SECTION 2: EXTERNAL IMPLICATIONS OF CHINA'S INTERNET–RELATED ACTIVITIES

Introduction

China continues to engage in Internet-related activities that have broad implications for U.S. interests. In January, Google announced that a sweeping computer network exploitation campaign had compromised the firm's operations in China. Other accounts of malicious computer activity tied to China continue to surface. In several cases, Chinese telecommunications entities disrupted or otherwise impacted U.S. Internet traffic. Chinese authorities in 2010 also rolled out a series of new Internet and communication technology-related rules and regulations that promote domestic and undermine foreign firms. After a brief discussion of the cybersecurity environment, this section of the Commission's Report seeks to provide an overview of each of the aforementioned issues.

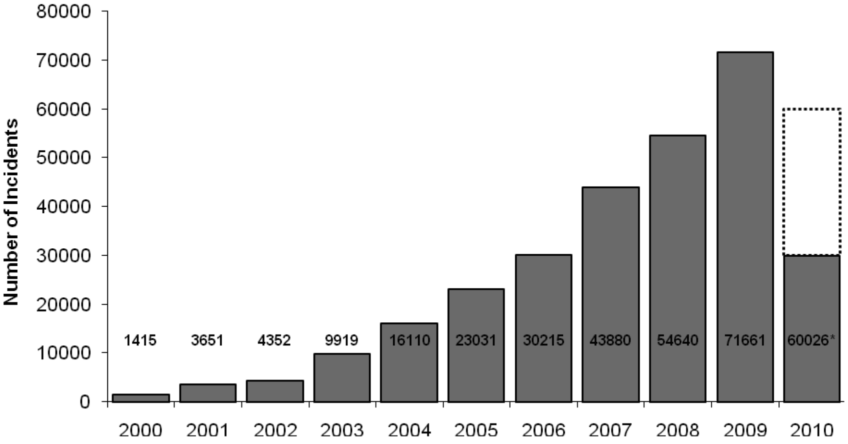
Trends in the Cybersecurity Environment

Discerning trends in the cybersecurity environment remains difficult given the problem's magnitude and other obstacles such as persistent underreporting of events. Even incidents of malicious cyber activity targeting the U.S. government cannot easily be quantified due to classification restrictions and fragmentary reporting. The Commission therefore uses Department of Defense figures as one indicator of trends in the threat environment. These figures are relevant because, as the Department of Defense has noted, China poses serious challenges with respect to network exploitation and attack. For example, in an annual report to Congress released in August, the Department of Defense stated that in recent years:

> *numerous computer systems around the world, including those owned by the U.S. government, continued to be the target of intrusions that appear to have originated within the [People's Republic of China]. These intrusions focused on exfiltratring information, some of which could be of strategic or military utility. The accesses and skills required for these intrusions are similar to those necessary to conduct computer network attacks. It remains unclear if these intrusions were conducted by, or with the endorsement of, the [People's Liberation Army] or other elements of the [People's Republic of China] government. However, developing capabilities for cyberwarfare is consistent with authoritative [People's Liberation Army] military writings.*[76]

Figure 1, below, demonstrates the volume of malicious computer activity against Department of Defense information systems over the past decade. Note that not all of the incidents depicted below specifically relate to China; the department has not made available that level of detail.

Figure 1: Department of Defense Reported Incidents of Malicious Cyber Activity, 2000–2009, with Projection for 2010



*This figure represents a projection based on incidents logged from January 1, 2010, to June 30, 2010. The projection assumes a constant rate of malicious activity throughout the year.

Sources: U.S.-China Economic and Security Review Commission, *Hearing on China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities*, testimony of Gary McAlum, May 20, 2008; Name withheld (staff member, U.S. Strategic Command), telephone interview with Commission staff, August 28, 2009; Name withheld (staff member, U.S. Cyber Command), e-mail interview with Commission staff, August 17, 2010.

If the rate of malicious activity from the first half of this year continues through the end of the year, 2010 could be the first year in a decade in which the quantity of logged events declines. This may or may not represent a decrease in the volume of attempts to penetrate defense and military networks. The Defense Department explained the lower figures as resulting from measures taken to mitigate threats before they reach the threshold that merits an incident log entry. Specifically, the department cited "greater visibility of threat activity, vulnerability, and ultimately risk by leaders at all levels across [the Department of Defense]" in addition to greater resources, enhanced perimeter defenses, and the establishment of U.S. Cyber Command.[77]

Operation "Aurora"

In early 2010, reports emerged of a large-scale cyber attack against Google's operations in China. In January, Google's chief legal officer announced that in mid-December 2009, Google had "detected a highly sophisticated and targeted attack on [its] corporate infrastructure originating from China that resulted in the theft of intellectual property,"[78] later reported to be the firm's invaluable source code.* [79] Evidence from the ensuing investigation suggested that another "primary goal of the attackers was accessing the [Google e-mail] accounts of Chinese human rights activists." [80] Investigators determined that the breech constituted one component of a larger computer network exploitation campaign targeting "a wide range of businesses—including the Internet, finance, technology, media, and chemical sectors," [81] with perhaps 33 or more other victim companies.† Computer security professionals now widely refer to this campaign as "Operation 'Aurora'" following revelations, based on technical indicators, that the perpetrators referred to the exploitation as such.[82]

The penetrations, combined with the Chinese government's increased restrictions on freedom of speech on the Internet, led Google "to conclude that [they] should review the feasibility of their business operations in China." [83] According to Google's official statement:

> *We have decided we are no longer willing to continue censoring our results on Google.cn, and so over the next few weeks we will be discussing with the Chinese government the basis on which we could operate an unfiltered search engine within the law, if at all. We recognize that this may well mean having to shut down Google.cn, and potentially our offices in China.*[84]

Google later announced that while it would maintain certain services in China, such as advertising, the firm would automatically redirect web search users from its mainland China site to its uncensored Hong Kong site.‡ Chinese authorities eventually deemed this interim solution unacceptable.[85] Ultimately, Google devised a system whereby users in mainland China would have to redirect themselves manually to the company's Hong Kong site by clicking a hyperlink.[86] This solution evidently sufficed for Chinese regulators, who subsequently renewed in early July Google's license to operate in China.[87] (For more information, see chap. 5, sec. 5, "China's Domestic Internet Censorship Practices.")

Google's initial announcement did not specifically attribute responsibility for the exploitation to the Chinese government. The company did, however, refer its users to a number of reports, including the Commission's 2009 Annual Report and Commission-sponsored research, that document the Chinese government's role in advanced computer exploitation schemes. As the Commission noted in its 2009 Report, this role varies from direct participation to some degree of sponsorship or simply acquiescence.[88] Other firms involved in the Aurora investigation provided more thorough details about those responsible. Security firm Secureworks, for example, determined that the malware used in the exploitation (described below) was written in Chinese and, at the time Google disclosed Operation Aurora, discussions about the code appeared only

* The term "source code" refers to the set of instructions that compose computer software programs.

† Google's initial announcement cited approximately 20 other victim firms. Reports since then have placed the number substantially higher. See Kelly Jackson Higgins, "Flaws in the 'Aurora' Attacks," *DarkReading*, January 25, 2010. *http://www.darkreading.com/database__security/security/attacks/showArticle.jhtml?articleID=222500010.*

‡ Google's mainland China site is Google.cn, and its Hong Kong site is Google.com.hk.

on Chinese-language websites.[89] Another security firm involved in the investigations, iDefense, went even further, stating that both the source Internet Protocol addresses and the servers used to facilitate the exploitation "correspond to a single foreign entity consisting either of agents of the Chinese state or proxies thereof."[90] Researchers further traced the penetration to two schools in China, one of which has ties to the Chinese military.[91]

Operation Aurora's perpetrators employed intelligence-gathering techniques and leveraged sophisticated exploits to compromise victims' systems. According to Google's information security manager, Operation Aurora specifically targeted certain Google employees in order to launch the exploitation. This effort included thorough reconnaissance of targeted Google employees such as the collection of data from their accounts on popular social networking sites like Twitter, Facebook, and LinkedIn. The perpetrators then, masquerading as an acquaintance, established a chat session with a targeted employee. In the course of this session, a Google employee clicked a hyperlink to an innocuous-looking photo-sharing website administered by Aurora's perpetrators,[92] reportedly hosted in Taiwan.[93] The site contained malicious code that automatically downloaded to the employee's system.[94]

This malware allowed the perpetrators to gain access to the victims' username and password information. With these credentials, the perpetrators:

> *set up a connection through a secure tunnel to the victim's machine and used the employee's credentials to gain access to other Google servers. . . . Once they gained super-user privileges, they installed a backdoor onto the server to view and steal files and attempt to stealthily gain access to other systems.*[95]

Once inside the systems, Aurora's perpetrators reportedly gained access to software-configuration management systems, which contain prized source code.[96] Remote activities in the exploitation, like the malicious photo-sharing site, appear to have been facilitated through servers outside China. A command-and-control server used by the perpetrators was also hosted in Taiwan.[97]

Other Examples of Chinese-tied Computer Network Exploitation

Other reports about Chinese-backed malicious cyber activity persisted throughout 2010. Quantifying the pervasiveness of such malicious activity remains challenging, but one analysis revealed that over 28 percent of all targeted phishing e-mails originate in China.*[98] Anecdotal reports about the success of these activities continue to surface, some with compelling links to the Chinese gov-

*"Phishing" is "an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent web site that appears legitimate. The user then may be asked to provide personal information such as account usernames and passwords that can further expose them to future compromises. Additionally, these fraudulent web sites may contain malicious code." U.S. Computer Emergency Readiness Team (U.S.-CERT), "Report Phishing." *http://www.us-cert.gov/nav/report_phishing.html*.

ernment.[99] One exceptionally well-documented study of a cyber intrusion against the Indian government deserves further discussion.

In April 2010, the Information Warfare Monitor and the Shadowserver Foundation* released a detailed report called "Shadows in the Cloud" that describes an elaborate computer exploitation campaign. According to the report, a China-based computer espionage network targeted primarily Indian diplomatic missions and government entities; Indian national security and defense groups; Indian academics and journalists focused on China; and other political institutions in India, as well as the Office of His Holiness, the Dalai Lama.[100] The network also compromised computers in at least 35 other countries, including the United States.†

Although the full extent of the exploitation remains unknown, the investigators determined that those responsible successfully obtained sensitive files, apparently belonging to the Indian government. Files removed included "one document that appears to be encrypted diplomatic correspondence, two documents marked "SECRET," six as "RESTRICTED," and five as "CONFIDENTIAL." These documents may constitute only a small portion of the files successfully exfiltrated in the course of this exploitation.[101] The report does not expressly link this malicious activity to the Chinese government. The report's authors, however, highlight the possibility of state involvement, citing the "obvious correlation to be drawn between the victims, the nature of the documents stolen, and the strategic interests of the Chinese state." The analysis also suggests the possibility that agents of the state carried out the exploitation, perhaps "either by sub-contract or privateering."[102]

The "Shadows in the Cloud" case study demonstrates at least three important emerging trends in malicious cyber activity related to China:

- *Increasingly sophisticated exploitations:* The penetration was not state of the art but seemed to demonstrate a higher level of sophistication than those reported in previous studies.[103] The perpetrators apparently did not discover their own previously unknown exploits but instead used vulnerabilities that had only recently been revealed by others. Furthermore, tools to leverage these vulnerabilities were not widely available at the time of the exploitation.[104]

- *Abuse of social media:* The people responsible for the penetrations exploited popular free web services—such as Twitter, Google Groups, Blogspot, Baidu Blogs, blog.com, and Yahoo! e-mail accounts—as part of the command-and-control infrastructure for their exploits.[105] Malicious actors can easily create ac-

* The Information Warfare Monitor (www.infowar-monitor.net) is a joint project between the Munk Centre for International Studies at the University of Toronto and the SecDev Group, a Canada-based computer security research and consulting organization. The Shadowserver Foundation (*www.shadowserver.org*) is a research organization comprised of information security professionals worldwide.

† Specifically, New York University and Honeywell, an organization involved in aerospace engineering and advanced materials research, seem to have been affected. These systems may have suffered "collateral compromise," wherein malicious software compromises unintended nodes (e.g., by users remotely accessing targeted systems). Information Warfare Monitor and Shadowserver Foundation, "Shadows in the Cloud: Investigating Cyber Espionage 2.0," April 6, 2010, pp. 28, 43. *http://shadows-in-the-cloud.net*.

counts at these sites, and traffic between them and the victims' computers looks innocuous to firewalls and network administrators.

- *Nexus with criminal software and techniques:* Some of the command-and-control servers used in this case have known ties to other malware operations.[106] These may be used for myriad other purposes, including criminal activities such as identity theft. The report's authors postulate that "political espionage networks may be deliberately exploiting criminal kits, techniques, and networks both to distance themselves from attribution and to strategically cultivate a climate of uncertainty."[107] According to the report, "murky relationships" between the Chinese state and the Chinese criminal underground mean that data gathered by the latter may end up in the "possession of some entity of the Chinese government."[108]

Internet Traffic Manipulation

In early 2010, two incidents demonstrated that China has the ability to substantially manipulate data flows on the Internet. First, for several days in March, China's Internet controls censored U.S. Internet users. Second, in April, a Chinese Internet service provider briefly hijacked a large volume of Internet traffic. Computer security researchers observed both incidents but were not able to say conclusively whether the actions were intentional. Nonetheless, each incident demonstrates a capability that could possibly be used for malicious purposes.

Spillover of China's Internet Censorship Activities

In March 2010, reports surfaced that China's Internet censorship regime (known colloquially as "the Great Firewall")[*] temporarily affected Internet users outside of China.[†] Specifically, certain users in Chile and the United States who tried to access popular social media sites, including Twitter, YouTube, and Facebook, were denied access by being redirected to incorrect or nonexistent servers.[109] This incident, which relates to the Internet "Domain Name System" (see text box below), helps illustrate the implications of China's effort to impose "localized" restrictions to something as inherently global in scope as the Internet.

[*] The term "the Great Firewall" initially referenced China's early attempts to block Chinese Internet users' access to foreign websites. Another term, "the Golden Shield," references China's comprehensive efforts to censor Internet content. The former term is widely used in place of the latter. For more information about "the Golden Shield," see U.S.-China Economic and Security Review Commission, *2008 Report to Congress* (Washington, DC: U.S. Government Printing Office, 2008), pp 297–8; and Greg Walton, "China's Golden Shield" (Montreal, Canada: International Centre for Human Rights and Democratic Development, 2001), especially pp 14–7. *http://www.dd-rd.ca/site/__PDF/publications/globalization/CGS__ENG.PDF*.

[†] This is not the first time an incident like this has occurred. See, for example, Declan McCullagh, "How Pakistan knocked YouTube offline (and how to make sure it never happens again)," *cnet.com*, February 25, 2008. *http://news.cnet.com/8301–10784__3–9878655–7.html#ixzz0zcR1AWUS*.

Domain Name System Susceptible to Tampering

The Internet is underpinned by a system of unique numerical identifiers called Internet Protocol addresses (for example, 74.125.227.50). Recognizing that many long strings of numbers would be difficult for users to remember, the Internet's architects developed the "Domain Name System," which allows Internet Protocol addresses to be assigned unique domain names (for example, www.uscc.gov). The system is facilitated by Domain Name Servers that contain and distribute lists of Internet Protocol address and their associated domain names. (A frequently cited analogy here is that an Internet Protocol address is like a phone number, a domain name is like a person's name, and a Domain Name Server is like a phone book that allows one to look up a phone number based on a name.)

When a computer user attempts to visit a website by typing a domain name into a web browser, the Domain Name System activates and requests that a Domain Name Server look up that domain name's Internet Protocol address. The Domain Name Server relays the information, which allows the browser to locate the website on the Internet and establish a connection. The process is automated and extremely rapid.

Thirteen primary (or "root") Domain Name Servers form the backbone of the Internet. These servers maintain numerous physical clone-like iterations,[*] implemented to accommodate the growth in Internet use within the bounds of existing protocols.[110] Trusted sources update and maintain these root servers and iterations, but each physically exists within a country, and many serve users outside that country. Therefore, data going to and from these servers must traverse local network infrastructure and, by extension, be subjected to domestic Internet control policies that may instruct the servers to send back incorrect responses. This can ultimately affect foreign Internet users' ability to connect to the websites they intend to visit.[111]

Starting on March 24, 2010, when certain Internet users in the United States and Chile attempted to connect to popular social networking websites, their computers requested routine Internet Protocol information, and a Beijing-based Domain Name Server (a clone-like iteration of a Swedish root server)[†] replied with faulty responses.[‡] As a result, these users were directed to incorrect servers, as if the users were trying to access restricted content from behind China's Great Firewall. These conditions persisted in some cases for several days before the administrators of the Sweden-based root server temporarily disabled requests to their Beijing server "clone."[112] The administrators eventually brought the server

[*] These iterations are otherwise referred to as "instances."

[†] The root server involved in this instance is administered by the firm Netnod. See "One of 13," *Netnod.se* (undated). *http://www.netnod.se/dns_root_nameserver.shtml#*.

[‡] Although responses ostensibly came from the Swedish root server iteration in Beijing, the actual response may have been generated by a component of China's Great Firewall.

instance back online, but computer researchers identified the same problem again in June.[113]

These incidents do not appear to be a deliberate act of cross-border censorship from China. Rather, because of vulnerabilities in the Internet's architecture, the faulty information likely resulted from an accidental "leak" of conditions intended only for a Chinese audience. Nonetheless, these events demonstrate the disregard networked systems have for national borders and illustrate ripple effects from China's elaborate censorship activities.

Interception of Internet Traffic

For a brief period in April 2010, a state-owned Chinese telecommunications firm "hijacked" massive volumes of Internet traffic.* [114] Evidence related to this incident does not clearly indicate whether it was perpetrated intentionally and, if so, to what ends. However, computer security researchers have noted that the capability could enable severe malicious activities.[115]

Internet Routing Processes Susceptible to Manipulation

Internet browsing activities often employ numerous servers to facilitate the exchange of data. This process typically relies on trust-based transactions between each server involved. In order for a server to determine where to route data, the server will consult a "routing table" that maps paths from one point on the Internet to another. Servers issue these routing tables to "advertise" (that is, notify other servers) that they can provide an efficient path between servers.

If a computer user in California, for example, seeks to visit a website hosted in Texas, the data would likely make several "hops" (that is, transit multiple servers) along the way. Data are supposed to travel along the most efficient route. However, Internet infrastructure does not necessarily correlate to the geographical world in a predictable way, so it would not be completely unusual for data to transit a server physically located in Georgia, or some other somewhat removed location.

This process, however, is susceptible to manipulation. If a server in an out-of-the-way location, such as China, advertised a route that claimed to be the most efficient path to transfer data from California to Texas, other servers in the transaction might well pass those data across the Pacific for a hop in Beijing before the data ultimately reached their intended destination. While in Beijing, those data could conceivably be monitored, censored, or replaced with other data. This could take place quickly enough to go unnoticed by the computer user.

*This is not the first time an incident like this has occurred. See, for example, Todd Underwood, "Internet-Wide Catastrophe—Last Year," *Renesys blog*, December 24, 2005. *http://www.renesys.com/blog/2005/12/internetwide__nearcatastrophela.shtml*. By way of comparison, the incident referenced therein affected a much greater volume of Internet traffic than the incident described above.

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.* Other servers around the world quickly adopted these paths, routing all traffic to about 15 percent of the Internet's destinations through servers located in China. This incident affected traffic to and from U.S. government (".gov") and military (".mil") sites, including those for the Senate, the army, the navy, the marine corps, the air force, the office of secretary of Defense, the National Aeronautics and Space Administration, the Department of Commerce, the National Oceanic and Atmospheric Administration, and many others. Certain commercial websites were also affected, such as those for Dell, Yahoo!, Microsoft, and IBM.[116]

Although the Commission has no way to determine what, if anything, Chinese telecommunications firms did to the hijacked data, incidents of this nature could have a number of serious implications. This level of access could enable surveillance of specific users or sites.† It could disrupt a data transaction and prevent a user from establishing a connection with a site. It could even allow a diversion of data to somewhere that the user did not intend (for example, to a "spoofed" site). Arbor Networks Chief Security Officer Danny McPherson has explained that the volume of affected data here could have been intended to conceal one targeted attack.[117] Perhaps most disconcertingly, as a result of the diffusion of Internet security certification authorities,‡ control over diverted data could possibly allow a telecommunications firm to compromise the integrity of supposedly secure encrypted sessions.§

New Government Regulations

The Chinese government in 2010 proposed and, in some cases, implemented information and communication technology-related laws and regulations with broad implications for China, the United States, and the rest of the world. These conventions, described below, directly affect norms related to computer security.

Encryption Information Provision

In May 2010, long-anticipated Chinese regulations requiring high-technology foreign firms to disclose proprietary information about their products came into effect. After a year of discussions, China's General Administration of Quality Supervision, Inspection and Quarantine officially proposed in 2008 a set of rules that would

* This type of attack is referred to alternatively as "IP [Internet Protocol] hijacking" or "prefix hijacking." Note that the erroneous data appear to have originated at a smaller Internet Service Provider, IDC China Telecommunication, and were subsequently propagated by China Telecom.

† There are unconfirmed reports that Chinese Internet Service Providers have engaged in such activities. See, for example, Oiwan Lam, "China: ISP level Gmail phishing," *Global Voices Online*, August 11, 2010. *http://advocacy.globalvoicesonline.org/2010/08/11/china-isp-level-gmail-phishing/*.

‡ For a brief explanation of the vulnerabilities associated with the current Internet certificate authority regime, see Danny O'Brien, "The Internet's Secret Back Door," *Slate*, August 27, 2010. *http://www.slate.com/id/2265204/*. For a detailed description that relates specifically to China, see Seth Schoen, "Behind the Padlock Icon: Certificate Authorities' Mysterious Role in Internet Security," in *China Rights Forum no. 2 (2010), "China's Internet": Staking Digital Ground* (New York: Human Rights in China). *http://www.hrichina.org/public/contents/article?revision__id=175292&item__id=175290*.

§ This is referred to as a "man in the middle" attack. Dmitri Alperovitch (vice president, Threat Research, McAfee, Inc.), briefing to Commission staff, August 25, 2010.

compel makers of 13 categories of technology products, including intrusion detection systems, secure network routers, and certain firewall systems,[118] to disclose sensitive cryptography information to Chinese authorities by May 2009 in order to be able to sell these products to anyone in China. Pushback from U.S. and European institutions reportedly convinced Chinese authorities at least to delay the implementation of these regulations by one year and to scale back requirements so as to cover only products procured by Chinese government entities.[119]

These revised regulations require firms to turn over "encryption algorithms, software source code and design specifications" to "government-connected testing laboratories,"[120] namely, the Certification and Accreditation Administration of China under China's General Administration of Quality Supervision, Inspection and Quarantine.[121] This presents several problems for U.S. high-technology industries:

- Required information constitutes sensitive trade secrets,[122] and U.S. trade groups report that the "government panels that would review foreign products include employees of rival Chinese companies."[123]
- Compliance with the regulations would undermine other potential buyers' trust in the products' integrity.
- Access to the details of such sensitive encryption information would assist the Chinese government's censorship regime[124] and likely boost its capacity to conduct computer network operations.

Taken together, these issues present a trade barrier that, perhaps by design, advantages Chinese firms over foreign competition.[125] According to a trade industry representative, no foreign firms had submitted to the certification process as of June 2010.[126]

Multilevel Protection Scheme

Chinese authorities may also implement more drastic regulations requiring foreign high-technology firms to provide sensitive details about proprietary products in order to provide goods for any of China's "strategic information systems." This sweeping category includes any system related to:

> *state affairs (party and government), finance, banking, tax administration, customs, audit administration, industry and commerce, social services, energy, transportation, national defense industry, and other information systems that are related to the national economy and peoples' livelihood including education, state science and technology institutions, public telecommunications, television broadcasting and other basic information networks.*[127]

Should the regulations come to fruition, foreign firms would need to submit for evaluation thorough information about components for any these systems. According to Dean Garfield, president and chief executive officer of the Information Technology Industry Council, such regulations would levy "completely unworkable testing requirements on nearly all high-tech products" to be sold in

China.[128] In order to safeguard intellectual property, most foreign firms would be unwilling to submit to such a process.[129] The regulations, according to the Associated Press, are "consistent with [Beijing's] efforts to build up Chinese technology industries by shielding them from competition and pressing global rivals to hand over know-how."[130]

Implications for the United States

China's actions with respect to the Internet in 2010 have several important implications for the United States. The "Aurora" campaign illustrates that actors within China, and with possible ties to the Chinese government, have used computer exploitation techniques to target the intellectual property of numerous American firms operating in China. To the extent that these penetrations are successful, they undermine the competitiveness of American industry. Chinese actors reportedly used similar, if less sophisticated, techniques recently to target the Indian government. A wide body of literature, including a notable Department of Defense report to Congress in 2010, suggests that actors within China target U.S. government institutions in a similar manner.

Several incidents in early 2010 demonstrate that, regardless of whether Chinese actors actually intended to manipulate U.S. and other foreign Internet traffic, China's Internet engineers have the capability to do so. Although China is by no means alone in this regard, persistent reports of that nation's use of malicious computer activities raise questions about whether China might seek intentionally to leverage these abilities to assert some level of control over the Internet, even for a brief period. Any attempt to do this would likely be counter to the interests of the United States and other countries. At the very least, these incidents demonstrate the inherent vulnerabilities in the Internet's architecture that can affect all Internet users and beneficiaries at home and abroad.

Finally, the Chinese government in 2010 moved to place onerous restrictions on U.S. and other foreign firms that seek to conduct business in China. In one instance, new regulations may force companies to provide key information to Chinese authorities that can jeopardize the security of the firms' products. In another case, proposed rules would create a dilemma for foreign firms by forcing them to choose either to compromise their products' security and intellectual property or else lose access to large portions of the Chinese market.

Conclusions

- China's government, the Chinese Communist Party, and Chinese individuals and organizations continue to hack into American computer systems and networks as well as those of foreign entities and governments. The methods used during these activities are generally more sophisticated than techniques used in previous exploitations. Those responsible for these acts increasingly leverage social networking tools as well as malicious software tied to the criminal underground.

- Recent high-profile, China-based computer exploitations continue to suggest some level of state support. Indicators include the massive scale of these exploitations and the extensive intelligence and reconnaissance components.
- In 2010, China's "Great Firewall" affected select U.S. Internet users, and a state-owned Chinese Internet Service Provider "hijacked," or inappropriately gained access to, select U.S. Internet traffic. Other nations were also affected in these incidents.
- Chinese authorities are tightening restrictions on foreign high-technology firms' ability to operate in China. Firms that fail to comply with the new regulations may be prohibited from doing business in Chinese markets. Firms that choose to comply may risk exposing their security measures or even their intellectual property to Chinese competitors.