The People's Republic of Hacking

China's campaign of cyber attacks has reached epidemic proportions. Can anything be done to stop it?

BY ADAM SEGAL

In an extraordinary story that has become depressingly ordinary, the *New York Times* reports that Chinese hackers "persistently" attacked the newspaper, "infiltrating its computer systems and getting passwords for its reporters and other employees." The attacks began around the time journalists were preparing a story on the massive wealth the family of China's Prime Minister Wen Jiabaohas allegedly accumulated, but the methods, identification, and apparent objectives of the hackers have been seen before in previous attacks on defense contractors, technology companies, journalists, academics, think tanks, and NGOs. *Bloomberg*, which published a story on the wealth of the family of Xi Jinping, China's top leader, has also been reportedly attacked. While just one case in a sweeping cyber espionage campaign that appears endemic, the attack on the *Times* does highlight both the willingness of Beijing lean out and shape the narrative about China as well as the vulnerability the top leadership feels about how they are portrayed.

As with many cases of cyber espionage, the break-in is assumed to have started with a spear-phishing email, a socially engineered message containing malware attachments or links to hostile websites. In the case of the attack on the security firm RSA in 2011, for example, an email with the subject line "2011 Recruitment Plan" was sent with an attached Excel file. Opening the file downloaded software that allowed attackers to gain control of the user's computers. They then gradually expanded their access and moved into different computers and networks.

Once in, the hackers are pervasive and fairly intractable. The hackers involved in the attacks on the British defense contractor BAE Systems, for example, were reportedly on its networks for 18 months before they were discovered; during that time they monitored online meetings and technical discussions through the use of web cameras and computer microphones. According to Jill Abramson, executive editor of the *Times*, there was no evidence that sensitive information related to the reporting on Wen's family was stolen, but in previous cases hackers encrypted data so that investigators had a difficult time seeing what was actually taken.

Evidence that the hackers are China-based in all of these cases is suggestive, but not conclusive. Some of the code used in the attacks was developed by Chinese hacker groups and the command and control nodes have been traced back to Chinese IP addresses. Hackers are said to clock in in the morning Beijing time, clock out in the afternoon, and often take vacation on Chinese New Year and other national holidays. But attacks can be routed through many computers, malware is bought and sold on the black market, groups share techniques, and one of the cherished clichés of hackers is that they work weird hours.

Perhaps the most compelling evidence has been the type of information targeted. The emails and documents of the office of the Dalai Lama and Tibetan activists, defense industries, foreign embassies, journalists, and think tanks are not easily monetized and so would apparently have little attraction to criminal hackers. The information contained in them would be of much greater interest to the Chinese government.

Beijing is pushing its Internet power outside of China into the rest of the world. At home, it controls the flow of information on the Web domestically through censoring and filtering technologies as well as attempts to steer conversations or drown out opposition on social media sites by government-paid commentators, known in China as the 50 Cent Party for the going rate per posting. What the *New York Times* and other hacks

demonstrate is the desire to shape international political narratives as well as gather information from those who might influence the debates on topic of importance to Beijing. The *Times*' worry that the hackers might take the paper offline on election night also reveals an attempt at intimidation as well as influence.

What will also be dispiritingly familiar in the aftermath of the attacks is the discussion about what can be done. Over the last several years, U.S. government officials have mounted an increasingly public campaign of naming and shaming China. But this has had little effect, and the Chinese response has been one of denial, calling the accusations "irresponsible," noting that hacking is illegal under Chinese law, and pointing out that China is also a victim of cyber crime, most of it coming from IP addresses in Japan, South Korea, and the United States.

So what can be done? Private security experts and U.S government officials say they are getting better at attributing attacks to groups and individuals. If that is the case, then the United States may begin to think about targeted financial sanctions or visa restrictions on identified hackers. What might cause the most difficulty for Beijing, however, are private and government efforts to ensure that reporting of the caliber of *New York Times* and *Bloomberg* is made widely available within China through translation and efforts to circumvent the Great Firewall of China. U.S. diplomatic cables posted online by WikiLeaks suggested that the hack on Google in January 2010 was ordered by a member of the Politburo who "typed his own name into the global version of the search engine and found articles criticizing him personally." Wen Jiabao and Xi Jinping might have had the same reaction.

FREDERIC J. BROWN/AFP/Getty Images

Measure for Measure