Cyber threat: The Thief You Never See Coming

©John L. Mariotti 2013

The reports say that President Barack Obama and Chinese President Xi Jinping plan to discuss many important issues in their June "informal meeting." Few issues they will discuss are more important than the issue of cyber attacks and hacking, at which the Chinese have been long believed to be the greatest threat, but far from the only one.[1]

The irony is that Chinese President Xi will almost certainly take the position that the US is the worse offender, a position from which he can then blunt or neutralize Obama's grave concerns and warnings. Nothing could be further from the truth. Since I began studying this field in 1999, and continued while I wrote for my 2010 book (fact-based novel) *The Chinese Conspiracy*[2], China has a long and growing record of being tracked as the primary source of the worst and most pervasive cyber attacks globally.

In the intervening years, there have been many books, both fiction and non-fiction, which explored the use of cyber attacks for various illicit or evil purposes. The quote for the dust cover of my book, from retired CIA station chief, and former CIA/Defense Intelligence Program Manager Paul Broadbent, says it very well. *"…a glimpse into warfare of the future. The outcome of future wars will be determined far in advance of the actual conflict. This is but a preview of things to come."* He first gave me that quote almost a decade ago!

Fast forward to 2013, and consider the fact that millions of computer systems have been compromised and had information stolen from them. This includes systems such as the Department of Defense, The White House, The Department of the Army, and many, many more private sector systems, including Lockheed-Martin, where plans for the F-35 fighter aircraft were stolen before the plane ever flew a mission. Now imagine that America's enemies have such information, and worse yet, access to critical systems.

Most sophisticated hackers leave behind either a "back door" or a Trojan Horse—a remnant of code that lets them come back later, without being stopped or even detected. Now how that "leave-behind" could result in this imagined scenario:

> *…Your cell phone doesn't work. Neither does your landline, or your Internet. Your cars navigation system can't find a GPS signal. Satellite and cable TV signals keep dropping out. Your bank's ATM access is unavailable and the NYSE ticker is showing no activity. Airline reservation systems are down, or acting strangely. Mysterious, intermittent power blackouts are plaguing major cities, especially Washington, DC and New York. And that's not all…*

[1] http://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms

[2] http://www.amazon.com/The-Chinese-Conspiracy-ebook/dp/B00472O93G/ref=sr_1_1?ie=UTF8&qid=1370355184&sr=8-1&keywords=The+chinese+conspiracy

What do all of these events have in common? They are all systems controlled by computers, virtually all of which are networked. If a hacker can penetrate the first few, the others become easier as the malware is spread via the network. Since the military also uses GPS heavily, and relies on special computer systems, it has been either shutdown or dramatically limited. Author Tom Clancy describes this latter scenario in his latest novel, *Threat Vector*[3].

Experts like Richard Clarke, a former high-ranking US government official have warned about such events for a decade—before and after he left government service, during the terms of presidents Clinton, Bush and Obama. His 2010 book, *CyberWar*[4], explains the problem and offers some potential solutions.

Finally, lest we think that cyber threats are localized to China, they are not! As far back as 2000 Algerian hackers stole millions of dollars in unpublicized bank attacks. The global monetary trade, trillions of dollars each day, is now completely done with vulnerable computer networks.

The first known call for fatwa and cyber-jihad was reported in 2000.[5] A more significant fatwa came in 2008 from the Fatwa Committee of al-Azhar University in Egypt. This is Sunni Islam's most influential body, and this fatwa supported hacking/damaging American and Israeli web sites. This kind of fatwa was echoed on-line by Saudi preacher Salman al-Odah in 2008. Then in June 2011, the leader of the Kuwaiti branch of the Muslim Brotherhood, Dr. Tareq al-Suwaidan called for electronic jihad against Israel.

Most concerning of recent reports was last month, when the underground groups Tunisian Cyber Army and al Qaeda Electronic Army announced via Twitter that they had hacked the Pentagon, the State Department and the Department of Homeland Security web sites as part of their #opBlackSummer campaign—one that they promise will continue.

Meanwhile, back at home in America, most of the millions of smartphones remain totally unprotected. Most do not even use a lockout security code. Millions of home computers and tablets, which access the Internet daily and send/receive email constantly, have little of no protection. As American workers "bring home work" from their jobs in either the government of the private sector, any robust security that might exist at work is compromised or circumvented.

[3] http://www.amazon.com/Threat-Vector-Jack-Novels-ebook/dp/B0095ZMMCK/ref=sr_1_1?s=books&ie=UTF8&qid=1370355279&sr=1-1&keywords=Threat+vector

[4] http://www.amazon.com/Cyber-War-National-Security-ebook/dp/B003F1WMAM/ref=sr_1_1?s=books&ie=UTF8&qid=1370355330&sr=1-1&keywords=Cyberwar

[5] http://online.wsj.com/article/SB10001424127887324744104578475571183053736.html?KEYWORDS=China+isn%27t+teh+only+source+of+cyberattacks

Even the most secure military systems depend on the “air gap”—separation of the secure networks from public ones because there is no physical connection. The simple act of copying a malware-contaminated file onto a flash drive and then plugging that flash drive into secure network computer, effectively defeats the “air gap” protection. When people work at home, this is a common security failure. When people work on non-secure WiFi away from home, a similar risk can occurs. Lost or stolen computers can also lead to cyber-penetration.

The question is not “will some enemy inflict a massive cyber attack on America?” The question is “When?” And “how bad will it be?”

Forewarned is forearmed. The next war we will be fighting will be using bits and bytes, and not bullets. Be ready for the day when everything electronic is disrupted—it’s coming!