By Sean Noonan

A recent batch of WikiLeaks cables led Der Spiegel and The New York Times to print front-page stories on China's cyber-espionage capabilities Dec. 4 and 5. While China's offensive capabilities on the Internet are widely recognized, the country is discovering the other edge of the sword.

China is no doubt facing a paradox as it tries to manipulate and confront the growing capabilities of Internet users. Recent arrests of Chinese hackers and People's Liberation Army (PLA) pronouncements suggest that China fears that its own computer experts, nationalist hackers and social media could turn against the government. While the exact cause of Beijing's new focus on network security is unclear, it comes at a time when other countries are developing their own defenses against cyber attacks and hot topics like Stuxnet and WikiLeaks are generating new concerns about Internet security.

One of the U.S. State Department cables released by WikiLeaks focuses on the Chinese-based cyber attack on Google's servers that became public in January 2010. According to a State Department source mentioned in one of the cables, Li Changchun, the fifth highest-ranking member of the Communist Party of China (CPC) and head of the Party's Propaganda Department, was concerned about the information he could find on himself through Google's search engine. He also reportedly ordered the attack on Google. This is single-source information, and since the cables WikiLeaks released do not include the U.S. intelligence community's actual analysis of the source, we cannot vouch for its accuracy. What it does appear to verify, however, is that Beijing is regularly debating the opportunities and threats presented by the Internet.

A shift from offensive capabilities

On Nov. 2, the People's Liberation Army Daily, the official paper for the PLA and the primary medium for announcing top-down policy, recommended the PLA better prepare itself for cyber threats, calling for new strategies to reduce Internet threats that are developing "at an unprecedented rate." While the report did not detail any strategies, it quoted a PLA order issued for computer experts to focus on the issue.

The Nov. 2 PLA announcement is part of a long trend of growing network-security concerns in China. In 2009, Minister of Public Security Meng Jianzhu emphasized that the development of the Internet in China created "unprecedented challenges" in "social control and stability maintenance." In June 2010, the State Council Information Office published a white paper on the growing threat of cyber crime and how to combat it. Clearly, these challenges have been addressed this year. The Ministry of Public Security (MPS) announced Nov. 30 that it had arrested 460 suspected hackers thought to have been involved in 180 cases so far in 2010.

This is part of the MPS' usual end-of-year announcement of statistics to promote its success. But the MPS announcement also said that cyber crime had increased 80 percent this year and seemed to blame the attacks only on hackers inside China.

These were cases mainly of producing and selling "Trojan" programs (malware that looks legitimate), organizing botnets, assisting others in carrying out denial-of-service attacks and invading government websites. The MPS also closed more than 100 websites that provided hackers with attack programs and taught them various tactics.

The PLA already has two notoriously large and capable network security units: the Seventh Bureau of the Military Intelligence Department (MID) and the Third Department of the PLA. In simple terms, the MID's Seventh Bureau is an offensive unit, responsible for managing research institutes that develop new hacking methods, train hackers and produce new hardware and software. The PLA Third Department, defensive in nature, is the third largest signals intelligence-monitoring organization in the world. STRATFOR sources with expertise in network security believe that China's government-sponsored hacking capabilities are the best in the world. But this perception is based in part on the fact that China demonstrates these capabilities quite often. The United States, on the other hand, is much more restrained in exercising its offensive cyber capabilities and is not inclined to do so until there is a dire and immediate need, such as war.

Piracy vulnerability

The details of China's escalating effort to improve network security are still murky, but one recently announced campaign against software piracy is notable. On Nov. 30, Deputy Commerce Minister Jiang Zengwei announced a new six-month crackdown on illegally copied products in China. He said the focus was on pirated software, counterfeit pharmaceuticals and mislabeled agricultural products. The Chinese public has pushed for more regulation of pharmaceuticals and food due to a rising number of cases in which people have become sick or even died because of falsely labeled or tainted products, such as melamine-contaminated milk. But Beijing seems to be even more concerned about the vulnerabilities created by running unlicensed and non-updated software, and publicizing the crackdown is clearly an attempt by Beijing to appease Western governments and businesses that are placing growing pressure on China.

Indeed, China has a sizable counterfeit economy, much to the ire of Western businesses. While Beijing may placate Westerners by announcing crackdowns for the benefit of international audiences, it takes more forceful measures when it sees a larger threat to itself, and the security emphasis now seems to be on the threat of running insecure software on government computers. The problem with unlicensed software is that it does not receive automatic updates from the manufacturer, which usually are sent out to fix vulnerabilities to malware. Unlicensed software is thus left open to viral infiltration. It is also cheap and easy to get, which makes it pervasive throughout both government and private computer networks.

One of the measures Beijing has started to implement is requiring licensed software to be installed on new computers before they are sold, which also gives the government an

opportunity to install censorship measures like Green Dam. One persistent problem is that much of the pre-installed software still consists of pirated copies. While China has released statistics showing that the use of legitimate software in China has increased dramatically, the Business Software Alliance, an international software industry group, estimates that 79 percent of the software sold in China in 2009 was illegally copied, creating a loss to the industry of $7.6 billion in revenue. Even more important to Beijing, these statistics mean the vast majority of Chinese computer systems — government and private alike — remain vulnerable to malware.

At the same Nov. 30 news conference at which Jiang announced the new anti-piracy initiative, Yan Xiaohong, deputy head of the General Administration of Press and Publication and vice director of the National Copyright Administration, announced a nationwide inspection of local and central government computers to make sure they were running licensed software. While this suggests Beijing's major concern is the security of government computers, it also emphasizes how widespread the unlicensed software problem is.

This new focus on using legitimate software, however, will not be a complete solution to China's Internet vulnerabilities. There has been little effort to stop the selling of copied software, and it is still very easy to download other programs, licensed and unlicensed, and malware along with them (such as QQ). Moreover, the new security measures are dealing only with the symptoms, not the underlying problem, of a counterfeit-heavy economy. A six-month crackdown will not undermine or eliminate software piracy in China; to do so would require an immense and sustained investment of time, money and manpower. Indeed, China has been a hub for pirating software, films and other copyrighted material for so long that the enormous domestic economic base that has grown up around it would be virtually impossible to dismantle. In any case, vulnerabilities still exist in legitimate software, even if it is better protected against novice hackers. New vulnerabilities are constantly being found and exploited until software companies come up with the appropriate patches.

From nationalist hackers to dissident threats

China's highly developed hacking capabilities, more offensive than defensive, include Internet censorship measures like the infamous Great Firewall, and the official police force run by the MPS specifically to monitor Chinese Internet traffic and censor websites is 40,000 strong. China also has developed two unofficial methods of censorship. First, operators of private websites and forums must follow certain government regulations to prevent statements critical of the government from being disseminated, which encourages private operators to be their own censors. Second, there is a veritable army of nationalistic computer users in China that include "hacktivist" groups such as the Red Hacker Alliance, China Union Eagle and the Honker Union, with thousands of members each. They became famous after the 1999 "accidental" bombing of the Chinese Embassy in Belgrade, which prompted China-based hackers to attack and deface U.S. government websites. The Chinese government, state-owned enterprises and private companies also engage public relations firms to hire, deploy and manage what have become colloquially known as "Party of Five Maoists." These are individuals who get paid half a yuan (5 mao) for every positive Internet post they write regarding government policy, product reviews and other issues.

But as China's Internet-using population nears 400 million, with nearly 160 million using social networking, Beijing recognizes the risk of all this spiraling out of control. Censors have not been able to keep up on the social-networking front. Even with limited or banned access to sites like Twitter and Facebook, their Chinese versions, Weibo and Kaixin, for example, are expanding exponentially. While the government may exercise more control over the Chinese-based sites, it cannot keep up with the huge number of posts on topics the CPC considers disharmonious. The recent announcement of Liu Xiaobo's Nobel Peace Prize is an example of news that was not reported at first in Chinese media but through social networking sites, spreading like wildfire. And the censorship is not exclusive; even non-dissidents can be censored, such as Prime Minister Wen Jiabao when he recently called for limited political reform.

China's large Internet population will not all be nationalists. And if those who learn skills from informal hackers turn into dissidents, Beijing would consider them a serious threat. The Internet presents exactly the type of tool that could pose a major threat to the CPC because it spans regions, classes and ethnicities. Most social grievances are local and economic or ethnic-based. The potential for one opposition group to be united nationwide over the Internet is one of Beijing's gravest concerns. It has realized that a weapon it once wielded so deftly against foreign powers and business entities can now be used against Beijing.

Outside issues

At the same time Beijing reached this realization, WikiLeaks demonstrated the possibility for sensitive government information to be spread globally through the Internet. Beijing saw that if the United States, with its expertise in signals intelligence and security, could be vulnerable to such a threat, so could China. Stuxnet demonstrated the vulnerability of important infrastructure to cyber attack, one reason for China's new emphasis on licensed software (Iran is known to run unlicensed Siemens software). China's recent emphasis on network security is likely linked to all of these factors, or it may be due to a threat seen but as yet unpublicized, such as a cyber attack or leak inside China that the government has been able to keep quiet.

Other countries have also been implementing new network security measures, most notably the United States. On Oct. 31, the Maryland-based U.S. Cyber Command became fully operational, and its commander is also the head of the National Security Agency, the premier U.S. government entity for signals intelligence. (Thus, China's giving Internet security responsibility to the PLA should come as no surprise to the United States.) And as China realizes the difficulties of defending against attacks in cyberspace, which tend to favor the offense, the United States is wrestling with the same problems and complexities as it tries to shield government, civilian and commercial computer systems, all of which require different degrees of control and operate under different laws. As cyber espionage and cyber sabotage become even greater concerns, China will be forced to face the far more difficult task of not only pecking away at the Pentagon's firewalls but also providing for its own internal system security.

These new efforts all contradict China's long-standing policy of cultivating a population of nationalistic computer users. This effort has been useful to Beijing when it sees a need to cause disruption, whether by attacking U.S. sites after perceived affronts like the Chinese Embassy bombing in Belgrade or preventing access from powerful foreign entities like Google. But China

has also recognized that developing these public capabilities can be dangerous. Nationalist Chinese hackers, if motivated by the right cause and united through the pervasive Internet, can always turn on the government. And the situation seems to have more and more governments on edge, where simple mistakes can raise suspicions. China's redirection of a large amount of Internet traffic in April caused an outcry from the United States and other countries, though it may well have been an accident.

It is hard to tell what Beijing sees, specifically, as a first-tier cyber threat, but its decision to develop an effective response to all manner of threats is evident.

Read more: China and its Double-edged Cyber-sword | STRATFOR

Reproduced with the permission of STRATFOR