China’s cyber war

Washington Post Editorial Board, Published: December 15, 2011

CHINA IS waging a quiet, mostly invisible but massive cyber war against the United States aimed at stealing its most sensitive military and economic secrets and obtaining the ability to sabotage vital infrastructure. This is, by now, relatively well known in Washington, but relatively little is being done about it, considering the enormous stakes involved.

What exactly is happening? Hackers mostly backed by the People’s Liberation Army are trying daily to penetrate the computer systems of U.S. government agencies, defense contractors, technology firms, and utilities such as power and water companies — not to mention the private e-mail accounts of thousands of Americans. To an alarming degree, they are succeeding. In recent years hacks have been reported of the State, Defense and Commerce departments; Lockheed Martin; Google, which said its source code and the e-mail accounts of senior government officials were targeted; and the computer security company RSA, which protects critical networks through the SecureID system.

“The computer networks of a broad array of U.S. government agencies, private companies, universities and other institutions — all holding large volumes of sensitive economic information — were targeted by cyber espionage,” said a report issued in October by the Office of the National Counterintellingence Executive. “Much of this activity originated in China.”

As in the case of other novel and slowly developing threats — international terrorism in the 1990s comes to mind — the U.S. response has been slowed by bureaucratic infighting, poor information-sharing and a failure to prioritize the problem above more familiar business with Beijing. The Pentagon has set up a cyber-command, but it has the authority to protect only military networks; the Department of Homeland Security jealously guards its prerogative to guard domestic civilian targets. Government agencies often don’t share sensitive intelligence with companies, while many companies are reluctant to report on penetrations of their networks.

A further difficulty is identifying exactly where cyber-attacks originate and connecting them to their government sponsors. Predictably enough, the Chinese government aggressively denies any involvement in the attacks on U.S. agencies and companies — which makes it difficult for diplomats to pressure for a cease-fire. But an encouraging report in the Wall Street Journal this week said that U.S. intelligence agencies had managed to identify many of the Chinese groups, and even individuals, including a dozen cells connected to the People’s Liberation Army.

This should provide an opportunity for the Obama administration to more directly confront the problem. It should demand that Beijing shut down the military-backed groups; if it does not do so, they could be subjected to countermeasures, including sanctions against individuals. Congress could also consider legislation punishing companies connected to the Chinese military if the cyber war does not cease. Yes, such responses have the potential to roil relations between Washington and Beijing. But the Chinese offensive — and the economic and national security threats it poses — is simply too important to ignore.

DOD spending $500B on 6 preparations for cyber war

February 28, 2012 5:42 PM Meghan **Kelly** Venturebeat.com

Cyber war is more than a threat; it is something the Department of Defense is spending money on as we speak. Deputy Secretary of Defense Ashton Carter outlined six ways the DOD is taking action today, as well as legislation he believes can help the government act quickly against hackers at home and abroad.

“Cyber will overtake terrorism as the persistent gnawing … kind of threat and danger,” said Carter at the RSA Conference in San Francisco today. “The market, both economic and political, undervalues security at the moment. Doesn’t see it. Doesn’t fully get it. This is wrong, this is a mistake.”

The DOD is charged with protecting the United States not only with ships, airplanes, and tanks but also with cyber weapons. Former National Security Agency director Mike McConnell pointed out that if terrorists find their way into our banks, the ensuing economic havoc could result in greater devastation than that of 9/11. He said the US must be prepared not only to defend itself on the Internet but also to fight back. Six core DOD missions speak to this responsibility:

1. Developing and preparing to use weapons of cyber warfare
2. Preparing the U.S. for what the battlefield may look like
3. Listening for and analyzing defense intelligence over the Internet
4. Defending both classified and unclassified networks
5. Creating technology using the DOD’s and the NSA’s “weight and resources” and distributing them to Homeland Security, law enforcement agencies, and partners
6. Protecting these tools and infrastructure with the military.

The DOD is spending half a trillion dollars to run these projects, according to Carter. He says he has never heard of anyone wanting to cut the budget back. Indeed, he would like to increase the spending if he can find worthy areas to develop. However, despite governmental support, he wants the technology sector to help push the agenda further. The legislation Carter is pushing for would allow the government to act more freely with the public sector to develop tools. He explained it would enable the government to share threat information with the private sector and would enable public companies to report intrusions “without liability or trust concerns.” It would also allow members of the private sector to share threat information with each other “without liability or trust concerns.” And, if passed, it would force companies to report intrusions to the government.

Carter is aware that legislation and bullet points are small steps but asks that the security industry understand that “trying to get our act together as a country … is not an easy thing to do.”

“Of course, we were involved in birthing the Internet itself,” said Carter, “We have a history here, and we’re going to continue it.”

U.S. Steps up Alarm over Cyber attacks

SIOBHAN GORMAN and SIOBHAN HUGHES

March 13, 2013, on page A1 in the U.S. edition of The Wall Street Journal.

WASHINGTON—The nation's top spies warned Tuesday of the rising threat of cyber- attacks to national and economic security, comparing the concern more directly than before to the dangers posed by global terrorism.

U.S. intelligence officials told a Senate hearing that the nation is vulnerable to cyber espionage, cybercrime and outright destruction of computer networks, both from sophisticated, government-sponsored assault as well as criminal hacker groups and cyber-terrorists. "It's hard to overemphasize its significance," Director of National Intelligence James Clapper said, addressing members of the Senate Intelligence Committee. "These capabilities put all sectors of our country at risk—from government and private networks to critical infrastructures."

Federal Bureau of Investigation Director Robert Mueller cited cyber-security as something that keeps him awake at night, saying at the hearing it "has grown to be right up there" with terrorism. The intelligence officials, in describing an annual inventory of global problems, didn't reveal imminent new cyber-threats or previously undisclosed plots. But they amplified their warnings by casting them in terms usually reserved for threats emanating from al Qaeda and Iran, and they included projections of where the danger is expected to lead in the next two years. WSJ reporter Siobhan Gorman says the recent cyber-attacks have revived concerns over U.S. vulnerability to foreign hackers. A key concern: how the government and business sector can defend themselves against future attacks.

The warnings came as part of an aggressive Obama administration campaign to draw attention to cyber-security and to stir action to counter infiltrations and attacks that officials have said could allow foes to commandeer a nuclear-power plant or disrupt the financial system.
Last month, President Barack Obama signed an executive order aimed at bolstering computer-network protections, and he noted the "rapidly growing threat from cyber-attacks" in his State of the Union address. "We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy," he said then.

The following week, the administration rolled out a strategy to combat the theft of trade secrets. And Monday, in a speech in New York, National Security Adviser Thomas Donilon singled out China as a top perpetrator, demanding it adopt international standards of behavior in cyberspace.
Chinese officials deny that Beijing engaged in such activities. On Saturday, China's foreign minister, Yang Jiechi, called for cooperation on cyber-security and said that China is a victim of cyber-attacks. "Cyberspace needs not war, but rules and cooperation," Mr. Yang said at a news conference. He said cyberspace shouldn't become a "new battlefield."

Mr. Obama discussed the issue with lawmakers when he met behind closed doors Tuesday with a group of Senate Democrats, participants in the meeting said. The administration push continues Wednesday when Mr. Obama holds a meeting with U.S. executives in the White House Situation Room to discuss cyber-security. But for all the collective worrying, there was little agreement between the Obama administration and Congress Tuesday over how to address the problem. At a second Senate hearing, before the Armed Services Committee, lawmakers tussled over the role of the federal government in guarding against threats. Army Gen. Keith Alexander, head of the U.S. Cyber

Command, a part of the military, acknowledged that the Obama administration is debating internally how to proceed when U.S. companies are under cyber-attack.
"The issue that we're weighing is: When does a nuisance become a real problem and when are you prepared to step in for that?" he said at the hearing. "That's the work that I think the administration is going through right now and highlighting that." Lawmakers, too, acknowledged they can't agree on legislative measures to bolster protections for computer networks. Last year, Republicans defeated a White House-backed bill that would have established voluntary cyber-security standards for companies running critical infrastructure such as the electrical grid, citing concerns about a government role in cyber-security.

Mr. Obama's executive order last month established voluntary standards as an interim measure, but the order lacks key incentives for companies to participate, like liability protections, that would require legislation. The cost of protections remains another stumbling block, particularly for power companies, Gen. Alexander said, as he provided a relative ranking of computer protections in private industry. "The banks and the Internet-service companies are pretty good; the power companies, not so good," Gen. Alexander said. In testimony before the House Intelligence Committee in February, Kenneth W. DeFontes Jr., chief executive of Baltimore Gas & Electric Co., told lawmakers that the electric industry takes cyber-security "very seriously."

Intelligence officials cited cyber-assaults last year on the websites of many U.S. banks and a more destructive attack on a Saudi oil company that destroyed 30,000 computers as examples of the kind of disruptions already taking place. They didn't discuss who mounted those attacks, but U.S. defense and intelligence officials have said the Iranian government is behind them. Iran has denied any involvement in the attacks.

"What we're seeing with the banks today I am concerned is going to grow significantly throughout the year," Gen. Alexander said at the hearing. Looking ahead, Mr. Clapper said that chances of an ultra-sophisticated attack capable of wiping out major nationwide computer networks are "remote." Countries most capable of carrying out such an attack—China and Russia—are unlikely to launch such assaults in the absence of a conflict or crisis, according to the assessment. But even relatively unsophisticated hackers were projected by the intelligence officials of eventually being capable of disrupting insecure computer networks running parts of vital functions—like the power grid. Cyber-attacks from "less advanced but highly motivated actors" could do great harm because of impacts on computer networks connected to the one under attack, the assessment concluded. U.S. intelligence has picked up indications that terrorists, too, are weighing cyber-attacks, according to the annual assessment.

Fear Factors

The government's annual intelligence review cites threats other than cyber-attacks:
- **Terrorism and organized crime:** A decentralized extremist movement still poses dangers.
- **Nuclear fears:** Iran may develop longer-range missiles that could carry weapons of mass destruction; North Korea is a threat to neighbors and the U.S
- **Space wars:** U.S. reliance on satellites for communications, navigation and surveillance could be undermined
- **Food, water, energy, minerals:** Natural disasters and growing competition tighten supplies.
- **Health and pandemic threats:** Pathogens jumping from animals to humans increases risks
- **Eurozone crisis:** Economic deterioration remains a threat.