# Silicon Valley at front line of global cyber war

June 4 2013, by Martha Mendoza

Chinese President Xi Jinping and American counterpart Barack Obama will talk cyber-security this week in California, but experts say the state's Silicon Valley and its signature high-tech firms should provide the front lines in the increasingly aggressive fight against overseas hackers.

With China seeking to grow its economy and expand its technology base, companies like Facebook, Apple, Google and Twitter are inviting targets. In fact, all have been attacked and all point the finger at China, which has denied any role.

The U.S. government has stepped up efforts to thwart cyber-attacks, but those efforts are mainly focused at protecting its own secrets, especially regarding military operations and technologies.

Paul Rosenzweig, a former Department of Homeland Security official whose Red Branch Consulting provides national security advice, said the responsibility for preventing attacks in the private sector lies with the U.S. innovators who created the technology that's being hacked in the first place.

"To some degree, they were getting a pass," he said. "If a car manufacturer made a car that was routinely able to be stolen, they'd be sued. If software is made with gaps that are a liability, they bear some responsibility, and in recent years there's been a sea change in high tech firms accepting that responsibility."

Big firms like Google employ thousands of security experts who can spot a potential attack on just a few individuals and quickly disseminate protection for everyone using their products. Google routinely detects unsafe websites that spread malicious software or trick people into revealing personal information, posting warnings in front of users and contacting webmasters who may have been hacked.

But Chinese hackers have managed to hit even Google, and in a book released this spring, Google's executive chairman Eric Schmidt said China is the world's "most sophisticated and prolific hacker."

Cybersecurity is high on the agenda for the meeting between Obama and Xi on Friday and Saturday in Southern California's Rancho Mirage. A recent government report found nearly 40 Pentagon weapons programs and almost 30 other defense technologies were compromised by cyber intrusions from China. Earlier this year, cybersecurity firm Mandiant linked a secret Chinese military unit to years of cyber-attacks against U.S. companies.

Mandiant's chief security officer, Richard Bejtlich, said his firm tracks more than 20 potentially threating groups of hackers in China, some with links to the government and military.

China's government denies any involvement, with Defense Ministry spokesman Geng Yansheng telling reporters Sunday that the U.S. claims "underestimate the intelligence of the Chinese people."

Frustration is growing, however, as the attacks continue. Although none have come out publically, analysts say some U.S. companies even are considering cyber-attacks of their own as retaliation, even though it's illegal. Retaliatory hacking was a hot topic at the 2013 RSA Conference on tech security in March, where attorneys and sitting judges even held a mock trial over an imaginary firm that struck back.

And on May 20, the Commission on the Theft of American Intellectual Property, headed by former U.S. Ambassador to China Jon Huntsman and former U.S. Director of National Intelligence Dennis Blair, recommended that Congress and the Obama administration reconsider the laws banning retaliation.

"If counterattacks against hackers were legal, there are many techniques that companies could employ that would cause severe damage to the capability of those conducting IP theft," they wrote.

Marc Maiffret, chief technology officer at security firm BeyondTrust in San Diego, warns against private firms going on the offensive.

"There are a lot of people lobbying to 'hack back' but I think that is a disastrous idea," said Maiffrett, who was a hacker of government sites before discovering the first Microsoft computer worm, "CodeRed."

"Most of corporate America is failing to secure themselves, let alone become competent hackers to hack back against someone like a China."

Tim Junio, who studies cyber-attacks at Stanford University's Center for International Security and Cooperation, doesn't expect much to change because of the Xi-Obama talks.

"China benefits too much by stealing intellectual property from the U.S., so it's really hard to imagine anyone convincing them to slow down," he said.

Indeed, the payoff for successfully stealing critical information can be enormous. For example, if a company spends many millions of dollars developing expensive intellectual property, such as a pharmaceutical firm investing in a new drug, it's very cost-effective for a Chinese firm or government entity to dedicate a small team of hackers to gain access

to that company's networks.

A patient approach of sending emails for months, hoping an employee eventually clicks on a link or opens an attachment that they shouldn't, usually works. It's a probabilities game, and the offense has the advantage, especially when targeting a company with thousands of employees. Sooner or later, someone will make a mistake.

Hackers then sell the stolen intellectual property to competing companies, which can try to replicate the product and sell counterfeits at a cut rate. For a developing country like China, this is a great way to stimulate domestic economic growth.

Junio suspects that China's political leaders may not even be aware of the extent of hacking by their own cyber teams, because corrupt government officials may also be using them for personal gain.

James Barnett, former chief of public safety and homeland security for the Federal Communications Commission, said the government's role in fighting Chinese hackers should be to offer high-tech firms tax deductions, credits or liability limits.

"The private sector's role is to continue to innovate, something it can do much better than the government, and something that Silicon Valley does better than just about anywhere in the world," he said.