Enter Search Term

Comments (0)

Prev | Table of Contents | Next

ADVANCED

Science Home Current Issue Previous Issues Science Express Science Products My Science About the Journal

Science Magazine

Home > Science Magazine > 1 March 2013 > Stone, 339 (6123): 1026-1027

- -

Science
www.sciencemag.org
Science 1 March 2013:
Vol. 339 no. 6123 pp. 1026-1027
DOI: 10.1126/science.339.6123.1026

AAAS.ORG | FEEDBACK | HELP | LIBRARIANS

NEWS FOCUS

## A Call to Cyber Arms

**Richard Stone** 

China's extensive cyber research activities and allegations over cyber espionage have put the United States on high alert.

XI'AN, CHINA—The leaflet posted in the school of information engineering here at Xi'an Jiaotong University was brief but enticing, offering computer-savvy graduates a hefty stipend and the chance to serve their motherland. "I was curious," says Liu, who asked that only his surname be used in this article. It was the spring of 2007, and Liu, then 24 years old, was wrapping up a master's degree in computer algorithms. Encouraged by his supervisor, Liu called the number on the leaflet; that summer, he joined an elite corps of the People's Liberation Army (PLA) that writes code designed to cripple command–and–control systems of enemy naval vessels.

PLA writings call the electromagnetic spectrum "the fifth domain of battle space," putting cyberspace on an equal footing with ground, air, sea, and space. Cyber conflicts "threaten national security and the very existence of the state," two scholars with the Academy of Military Sciences wrote in China Youth Daily in 2011. State media regularly tout PLA activities in cyber defense, a catchall term encompassing everything from surveillance and espionage to weapons such as electromagnetic pulse generators that disable computer networks and malware designed to take down power grids or contaminate water supplies. Augmenting PLA efforts is a legion of civilian researchers and hackers whose efforts ostensibly are directed at repelling electronic intruders. In 2011, more than 8.5 million computers in China "were attacked by rogue programs every day," a 48% increase over the previous year, says Li Yuxiao, a cyber law expert at Beijing University of Posts and Telecommunications.

Related Resources In Science Magazine PODCASTS <u>Science Podcast: 1 March</u> <u>Show</u> Science 1 March 2013: 1103.



View larger version: <u>In this page</u><u>In a new window</u> <u>Download PowerPoint Slide for Teaching</u>

Twenty-first century battleground. The U.S. government is ramping up efforts to shore up power grids, air traffic control systems, and other critical infrastructure against cyber incursions.

CREDITS: (MAIN) ISTOCKPHOTO.COM; (INSETS, LEFT TO RIGHT) WESLEY HITT 2012/GETTY IMAGES; ROBERT HARDING/GETTY IMAGES; ISTOCKPHOTO.COM

But evidence is accumulating that China can dish it out, too. In a report issued last week, the U.S. computer security firm Mandiant tracked one especially adept group of hackers,

sometimes called the Comment Crew or Comment Group, to a neighborhood in Shanghai housing Unit 61398, a bureau of the PLA General Staff Department's Third Department. According to Mandiant, other computer security analysts, and U.S. State Department sources, hackers in China have gathered gigabytes of data on industrial secrets, military hardware, and government strategy for political negotiations.

This is not a unilateral arms buildup. Another heavyweight in the cyber arena is Russia; hackers took down Georgian government servers in advance of Russia's invasion of that former Soviet republic in August 2008. The United States, too, has gone all-in on cyber warfare. In 2009, it established the U.S. Cyber Command in Fort Meade, Maryland, to conduct "full-spectrum military cyberspace operations." The Defense Department's operational needs "will require the integration of cyber and electronic warfare at unprecedented levels," said Regina Dugan, then-director of the U.S. Defense Advanced Research Projects Agency, in a statement released by DARPA before the Senate took up the 2013 defense authorization. According to U.S. Defense Secretary Leon Panetta, the Pentagon spends about \$3 billion a year on cyber security.

An early fruit of this massive enterprise may be the most successful cyber weapon deployed to date:

Stuxnet. The computer worm came to light in 2010 after instructing centrifuges in Iran that enrich uranium to spin at damaging speeds. Computer security experts have credited the United States and Israel for Stuxnet's sophisticated code and for orchestrating its insertion into the Iranian machines. Whoever's handiwork it was, Stuxnet has "shown the world how to stage a damaging cyber attack," says James A. Lewis, an analyst with the Center for Strategic and International Studies in Washington, D.C.

Now that Pandora's box is open, the United States fears that it, too, may someday be on the receiving end of an effective attack. In his State of the Union speech on 12 February, U.S. President Barack Obama declared that unidentified enemies are "seeking the ability to sabotage our power grid, our financial institutions, [and] our air traffic control systems." That day, he signed an executive order to strengthen cyber defenses and called on Congress to pass legislation that would "give our government a greater capacity to secure our networks and deter attacks." Last week, the U.S. Department of Energy announced \$20 million in funding for the development of technologies to strengthen the cyber security of delivery systems for electricity, oil, and gas.

A one-two punch featuring a cyber attack on critical infrastructure and a physical strike against U.S. targets could leave the country reeling from a "cyber Pearl Harbor," Panetta warned in a speech last October. "It would paralyze and shock the nation and create a new, profound sense of vulnerability," he said. Panetta did not call out China. But with territorial disputes between China and U.S. allies raising tensions in East Asia, Panetta, in a meeting with Chinese defense officials in Beijing last September, said that he "underscored the need to increase communication and transparency with each other so that we could avoid a misunderstanding or a miscalculation in cyberspace."

## Raising an army

In a quiet corner of a hotel lobby here in the capital of western China's Shaanxi Province last November, Liu sips puer tea and shifts nervously in his chair as he describes how his high marks in mathematics propelled him from rural Shaanxi to Xi'an Jiaotong University. Like many other computer science students there, he says, he learned to hack in his spare time. "We felt it was a patriotic duty," he says.

In the PLA unit, which he declined to identify, Liu says he spends about half of his time working on programming teams to develop algorithms ordered by superiors. The rest of the time he reads up on computer literature or political ideology and takes part in simulations with other units in which he and his colleagues stage or repel attacks. "Our work is purely defensive," says Liu, who claims he was given permission to speak with *Science* in order to emphasize the defensive nature of the research. PLA and foreign ministry spokespersons last week insisted that China has not carried out cyber espionage or attacks on other nations.

The kaleidoscopic patterns of activity in cyberspace may be hard

Civilian research sits at one end, and it is largely out in the open.

Administration for the Protection of State Secrets has tapped 10

to interpret, but the wellspring of China's strength is hundreds

of computer and information departments across the country.

For example, over the past 5 years China's National



View larger version: <u>In this page</u> <u>In a new window</u> <u>Download PowerPoint Slide for Te</u>

**Digital hands on deck!** In a conflict in the Pacific, the *USS Blue Ridge*, the U.S. Navy's command ship in the region, would be a ripe target for a cyber strike.

CREDIT: WIKIMEDIA COMMONS

universities to host academies for training students in computer science and other disciplines for sensitive jobs in government agencies. Research in information engineering and cyber defense is also funded through standard science grant programs as well as initiatives supporting sensitive dual-use projects, including the information ministry's 242 program and the security ministry's 115 program.

In the academic world, a leader in cyber defense research is Shanghai Jiao Tong University's School of Information Security Engineering. In the past several years, its scientists have published openly on the injection of Trojan horses into the Windows platform, for instance, and on the pros and cons of Rootkit, a program for hijacking a computer system. In Changsha, the National University of Defense Technology has a research program in electronic and information warfare. And at Dalian University of Technology in northeast China, a pair of researchers funded by the science ministry and the National Natural Science Foundation of China published a report in *Safety Science* in July 2011 on vulnerabilities in the western U.S. power grid.

The real action in the cyber sphere is in the PLA's General Staff Department. As one of several bureaus in the Third Department, Unit 61398 "appears to function as the Third Department's premier entity targeting the United States and Canada, most likely focusing on political, economic, and military-related intelligence," according to a 2011 report from the Project 2049 Institute, a think tank in Arlington, Virginia. (At least one Unit 63198 researcher has published in the open literature, as co-author with three colleagues at Shanghai Jiao Tong University of a 2009 abstract on network security alerts and attack scenarios. Mandiant's report flagged job recruitment fairs for Unit 63198 in 2004 at the Harbin Institute of Technology and Zhejiang University in Hangzhou that were advertised openly on the universities' Web sites.) The General Staff 's Fourth Department, meanwhile, "has primary responsibility for the offensive electronic-based information warfare missions in the PLA," states a report last March on China's cyber espionage capabilities, prepared by Northrop Grumman Corp. analysts for the U.S.-China Economic and Security Review Commission.

In a speech last May, the head of the United Kingdom's MI5 counterintelligence agency, Jonathan Evans, decried an "astonishing" level of cyber espionage in the world, with "industrial-scale processes involving many thousands of people lying behind both state-sponsored cyber espionage and organized cyber crime." Evans did not name China, but security experts were quick to point out that no country rivals

China's dedication, and prowess, in cyber espionage.

China so far has shown only some of its cards. Chinese hackers have allegedly used computer network exploitation techniques such as spearphishing, in which malware is embedded in target computers, to harvest data from a long list of Fortune 500 companies, think tanks, and government agencies. Since 2006, the Mandiant report documents, the Shanghai-based hacking group it tracked has pilfered hundreds of terabytes of data from 141 organizations, including 115 in the United States. Information technology and aerospace firms were targeted most frequently. Mandiant said it believes the activity it observed "represents only a small fraction of the cyber espionage" committed by the Shanghai outfit. Delays and cost overruns in the U.S. F-35 fighter jet program "may be the result of cyber espionage, as could the rapid development of China's J-20 stealth fighter," Lewis testified before the U.S. Congress last April. "Cyber espionage is the most pressing threat we face," he asserted.

On the diplomatic front, the State Department in 2011 established an Office of the Coordinator for Cyber Issues. "We're writing foreign policy from scratch," says a U.S. State Department official who requested anonymity. Chinese and U.S. defense officials have begun swapping views on cyber security under a Strategic Security Dialogue launched last year. The two sides have struggled to identify confidence-building measures that would reduce distrust, says the State official.

In the meantime, the official says, "there is a debate going on" in the U.S. government about whether China's cyber espionage activities "have reached a level where they constitute a national security threat." It's only a matter of time, he says, before China crosses that Rubicon.

The editors suggest the following Related Resources on Science sites

In Science Magazine

PODCASTS Science Podcast: 1 March Show Science 1 March 2013: 1103. Summary Full Text Transcript

Comments (0)