Cyberwarfare: Western and Chinese Allegations

Nir Kshetri, *University of North Carolina–Greensboro*

Allegations and counter-allegations have been widespread in the US-China discourse on the governance of cyberspace. According to Joel Brenner, a previous US counterintelligence chief, in the last decade, over 2,000 companies, universities, and government agencies in the US have experienced cyberattacks originating from China.[1] Furthermore, US intelligence officials and private-sector security professionals and analysts have argued that China-originated cyberattacks, such as IP and trade secret thefts, will result in substantial economic damage in the long term.[2] Such attacks prompted Kevin Mandia, CEO of the security firm Mandiant, to suggest that "cybercrime [will be] the biggest security issue corporations will face in 2022."[2]

Here, I review some of the allegations of China-based cyberattacks to shed light on today's cyber Cold war and what it means for tomorrow's cybersecurity efforts.

Sophisticated Attacks

Although no reliable, hard statistics are available on the number of hackers in China and other countries, nonscientific estimates suggest there's a substantial hacker population in China. A US security analyst, monitoring various hacker websites, found that 380,000 hackers logged into Chinese hacking sites over a period of several days.[3] According to some Western analysts, Chinese hacking groups consist of independent criminals, patriotic hackers focusing on political targets, intelligence-oriented hackers, and other groups believed to work with the government.[4]

Most professional cybercriminals prefer to steal financial information, because it can be converted into cash more easily than other data (such as trade secrets and IP). Some frauds involving online theft of financial credentials and bank accounts have been traced to China.[5] However, analysts have noted that a larger proportion of attacks originating from China are advanced persistent threats (APTs), aimed at extracting high-value IP.[6] A theory among some analysts is that if profit-motivated hackers break into foreign governments' networks, which might lack monetary value, the hackers might then trade with state-sponsored hackers, facilitated by "information broker" middlemen.[7]

Furthermore, according to media reports,[8] China-originated cyberattacks are highly targeted, often tied to specific high-value targets. According to analysts, these cyberattacks employ sophisticated means to gain access into a network, compromising data for an extended period of time as the attacks remain undetected.

For example, in 2005, a Trojan horse code named Myfip reportedly sent sensitive documents such as computer-aided design and computer-aided manufacturing files, containing mechanical designs, electronic circuit board schematics, and layouts from networks of US-based companies to Tianjin, China.[3] Likewise, a 2009 report of Google noted that the Aurora attacks on its networks were part of a larger China-based operation that infiltrated the infrastructures of at least 34 other large companies.[1,9] Other reports have indicated that the Aurora hackers attacked networks of more than 100 companies.[10] In February 2011, McAfee researchers published a report indicating that hackers operating from China

 Published by the IEEE Computer Society

Editor's Introduction: Confronting Cyberattacks

Cyberattacks originate globally, and every organization is a potential target. By attacking systems, hackers are accessing organizational information, trade secrets, and confidential strategies, thus creating enormous losses for the overall economy. Attribution of cyberattacks is very difficult, because counter intelligence techniques can be used on the Internet—such as spoofing source IPs, using proxy servers, using botnets to deliver attacks out of other locations, using keyboard maps of different languages, and other methods. Furthermore, it's often difficult to differentiate between state-sponsored and individual-initiated attacks. Nevertheless, nation state actors will likely be more successful, because they often have the time and resources to breach the security of organizations with many different capabilities.

Most threat actors employ similar types of exploitations or tools, such as social-engineered Trojans, malwares, phishing attacks, network-traveling worms or viruses, or other advanced persistent threats. Given they're using similar tools and capabilities, it's important to focus on effective security controls that protect against all of these attack capabilities. Organizations shouldn't be distracted by the source of the exploitation. Instead, they should invest time and money into defending against the threats they're apt to confront.

Since cyberattacks have become more targeted and persistent, and attack tools have gotten more sophisticated and specialized, a multilayered solution to defend against these advanced threats is needed. Single-layered mechanisms alone can't adequately defend against today's attacks. Comprehensive solutions that use some combination of scanning, heuristic, behavioral, emulation, and sandboxing technologies are necessary to reduce vulnerability and minimize risk. For instance, the malware can be handled by a number of technologies at the network layer and at the desktop endpoint. SQL injection can be addressed with a combination of vulnerability scanning, intrusion prevention systems, and Web application firewalls.

Reports in recent years have highlighted China, among other countries, as a cyberattack actor. However, again, it's difficult to prove which attacks are state-sponsored attacks. Furthermore, the country of origin isn't as important as the protection mechanisms that must be in place. The fact is, most organizations face similar threats and should be doing their utmost to counteract those risks. Organizations should adopt an in-depth defense approach to combat threats from any location and not focus on the country of origin. Threats come from everywhere, so organizations must be prepared to address them.

— Simon Liu, US National Agricultural Library

stole information related to operations, financing, and bidding from oil companies based in the US, Taiwan, Greece, and Kazakhstan.[11]

Counter Allegations and Responses

The Chinese government often blames foreign hackers for cyberattacks targeting China. For example, Gu Jian of the Chinese Ministry of Public Security said that over 200 Chinese government websites experience cyberattacks on a daily basis, most of which are foreign-originated.[12] According to the Information Office of the State Council, over one million IP addresses in China were controlled and 42,000 websites were hijacked by foreign hackers in 2009.[13] Likewise, a report from China's Computer Emergency Response Team noted that the country's 8.9 million computers were attacked by 47,000 foreign IP addresses, and foreign hackers compromised 1,116 Chinese websites in 2011.[14] The report also observed that 96 percent of phishing websites targeting Chinese banks in 2011 were foreign-originated.

Chinese officials argue that they should be praised, not criticized, for taking measures to control cybercrime and for collaborating with other countries. Undoubtedly, some progress has been made in fighting cybercrime. China took the first major step toward criminalizing cybercrime in February 2009 by including computer crime in its Criminal Law. The punishment for hacking includes up to seven years in prison. Jian noted that the Chinese police shut down over 80 cybercriminal gangs from February 2009 to October 2010.[12]

China has also engaged in international collaborations to fight cybercrime. The spokesperson for the Chinese Embassy in the UK, Dai Qingli, wrote a letter to the editor of the *Financial Times*, noting that Chinese police helped 41 countries investigate 721 cybercrime cases between 2004 and 2010. She also said that China had interpolice cooperation with more than 30 countries.[15]

Some Chinese officials are also responding to Western allegations of Chinese-based cybercrime with a strong denial and counter allegations that US government agencies lacked interest in fighting cybercrime and failed to cooperate with Chinese counterparts. Jian noted that China received no response in its request for cooperation from the US on 13 cybercrime cases involving issues such as fake bank websites and child pornography.[13] He further noted that in other cases, it took up to six months to receive replies from the US.

China has warned against a "blame game." According to Qingli, "The only solution is through enhanced co-operation based on equality, mutual respect and mutual benefit, rather than politicizing the issue or pointing fingers at others."[15]

These allegations and counter allegations aren't new.[16] An article published in *China Economic Times* on 12 June 2000,[17] Xu Guanhua, then Chinese vice minister of science and technology, argued that high technology is tightly linked to a nation's military security, economic security, and cultural security. Regarding military security, Guanhua forcefully argued that developed countries have put many high-tech arms into actual battles and discussed the likelihood of ICT-exporting countries installing software for "coercing, attacking or sabotage."

More specifically, some Chinese government officials suspect that China is under cyberattack from the US. There has been a deep-rooted perception among Chinese policy makers that Microsoft and the US government spy on Chinese computer users through secret "back doors" in Microsoft products. Computer hardware and software imported from the US and its allies are subject to detailed inspection. Chinese technicians take control of such goods and either resist or closely monitor if Western experts install them.[18] Chinese cryptographers reportedly found an "NSA Key" in Microsoft products, which was interpreted as the National Security Agency. The key allegedly provided the US government back-door access to Microsoft Windows 95, 98, N-T4, and 2000. Microsoft's denials of such access and its patch to fix the problem haven't reassured the Chinese government.

Understanding Cyberattack Sources

In light of China's allegations, I thought it would be interesting to explore the origins of cyberattacks targeting China by looking at indicators related to foreign and domestic origins of malware products infecting Chinese computers. One such indicator concerns the malware infection rate (MIR) per 1,000 computers, based on the Microsoft telemetry data, which is collected from the users of Microsoft security products opting in for data collection. Although Microsoft antivirus isn't common in China, the telemetry data indicated that China was among the countries with the lowest infection rates worldwide. Only Japan and Finland had lower infection rates than China among the countries considered in the Microsoft study.

Another measure of cybercrime vulnerability is security company Sophos's threat exposure rate (TER). TER measures the percentage of PCs that have experienced a malware attack. According to TER data, China was the second most malware-infected country, only behind Chile in the third quarter of 2011, with a TER of 45 (sophos.com 2012). To put things in context, some of the cleanest countries in Sophos' studies were Luxembourg (TER of 2), Norway (3), Finland and Sweden (4), Japan and the UK (6), and the US and Germany (7).

So although China is among the most malware-infected countries according to the TER data, it has the lowest MIR values. Although TER captures all types of malware attacks, MIR data can detect globally prevalent malware products but not necessarily malware written in Chinese. A Microsoft report concluded that the low infection rate, as detected by the telemetry data, can be attributed to the unique characteristics of the Chinese malware ecosystem, which tends to be dominated by the Chinese-language threats, which aren't found in other countries.[19]

I triangulate this evidence with that coming from other sources. According to a survey released by the Anti-Phishing Working Group (APWG) in November 2011,[20] approximately 70 percent the world's maliciously registered domain names were established by Chinese cybercriminals for use against Chinese businesses. In the first half of 2011, such cybercriminals established 11,192 unique domain names and 3,629 "co.cc" subdomains for these attacks, compared to 6,382 unique domain names and 4,737 "co.cc" subdomains in the second half of 2010. (The "co.cc" domain is for companies and includes two free subdomains and bulk discounts for buyers of 15,000 or more domains. These domains have been widely used by spammers, sellers of fake antivirus programs, and others engaged in frauds.) Chinese phishers prefer to register new domains instead of using hacked domains. The majority of Chinese phishing perpetrated by Chinese criminals attack Chinese companies, and 80 percent of such attacks targeted Taobao.com, China's biggest online retailer.[20]

The bottom line is that, regardless of origin—internal or foreign—institutions must be prepared to protect against cyberattacks. Businesses and government agencies in industrialized countries are increasingly taking measures to make cyberattacks an integral part of risk assessment. In addition to deploying firewalls, antivirus software, and other security systems, organizations need to scale up efforts to enhance their employees' behaviors and

technological solutions to cybersecurity with relevant awareness and training programs. Regulators can promote cyberspace safety by developing and enforcing appropriate cybersecurity standards and regulations for critical infrastructure protection and private-sector companies. IT

References

1. M. Riley, "SEC Push May Yield New Disclosures of Company Cyber Attacks," *Bloomberg News*, 10 Jan. 2012; www.businessweek.com/news/2012-01-10/sec-push-may-yield-new-disclosures-of-company-cyber-attacks.html.
2. N. Easton, "Fortune's Guide to the Future," *Fortune*, 16 Jan. 2012, p. 44.
3. N. Vardi, "Chinese Take Out," *Forbes*, 25 July 2005; www.forbes.com/forbes/2005/0725/054.html.
4. D. Barboza, "Hacking for Fun and Profit in China's Underworld," 1 Feb. 2010, www.nytimes.com/2010/02/02/business/global/02hacker.html?pagewanted=all.
5. R. Chirgwin, "Feds Finger China in Wire Fraud: Where Phishing Victims' Money Goes," *The Register*, 26 Apr. 2011; www.theregister.co.uk/2011/04/26/feds_finger_china.
6. J. Blitz, "Security: A Huge Challenge from China, Russia and Organised Crime," *Financial Times*, 1 Nov. 2011; www.ft.com/intl/cms/s/0/b43488b0-fe2a-11e0-a1eb-00144feabdc0.html#axzz1dnezI1eF.
7. J. Leyden, "Hidden Dragon: The Chinese Cyber Menace," *The Register*, 24 Dec. 2011, www.theregister.co.uk/2011/12/24/china_cybercrime_underground_analysis/print.html.
8. T. Gjelten, "Cybersecurity Firms Ditch Defense, Learn to "Hunt," NPR, 10 May 2012; www.npr.org/2012/05/10/152374358/cybersecurity-firms-ditch-defense-learn-to-hunt.
9. "Shadows in the Cloud: Investigating Cyber Espionage 2.0," Joint Report of Information Warfare Monitor and the Shadowserver Foundation, JR03-2010, 6 Apr. 2010; www.utoronto.ca/mcis/pdf/shadows-in-the-cloud-web.pdf.
10. R. McMillan, "More Than 100 Companies Targeted by Google Hackers," *Computer World*, 27 Feb. 2010; www.computerworld.com/s/article/9163158/More_than_100_companies_targeted_by_Google_hackers
11. J. McDonald, "Cyber Attacks on Chemical Companies Traced to China," *USA Today*, 1 Nov. 2011; www.usatoday.com/money/industries/technology/story/2011-11-01/China-hackers/51024936/1.
12. "2010 Internet Policing Hinges on Transnational Cybercrime," *China Daily*, 10 Nov. 2010; www.china.org.cn/business/2010-11/10/content_21310523.htm.
13. N. Kshetri, "Pattern of Global Cyber War and Crime: A Conceptual Framework," *J. International Management*, vol. 11, no. 4, 2005, pp. 541–562.
14. D. Pauli, "China Named 'World's Biggest' Cybercrime Victim," 23 Mar. 2012; www.crn.com.au/News/294695,china-named-worlds-biggest-cybercrime-victim.aspx.
15. D. Qingli, "China Itself Is Facing Growing Cybercrime and Attacks," *Financial Times*, 11 Nov. 2011, www.ft.com/intl/cms/s/0/2a134f8c-f5be-11e0-bcc2-00144feab49a.html#axzz1dOy0Cfug.
16. N. Kshetri, *The Global Cyber-Crime Industry: Economic, Institutional and Strategic Perspectives*, Springer-Verlag, 2010.
17. "High Technology Affects National Security," *China Economic Times*, 12 June 2000; www.china.org.cn/english/GS-e/668.htm.
18. J. Adams "Virtual Defense," *Foreign Affairs*, May/June 2001, pp. 98–112.
19. "Microsoft Security Intelligence Report," Microsoft, 2011; www.microsoft.com/security/sir/keyfindings/default.aspx#!section_4_1_d.
20. "PayPal No Longer the Most Phished Brand," *Help Net Security*, 27 Apr. 2012; www.net-security.org/secworld.php?id=12828.

Nir Kshetri *is a professor at the University of North Carolina, Greensboro and a research fellow at Research Institute for Economics & Business Administration, Kobe University, Japan. His current research focuses on the dynamics of global cybercrime and cybersecurity. Kshetri holds a PhD in business administration from the University of Rhode Island. He's an advisory council member of the Pacific Telecommunications Council. Contact him at nbkshetr@uncg.edu.*