Cyber-victimization and Cybersecurity in China

By: Nir Kshetri

Kshetri, Nir (2013). "Cyber-victimization and Cybersecurity in China," *Communications of the ACM* , 56(4), 35-37.

Abstract:

Seeking insights into cyberattacks associated with China.

Keywords:

China | cybersecurity | cyber-victimization | economics | cyber security | Chinese government | Chinese economy

Article:

As a rapidly digitizing economy with over 538 million Internet users circa July 2012, China has been an attractive cybercrime target. The China Internet Network Information Center indicated that in the first half of 2011 217 million Chinese (45% of the Internet population) became malware victims, 121 million had online accounts hacked, and 8% were victimized by scammers. Likewise, the Ministry of Public Security's network security protection bureau noted that 80% of computers had been botnet-controlled.1

In the media and in international forums, Chinese government officials have repeatedly stressed and emphasized the country's victimization by foreign-originated cyberattacks. They are also concerned about the lack of cooperation or interest from Western countries in fighting cybercrimes. Given China's emphasis on and concern with foreign-originated cyberattacks, this Viewpoint assesses the extent of internally originated cybercrimes and China's capability, willingness, and resources to control them and examines the nature of its cybersecurity-related international engagements.

China's Greater Emphasis On and Concern about Foreign Originated Cyberattacks

China's senior government officials have commonly attributed cyberattacks targeting the country to foreigners. For instance, Gu Jian of the Chinese Ministry of Public Security said that over 200 Chinese government websites experienced cyberattacks daily and most are foreign originated. According to the State Council's Information Office, over one million Chinese IP addresses were controlled and 42,000 websites were hijacked by foreign hackers in 2009.

In the January 2011 meeting of the Intergovernmental Group of Experts of the UN Crime Prevention and Criminal Justice Program, the Chinese delegation noted that in 2010, over 90% of network sites' servers used to commit frauds such as phishing, pornography, and Internet gambling against Chinese targets were located outside China. The delegation also stated that over 70% of botnet control sites were in foreign countries. According to China's Computer Emergency Response Team's (CNCERT) Internet Security Perception Report, 8.9 million Chinese computers were attacked by 47,000 foreign IP addresses in 2011 and China was the world's biggest cyber-victim. The report further noted that foreign hackers had attacked 1,116 Chinese websites and accounted for 96% of phishing attacks targeting Chinese banks.6

Chinese government officials have also complained about U.S. government agencies' lack of cooperation and interest in fighting cybercrimes. Gu noted that China had received no response to its requests for cooperation from the U.S. on 13 cybercrime cases involving issues such as fake bank websites and child pornography and in other cases it took up to six months to receive replies.1

Cyberattacks Associated with China: Victimization versus Origination

Data proxies and indicators from a number of sources across a long time period indicate substantial cyberattacks originate in China. First, let us look at foreign and domestic origins of malware infecting Chinese computers. One such indicator concerns the malware infection rate per 1,000 computers (MIR) based on the telemetry data collected by Microsoft from users of its security products opting in. The telemetry data indicated China was among the countries with the lowest infection rates, only behind Japan and Finland. Another measure is Sophos' threat exposure rate (TER), which measures the percentage of PCs experiencing malware attacks. China was the second most malware infected country only behind Chile in the third quarter of 2011 with a TER of 45.8

The explanation regarding the differences in the two studies is that they differ in ability to detect Chinese and foreign malware. While TER captures all types of malware, telemetry data only detects globally prevalent malware. A Microsoft report concluded that the low infection rate as detected by telemetry can be attributed to a unique Chinese malware landscape that tends to be dominated by Chinese-language threats not found elsewhere.5

It is important to triangulate this evidence with that coming from other sources. In 2005 and 2009 China ranked #2—behind the U.S.—in top countries for originating cyberattacks.2 According to the Anti-Phishing Working Group (APWG), 70% the world's maliciously registered domain names were established by the Chinese to attack domestic businesses. In 2011, Chinese perpetrators established 11,192 unique domain names and 3,629 .cc subdomains for such attacks, the majority of which attacked Chinese companies and 80% targeted Taobao.com. Likewise, according to APWG, China had the world's highest malware infection rate of 54.1% in early 2012.

China's Capability, Willingness, and Resources to Control Cybercrimes

While fighting foreign-originated cybercrimes is an understandably challenging problem, it would be relevant and meaningful to examine China's capability, willingness, and resources to control domestically originated cybercrimes. In order to understand this complex phenomenon, let us first illustrate Brazil's experience. A computer crime bill has been pending in the Brazilian Congress since 2005 that has been unpopular with lawmakers due to a concern that it may facilitate government spying on citizens. While the Chinese government does not face similar constraints such as Brazil, due to unique institutional and economic characteristics, it faces challenges of different types.

Although about 40 governments control their online environments, China's unique approach and perspective to cybersecurity is reflected in its international engagement and domestic politics.3 Despite a broad agreement with the West on cybersecurity, China and its allies (Russia, Tajikistan, and Uzbekistan) diverge in important respects. One such difference is their preference to tackle the broader problem of information security rather than cybersecurity. In 2008, the Shanghai Cooperation Organization (SCO) Agreement in International Information Security expressed concerns about the West's monopolization in information and communications technology (ICT). The SCO economies like to control information that is likely to provoke what they call the three "evils" (terrorism, extremism, separatism). They also consider it important to prevent other nations from disrupting their economic, social, and political stability. In September 2011, the SCO economies submitted a draft International Code of Conduct for Information Security before the 66thUN General Assembly. In the document, they show concerns about threats to domestic stability of free flow of information and highlight the dominant role of the state.

China's senior government officials have commonly attributed cyberattacks targeting the country to foreigners.

On the domestic front, the Chinese government has emphasized a healthy and harmonious Internet environment. A healthy cyberspace that is "porn-free" and "crime-free" and "harmonious" means it does not threaten to destabilize the state's social and political order. Despite the tremendous difficulties associated with regulating and controlling the Internet, the Chinese government's cyber-control measures have been successful in some senses.9 However, it has encountered a host of problems and difficulties while attempting to achieve these goals, as illustrated in the following examples.

First, consider the Green Dam Youth Escort firewall software program launched in 2008. The Chinese government had announced a plan to make it mandatory to have the Green Dam

installed on all new PCs in the country. The stated goal of the mandate was to protect children from violent and pornographic content.

The first problem the Green Dam faced was that while addressing one cybersecurity issue, it created side effects that raised another. For instance, while it successfully blocked politically sensitive contents, many believed the software would represent significant risks to users as a single flaw in the Green Dam system would expose the entire Chinese population to cybercriminals.

A second problem stemmed from the fact that it increased PC manufacturers' costs, which led to an additional financial burden on consumers. While the Green Dam would be free to users, manufacturers needed to pay license fees to the Ministry of Industry and Information Technology (MIIT) to install the software. The vendor of the Green Dam, Beijing Dazheng Language and Knowledge Processing Research Center (BDLKPRC) had received $6 million from the MIIT to develop the software.

A third related problem had to do with strong opposition from computer manufacturers and the public. Even Lenovo, which is 57% government-owned, opposed it. Internet users, who are increasingly acting on a bottom-up approach, participated in collective resistance efforts to abort the Green Dam.

Given the national security and economic risks and a strong resistance, the Green Dam program was indefinitely delayed after being installed in 20 million PCs. The unsustainable business model led to the closure of BDLKPRC in the 2010 and the company was near bankruptcy.

As another example, consider the 2011 regulation that required microbloggers to register using their real names. The Nasdaq-listed Chinese online media company Sina warned that the requirement would negatively affect user activity and threaten its popular microblogging service, Sina Weibo. Even well after the March 16, 2012 deadline, Sina Weibo continued to allow users, who had not registered their real names to post and use its services.

Regarding the private sector's role, India would provide a particularly appropriate country for comparison. The active and influential roles of the National Association of Software and Service Companies (NASSCOM) have strengthened India's cybersecurity orientation. The Internet Society of China (ISC), a counterpart of the NASSCOM, has engaged in roles of different nature. In 2001, the ISC asked Internet companies to sign a voluntary pledge that required them not to disseminate information "that might threaten state security or social stability." In 2009, the ISC awarded China's biggest search engine company, Baidu, and 19 other companies the "China Internet Self-Discipline Award" for fostering and supporting "harmonious and healthy Internet development."4

Conclusion

As most economies, while China undoubtedly has suffered from foreign-originated cyberattacks, data triangulation from multiple sources indicates domestically originated attacks are no less severe. China, like many parts of the world, has a large number of hackers with diverse motivations, backgrounds, skills, and interests to engage in cyberattacks.

The base of regime legitimacy in China has shifted from Marx-Leninism to economic growth and prosperity.10 China thus would like to achieve the goal of its cyberspace governance initiatives without jeopardizing its economic development. In this regard, the government's cost/benefit calculus associated with cybercontrol measures may change over time. For instance, if the perceived risks of state insecurity or social instability increase with microblogging activities, the government may demand stricter enforcement.

Allegations and counter-allegations, which have been persistent themes in dialogues and discourses in the U.S.-China relationships in cybersecurity, can be linked to the lack of an extensive cooperation. For instance, if one country needs the help of the other country in investigating a cybercrime, a request for assistance takes place through an exchange of letters. It was reported that in 2010, the FBI office in Beijing forwarded 10 letters through the Ministry of Foreign Affairs and received responses to two. This is in sharp contrast to the deeper and stronger collaborations and partnerships between the U.S. and European Union (EU) countries. For instance, the Italy-based European Electronic Crimes Task Force, which has dedicated personnel from the countries involved to investigate and prosecute cybercrimes, provides a forum for law enforcement agencies, the private sector, and academia from the U.S. and EU nations.

China's unique approach and perspective to cybersecurity is reflected in its international engagement and domestic politics.

The resource constraint has necessitated a partial reliance upon the private sector and semi-private institutions to enforce cybersecurity regulations and policies. In order to minimize investment risk or the risk of losing customers, some private sector enterprises have chosen not to enforce the regulations and policies. The largely unsuccessful experiences with the implementations of the Green Dam and real name registration in microblogging suggest a decline in the state's institutional capacity to regulate cyberspace.

Responses of technology companies such as Sina indicate some degree of noncompliance with regulations. This is a significant deviation from the past practices of Chinese companies. Conformance to the existing institutions has been at the expense of technical and functional efficiency, which has acted as a force of institutional changes. This type of contradiction can be

described as "legitimacy that undermines functional ineffici ency."7 Sina has tilted the balance toward efficiency and productivity at the expense of political legitimacy.

References

1. *China Daily*, 2010 Internet policing hinges on transnational cybercrime. (Nov. 10, 2010); http://www.china.org.cn/business/2010-11/10/content_21310523.htm.

2. Kim, S.H., Wang, Q., and Ullrich, J.B. A comparative study of cyberattacks. *Commun, ACM 55*, 3 (Mar. 2012), 66–73.

3. Kshetri, N. Les activités d'espionnage électronique et de contrôle d'Internet à l'ère de l'infonuagique: Le cas de la Chine. *Télescope 18*, 1–2 (2012), 169–187.

4. MacKinnon, R. Inside China's censorship machine (Jan. 29, 2012); http://fullcomment.nationalpost.com/2012/01/29/rebecca-mackinnon-inside-chinas-censorship-machine/.

5. Microsoft. Microsoft Security Intelligence Report, 2011; http://www.microsoft.com/security/sir/keyfindings/default.aspx#!section_4_1_d.

6. Pauli, D. China is the "world's biggest cybercrime victim." (Mar. 22, 2012); http://www.scmagazine.com.au/News/294653,china-is-the-worlds-biggest-cybercrime-victim.aspx.

7. Seo, M.G. and Creed, W.E.D. Institutional contradictions, praxis, and institutional change: A dialectical perspective. *Academy of Management Review 27*, 2 (2002), 222–247.

8. sophos.com. Security Threat Report, 2012; http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.ashx.

9. Wu, G. In the name of good governance: E-government, Internet pornography and political censorship in China. In *China's Information and Communications Technology Revolution: Social Changes and State Responses*. Zhang, X. and Yongnian Zheng, Y., Eds. (2009), 69–83.

10. Zhao, S. Chinese nationalism and its international orientations. *Political Science Quarterly 115*, 1 (2000), 1–33.