Chinese Computer Games

Keeping Safe in Cyberspace

Adam Segai

In March 2011, the U.S. computer security company **rsa** announced that hackers had gained access to security tokens it produces that let millions of government and private-sector employees, including those of defense contractors such as Lockheed Martin, connect remotely to their ofiice computers. Just five months later, the antivirus software company McAfee issued a report claiming that a group of hackers had broken into the networks of 71 governments, companies, and international organizations. These attacks and the many others like them have robbed companies and governments of priceless intellectual property and crucial military secrets. And although officials have until recently been reluctant to name the culprit, most experts agree that the majority of the attacks originated in China.

In response, analysts and policymakers have suggested that Washington and Beijing work toward some form of détente, a broad-based agreement about how countries should behave in cyberspace that might eventually turn into a more formal code of conduct. Proponents argue that the two sides' long-term interests are aligned, that one day China will be as dependent on digital infrastructure for economic and military power as the United States is today. As Major General Jonathan Shaw, the head of the British military's Defence Cyber Operations Group, has said, Chinas "dependence on cyber is increasing, the amount of cyber crime taking place inside that society is huge, and the impact on their economic growth and their internai stability is also going to be huge.... Theres more common ground than people might suggest."

But a grand bargain wont be struck anytime soon. Both China and the United States consider operations in cyberspace a valuable tool, and China currently has litde interest in cracking down on hackers, who pose a constant threat to its economic and military rivais. This doesnt mean that there is nothing Washington can do, however. Instead of engaging in a futile effort to achieve some equivalent in cyberspace to nuclear détente, the

Adam Segal is Ira **A.** Lipman Sênior Fellow for Counterterrorism and National Security Studies at the Council on Foreign Relations.

U.S. government should pursue a wide-ranging approach to protecting American interests that includes working closely with other Internet powers and raising the costs of hacking. Cyberattacks are less like on-off switches and more like dials. The goal of U.S. policy should be to turn them down.

INTERNETIDEOLOGY

Washington and Beijing wont agree to a broad treaty governing cyberspace mainly because they hold fundamentally incompatible views on the Internet and society. The U.S. government, in its International Strategy for Cyberspace, says that it will promote a digital infrastructure that is "open, interoperable, secure and reliable" while supporting international commerce, strengthening security, and fostering free expression. It has championed an approach to the Internet that lends influence to commercial interests and nonstate actors, opposing calls from other countries for more authority to be given to state-centric organizations such as the **UN** or the International Telecommunication Union.

China, by contrast, regulates the Internet strictly, and although the country may share an interest in security and global commerce, it defines these concepts differently than the United States does. It is not that China has nothing to fear from cyberattacks: the country suffered close to 500,000 such attacks in 2011, with nearly 15 percent of them appearing to come from computers in the United States. Yet this vulnerability has not brought the two sides together: whereas Americans talk of promoting "cybersecurity," a fairly narrow term that implies protecting communications and other criticai networks, Chinese officials like to talk about "information security," a much broader concept that also includes regulating content.

Chinas stance is a matter of legitimacy and political control. Chinese policymakers, unlike their American equivalents, fear that communications technologies could foment instability. Beijing views attempts by the U.S. State Department and digital activists to overcome Internet filters as just as threatening as hackers trying to penetrate an electric power grid. Thus, in June 2011, for example, responding to reports that the United States was developing an "Internet in a suitcase" and other firewall-circumvention technologies, an editorial in the state-run *Peoples Daily* contended, "The U.S. State Department has carefully framed its support of such projects as promoting free speech and human rights, but it is clear that the policy is aimed at destabilizing national governments."

Chinas obsessive drive for indigenous innovation explains its opposition to global standards for both the technologies that keep the Internet operating and those that allow different types of devices to communicate online. As Chinese technology firms expand abroad, they will need an interoperable Internet as badly as any other international businesses, and they would benefit from the economies of scale and lower prices that global standards allow. For this reason, the Chinese computer manufacturer Lenovo helped found the Digital Living Network Alliance, a trade group that seeks to promote interoperability among consumer electronics. But the Chinese government views such attempts at unity as an effort to lock the rest of the world into technology standards dominated by U.S. companies.

As part of its plan to reduce its technological dependence on the West, China has proposed technology standards of its own.

CHINA'S CHOICES

In February **2011,** weeks after Google publicly announced that hackers had tried to steal its sensitive computer codes, security experts traced the attacks back to Shanghai Jiao Tong University and a vocational school in Shandong Province. Both schools denied any involvement, and it is possible that their computers were hijacked by others, but U.S. intelligence officials claim that **20** groups associated with the Peoples Liberation Army and several Chinese universities are responsible for the majority of the attacks on Google, **rsa**, and other U.S. targets. Attributing responsibility is often hard. Some hackers drift in and out of Beijings orbit over time, whereas others are independent criminais with no links to the state. Overall, however, much of the hacking originating in China can be classified as government-sponsored or government-tolerated. Beijing sees such hacking as a good way to eke out economic and military advantage—which creates another obstacle in the path of a U.S.-Chinese agreement.

Chinas motivation in this area is not mysterious. The government desperately wants its economy to move up the value chain, to become a source of innovation rather than just a producer of cheap goods. To make that happen, it has employed the traditional instruments of science and technology policy, but it has also relied on industrial espionage directed at foreign high-tech companies. Hackers have reportedly targeted the negotiation strategies, business plans, and financial information of foreign energy and banking companies, too.

Beijing also tolerates cyberattacks out of concern for internai stability. In some cases, the government appears to direct attacks at its domestic enemies, such as the Falun Gong movement, whereas in others, it seems to encourage political hacking as a sort of release valve for frustrated citizens. During the late 1990s, for example, the government called on "patriotic hackers" to vandalize U.S. government Web sites in response to the U.S. military's accidental bombing of the Chinese embassy in Belgrade and the collision of a U.S. surveillance plane with a Chinese fighter jet. The Chinese government's attitude began to shift by the middle of the next decade, when prominent editoriais and high-profile arrests signaled that it was starting to view independent hacking as unwanted interference in foreign relations.

But Beijing has continued to allow such hacking during tense times. After the human rights activist Liu Xiaobo won the Nobel Peace Prize in October **2010,** for example, Chinese hackers defaced the Nobel organizations Web site, and after Vietnam asserted sovereignty over contested islands in June **2011,** they targeted Vietnamese sites. In both cases, the government turned a blind eye to the illegal hacking in deference to the populations nationalist impulses.

Chinas military also finds value in cyberattacks, which would be an integral part of any Chinese military action in the region. Much of the Chinese open-source literature on information warfare suggests that the military, in the event of a conflict, would conduct quick cyberattacks on its

adversarys command-and-control centers. Although the Peoples Liberation Army has recruited some high-profile hackers and set up "cyber-militias" at technology companies, the military would probably stop short of rallying outside hackers during a conflict, since doing so would cede control to them over picking targets and make it difficult to stop escalation.

Cyberattacks also help China send a message of deterrence: that a limited regional conflict might not stay that way. Chinese intrusions into U.S. power grids or other criticai infrastructure, especially when evidence is left behind, act as a warning that the U.S. homeland may not be immune to attack in the case of a conflict over Taiwan or the South China Sea.

PLAYING DEFENSE

Given the obstacles standing in the way of a grand bargain, Washington should focus on improving its defenses, raising the costs to Chinese hackers, and cooperating with other Internet powers. The centerpiece of any comprehensive strategy should be cooperating with the private sector to defend the country against computer attacks, especially when they target intellectual property. The U.S. government has already begun to make progress in this area; since May 2011, for example, the National Security Agency has shared classified intelligence on cyberthreats with 20 defense contractors and their Internet service providers. Although the Pentagon is considering expanding the project to even more defense companies and to criticai infrastructure sectors, such as electricity generators and power grids, for the time being the rest of the U.S. private sector remains on its own.

This is a problem, since the rash of successful attacks over the last five years suggests that U.S. firms need ali the help they can get against their highly capable Chinese foes. A mix of government regulations and incentives could push American companies to spend more on security But since attackers will breach defenses anyway, these companies need to do a better job of protecting intellectual property and trade secrets. They should take inventory of ali data stored digitally, remove criticai information from vulnerable servers, limit the time hackers are able to spend on networks by deploying effective intrusion systems, and lure attackers into so-called honeypots, decoy computers sometimes baited with fake data.

The United States should also seek to raise the costs of cyber-espionage through trade policy. As the defense consultant James Farwell has argued, Chinas tight control over the Internet suggests that it has the ability, and thus the legal responsibility, to stop attacks coming from its soil. The United States could make the case to the World Trade Organization that Chinese intellectual property theft violates Chinas **WTO** obligations. A ruling against Beijing would allow Washington to label China a pirate state, collect damages or apply trade sanctions, and help mobilize international support for pressure on China. Even without a **WTO** ruling, the United States might consider levying economic sanctions on China and placing travei restrictions on cyber-spies.

More aggressive measures may be in order but for now are legally and strategically difficult. The United States'

strategy in cyberspace has always been about more than just defense; as Chinese officials are quick to note, it was the United States that first set up a cyber command and thus, in their view, militarized cyberspace. Although U.S. defense officials have hesitated to talk about how they would attack other countries' networks, this reticence is hardly working. (Consider this headline that ran in the *PLA Daily* on July 16, 2011: "The Offensive Posture of the U.S. 'Strategy for Operating in Cyberspace' is Difficult to Conceal.") It is time to give up the act. Chinese analysts are no doubt aware that Washington is planning offensive operations, and they probably believe that it is behind other attacks—in particular Stuxnet, the computer worm credited with slowing down Irans uranium-enrichment program at its facility in Natanz.

Last March, the Obama administration considered using cyberattacks to disable Libyas air defense systems but chose not to for various legal and strategic reasons. The legal issues of responding to Chinese intrusions are even more complicated, since espionage does not violate international law and so does not justify large-scale attacks in response. In other words, the United States cannot turn off the lights in Shanghai because terabytes of data were stolen in Washington. Self-defense is allowed, but the authority under which the U.S. military can exploit foreign networks in defense of private industry is unclear.

Now that U.S. intelligence officials have identified the specific groups behind some of the attacks the country has faced, the United States could target individual computers and personal or financial data. The U.S. government may have already hired private companies to conduct offensive operations in cyberspace. Several prominent security researchers have admitted selling previously undiscovered software vulnerabilities known as "zero-days" to defense contractors, who may use these exploits themselves to penetrate Chinese networks or may pass them on to U.S. government agencies. The benefits of contracting out hacking, however, must be weighed against the operational and legal issues that private but government-sponsored attacks would raise, as well as the damage they could do to diplomatic efforts to convince Beijing to rein in its own patriotic hackers.

CREATING CONSENSUS

Even as the U.S. government attempts to defend itself against Chinese hackers, it must also work directly with the Chinese government to try to solve the problem. It has taken some preliminary steps in this direction. In May 2011, for the first time, the U.S.-China Strategic and Economic Dialogue included discussions regarding cyberspace; such issues were also on the agenda in July when Admirai Mike Mullen, chairman of the Joint Chiefs of Staff, met with General Chen Bingde, chief of the general staff of the People's Liberation Army. U.S and Chinese officials, along with experts from think tanks, have also been privately discussing these issues in a parallel set of track-two meetings.

Yet these official bilateral discussions are not expansive enough. Diplomats should take their cues from the planned

dialogue on cyberspace between the United States and Rússia, which is to include discussions about how each side's military views the Internet and an effort to establish a hot line that could be used during a cybersecurity crisis. Washington and Beijing need to have a clear communications channel in case of emergency. To build trust over the longer term, the two sides should also discuss some common threats, such as the potential for terrorist attacks on power grids.

Negotiations on these topics are likely to be protracted and held hostage to the overall state of the U.S.-Chinese relationship. In the past, military-to-military discussions have often been canceled by one side or the other to signal displeasure. Confidence-building measures that reduce mutual irritants, such as a recent joint effort to reduce junk e-mail, are more likely to be sustainable. In the same vein, as Gu Jian, the deputy head of network security for Chinas Ministry of Public Security, has suggested, the two sides could act against activity that is illegal in both countries. For example, they might shut down Web sites that attempt to trick users into handing over their bank account numbers.

Perhaps more promising than these incipient discussions with China is the U.S. government's effort to work with allies and other like-minded countries to define international norms about cyberspace. It is especially important to find common ground with rising powers such as Brazil, índia, Indonésia, and South África. Agreements with them about acceptable behavior would ratchet up the pressure on China,

which rarely prefers to remain an international outlier.

Companies and governments should also call out China for its hacking crimes in the hope that this will embarrass the government into ending them. Google used this strategy when it announced in January 2010 that it had been the victim of sophisticated attacks and would no longer operate its search engine in China, as did the U.S. State Department in April 2011, when it pressed the Chinese Foreign Ministry about attacks against a Web site supporting the dissident artist Ai Weiwei. Naming and shaming, besides highlighting the fact that Beijing is violating international norms, may also embolden those within the Chinese government who worry that hackings long-term costs—in particular, the damage it does to relations with Japan, Europe, and the United States—outweigh its short-term gains.

The U.S. government should also keep lending a hand to other countries so that they can fight cybercrime on their own, especially those developing countries that lack the relevant expertise. In July 2011, for instance, the State Department sponsored a conference for six East African countries on investigating and prosecuting cross-border cybercrime. If the United States does not help such governments, China would be happy to do so. Yet along with its expertise, Beijing would seek to export its own attitudes about the Internet, values that could tempt these governments to adopt more totalitarian approaches to cyberspace and join China at the **UN** in its push to limit the role of nongovernmental groups in Internet governance.

Assembling an international consensus on norms about cyberspace, however, is a strategy that will probably take a long time to pay off, if it ever does. There is little the United States can do to alter China's conception of cyberspace, a vision it is actively promoting abroad. With a growing population of 500 million Internet users, it is easy to see why the Chinese believe that the future of cyberspace belongs to them. In the meantime, the most pressing tasks for the United States are to raise the costs incurred by Chinese hackers and to improve the security of networks at home. Yet U.S. officials should be realistic: Chinese-based cyberattacks will not disappear anytime soon.®

Fonte: Foreign affairs, New York, v. 91, n. 2, p. 14-20 March / April 2012.