html.

144. "Chinese Hackers Suspected of DDoS Attacks Against Japan," The New New Internet, September 27, 2010, http://www.thenewnewinternet.com/2010/09/27/chinese-hackers-suspected-of-ddos-attacks-against-japan; "Japan Suspects Cyber Attacks Amid China Row: Media," Agence France-Press, September 17, 2010, http://www.google.com/hostednews/afp/article/ALeqM5jrJX2uRX7gxO3zPa_dO-rE0FPbnA.

145. Rajeev Deshpande and Vishwa Mohan, "Pakistan, China Hackers Tried to Deface CWG Sites," *Times of India*, October 16, 2010, http://articles.timesofindia.indiatimes.com/2010-10-16/india/28235934_1_cyber-security-hackers-official-agencies; Indrani Bagchi, "China Mounts Cyber Attacks on Indian Sites," *Times of India*, May 5, 2008, http://articles.timesofindia.indiatimes.com/2008-05-05/india/27760718_1_cyber-warfare-government-networks-china.

146. "S. Korean Government Website Hit by Cyber Attacks," Agence France-Presse, June 9, 2010, http://www.google.com/hostednews/afp/article/ALeqM5j-cLHwEp033Jo3lRnOJSFM9L3z6Q.

147. David Hencke, "Whitehall Plans New Cyber Security Centre to Deter Foreign Hackers," *The Guardian*, June 14, 2009, http://www.guardian.co.uk/technology/2009/jun/14/government-security-cyber-crime-hacking.

148. Sam Diaz, "Law Firm That Sued Chinese Government Reports Cyber Attack," ZDNet, January 13, 2010, http://www.zdnet.com/blog/btl/law-firm-that-sued-chinese-government-reports-cyber-attack/29533; Lolita Baldor, "Pentagon Takes Aim at China Cyber Threat," ABC News, August 19, 2010, http://abcnews.go.com/Politics/wireStory?id=11439149.

149. "China Cracks Down on Internet Pornography," *People's Daily,* December 30, 2010, http://english.people.com.cn/90001/90776/90882/7246889.html.

150. "China Cracks Down on Online Gambling, Arrests 3,430," Xinhua.

151. See Wang Chen, "Development and Administration of Our Country's Internet."

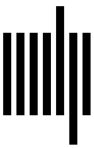
Access Contested

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