Hearing date: 15 June 2015

Dennis F. Poindexter

Testimony before the U.S.-China Economic and Security Review Commission

Panel II, Commercial Cyber Espionage

A worker in a Chinese factory made a simple statement that got my attention. When she held up an iPad she was working on, and looked at the camera, she said, “Take care of this. We work hard to make it, and we want it to last a long time.” I took better care of mine after that.

Most of the country believes the Chinese people are like us, and they are right about that. They are hard-working people, who work for less money than we do, make fantastic products that are popular in the world. But at that company, twenty of those workers had committed suicide the year before. The nets to stop others from doing the same thing were still up.

What we see most often is not the Chinese government. We are seldom reminded that China is one of the few Communist countries left in the world, and it is comfortable with that. We don’t think about what that means very often. Their Army, Intelligence Services and senior government leaders are inseparable, centrally managed, and not very prone to criticism. In their government, it is wise to know how far a person can stretch his independence before making a leap.

We don’t have an office of population control and could not imagine what that could be useful for. We don’t have a censorship bureau either, but we contemplated one once during the Reagan Administration.

In China, there are many state-owned businesses (though a decreasing number). There is differing opinions about how successful the private sector is, and whether it is more successful.[1] The leaders send their sons and daughters to the best schools, most of them in the U.S. Spouses and relatives of ranking party members run some of those “private” businesses, and the Chinese have adapted their definition of “state-owned” to remove many companies that were once on that list. This Committee has heard testimony on the 88 Queensway group that

[1] Nicholas R. Lardy, Markets over *Mao: The Rise of Private Business in China,* The Peterson Institute for International Economics, September 2014

operated several businesses out of the same address, and one of those was a front company for their Intelligence Services.[2]

Internet Service Providers have to sign agreements to support the efforts of the central government, and employ censors to help do that. Google did not particularly like having censorship rules applied to its global content and our news media are even less enamored with the idea.

The Chinese see the Internet as something to be managed and controlled, where we see it as a vehicle for disseminating information and sharing communications and ideas. They have the well-known Great Firewall and Great Cannon, but the lesser-known *Golden Shield*. The latter is an interesting mix of a surveillance network that would combine the National, Regional and Local police and security agencies to monitor every citizen of China. They can match data against the new national ID cards carried by everyone.

If we combined the Federal agencies involved in national security, law enforcement, prisons, jails and border patrols, personnel management, traffic management, crime statistics, fugitive warrants, foreign affairs management, combined them with the Task Forces, state vehicle departments, and regional police, and linked in the local police forces, we might be able to have something close to what they were trying to build.

In 2009, China went so far as to require the installation of software called Green Dam in all computers made there. It would have allowed monitoring and manipulation of data on any computer made in China. The World Trade Organization finally ruled against them on trade grounds, but there are still 53 million PCs in China, with the software *voluntarily* installed.[3] They think big, and… they are not the same as we are.

If the Chinese have done half of the things attributed to them by cyber security companies, the Federal government, and private individuals like myself, they are the most active cyber thieves in the world. That characterization allows some to interpret what the Chinese are doing as solely criminal.

[2] See Lee Lekowitz, Martella McLellan Ross and J.R. Warner, *The 88 Queensway Group: A Case Study in Chinese Investors' Operations in Angola and Beyond*, U.S.- China Economic and Security Review Commission, U.S. GPO, January 2011 & *National Security Implications of Investments and Products from the People's Republic of China in the Telecommunications Sector*, January 2011. Operations in Angola and Beyond, July 10, 2009

[3] Openet Initiative, *China's Green Dam: The Implications of government Control Encroaching on the Home PC*, https://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc

Over the past few years, we have come to accept that China is hacking a wide variety of industries and stealing both strategies and intellectual property, but they steal more than that.[4]

In President Obama's run against Senator McCain, the Chinese hacked both candidates and their staff for position papers and plans. They look for thought leaders in business, military, and governments and they monitor their positions over time. They are patient.

They aren't just hacking businesses. They have hacked industries that support our government and contractor personnel, like processors of security clearances, insurance companies, healthcare, defense, computer security, educational institutions, and information technology at all levels. They probably know more about our military, business, and government personnel than we do.

They steal teaming arrangements, pricing, and competitive intelligence. More importantly, they took source code, from commercial and government sites.[5] Source code is the original that is used to make object code the computer can use. Source code is useful to them for two reasons: first, they can shortcut production by copying, selling and profiting from it: second, they can modify it for reentry into the system. It looks like the original, functions like it, and does more than the original. Neither of those is good for us.

We tend to think of this as crime, but this is not crime in the way we are used to. It is preparation for a new kind of war. A popular Chinese author says that this is a strategy of Information War that uses three elements (warfares), psychological, media, and information operations, to manage its enemies.[6] One of those enemies is the U.S.

The Chinese used attacks on the Washington Post, New York Times, and Bloomberg teaming partners to dry up their sources in China. This year, they fired up their Great Cannon to blast companies serving up content like the Chinese language version of the New York Times. They apparently see something seriously wrong with the Times.

But the important thing is they are not content to manage only their own content; they want to manage ours. It gets harder to control as communications bypass governments and go directly from one person to another. Governments find it more difficult to track down any single individuals in millions of e-mails, Twitters,

[4] See *APT 1: Exposing One of China's Cyber Espionage Units* , APT 17: Hiding in Plain Sight: FireEye and Microsoft Expose Obfuscation Tactic and Operation for different perspectives on the extent of Chinese hacking. Mandiant is a FireEye Company.

[5] Examples are Avago, Google, American Superconductor Corp., Adobe, Cisco, U.S. Treasury Department

[6] Bill Gertz, *Chinese Colonel on Information War,* The Washington Times, 4 June 2015

and postings on Facebook, but it is something they are capable of, given improvements in monitoring technology.

Cyberwar is partly the use of that technology. Intelligence Services and covert operations increasingly fight Cyberwars, but our military defined it. Colonel Liu Mingfu, in his book *The China Dream*, mentioned that word “covert” when describing the three types of warfare. Being covert is essential to plausible deniability. Governments know how this works.

Our military believes cyber weapons can make war and has described a broader concept of Information War since the late 1980’s, exercising those principles by the early 1990’s.[7] In our doctrine, this is Information War, though Cyberwar has begun to replace Information War as a term of reference. Part of Information War is Economic Warfare, where the Chinese seem to spend most of their time, doing admirable work.

They would argue that none of the things we see are war. In fact, China says it does none of them. We can say, in aggregate, they are attempts to manipulate us to accept their will. The Spratly Islands are the best example of current events that have been managed to allow China to achieve a political objective that few countries agree should have been successful. Hacking the countries around the South China Sea, lets them find out what the governments’ positions might be, and influence them accordingly.[8] In the meantime, they built up the islands and armed them. They are good at managing perceptions, until it is too late.

There is some disagreement as to whether cyber weapons can be used to make war, regardless of their capabilities. [9] It is easy to understand those arguments, and call what our enemies are doing “cyber espionage”, “monitoring”, “economic competition”, or another less sensitive word that does not imply a threat to our national security. It is easier to describe it that way, but not as accurate.

Leon Panetta recently left no doubt that disruption of our power grid or other types of direct attack against our infrastructure would be an act of war.[10] The Defense Department has described its response to cyber attacks as having the same potential for “use of force” as conventional attacks.[11] If cyber weapons are

[7] Martin C. Libicki, *What is Information Warfare?* National Defense University, August 1995, page 1.

[8] Geok Meng Ong, Kenneth Geers, *APT 30: The Mechanics Behind a Decade Long Cyber Espionage,* FireEye Labs, 2015

[9] See Gal Beckerman, *Is Cyberwar Really War*, Boston Globe, 15 September 2013

[10] Jake Tapper, A Crippling Cyber Attack Would be an ‘Act of War’, This Week, ABC News, 27 May 2012

[11] Siobhan Gorman, *Cyber Combat: Act of War*, The Wall Street Journal, 31 May 2011

not war, we could not have a reason for war that stems from their use. Yet, the most difficult question to answer is not “Is it war?” but “Is a military response appropriate?” Cyberwar has changed considerably since these doctrines were published. The new version is more refined, subtle, and less oriented to military use.

We really hadn’t been paying attention to what they were doing until five years ago, when Google reported some problems in China. The Do-No-Evil guys were asked to filter some of their search results so certain types of things, like the term Falun Gong, would be missing. There was a long list of other things. Google objected.

After escalating problems, China hacked Google looking for dissidents on Gmail, and some of that source code. After that, security companies and governments started looking for how they got in.

While the good guys were looking, they found something called *Ghostnet*, a China-based network used for hacking. This happens often in cyber operations and is testament to its current state. One of the targets was the Dalai Lama and the information being stolen was coming from eight country’s embassies. They got 1500 of his personal letters. They got his intentions, his partners, and his plans. From that they can predict what he is going to do. China controls the distribution of ideas, modifies them to suit their own needs, removes them, or allows access to them and monitors those who have it. They manage thought leaders; sometimes with rewards for publishing what they want, other times by threats or jail. The free exchange of ideas is not free.

The Information Warfare Monitor et al, published two reports, a year apart[12] in the first one, they said it *might be* China; in the second, they said it *was* China who went after the Dalai Lama. This is because attribution has gotten better. Attribution, the ability to say with some certainty that is responsible for an event got considerably better after 2010. We are just now finding all the things that were done years ago.

We have whole industries that think they are capable of protecting their data from people intent upon taking it, when they almost always turn out to be wrong. They are competing with well-financed government operations, not other businesses. We are not well prepared to do that.

When Chinese hackers got into DoD’s unclassified NIPRNET in 2007, the Defense Department downplayed it as a network carrying only unclassified information. If this type of data were not valuable, there would be no reason to

[12] Information Warfare Monitor, et.al, Shadows in the Cloud, 6 April 2010

have a costly network to put it on.[13] At the same time, the UK's Ministry of Defense was saying it was concerned about attacks against its Top Secret networks. [14] He added that these systems were not connected to the Internet. This belief that we can be separated from the Internet is common, but not practiced very well. We leak almost everywhere, yet business and government leaders swear they are secure.

If networks were static, we could say with certainty whether something was connected to the Internet and be sure that when we went back to check, a year from now, that it might not be true. In business, commercial network mapping was even more surprising, with some of our customers unknowingly having basic research accessible from the Internet, or committing financing to companies that were ill suited for operation in such a hostile environment. One large aggregation of networks had over 200 back-door connections. The Chinese have thousands of targets of opportunity, and they don't have the same trouble with their networks.

The Chinese manage a disciplined national architecture, using state-owned telecommunications companies to support centralized monitoring and manipulation of large quantities of data (Google-sized efforts). They prohibit Virtual Private Networks to expose any traffic to scrutiny.[15] That provides a safe haven for their operations. They can't say they don't know who is hacking us.

The Chinese are allowed to plow what they get - back into the economy. That part of the playing field is not level.

This is not a technical problem; it is a political one. We know who the Chinese are stealing from and how they are doing it. We know how they have made it more difficult for industries to operate in China. We know what industries they want to dominate and the consequences if they do. What we don't know is what to do about it.

The main difference between our political system and theirs is how we apply what we know. They are perfectly willing to use stolen technologies to set up competition for our business sectors. They use their Intelligence and military functions, university research centers, enhanced with state-owned businesses, to gather the information and apply it. Then, they deny everything, and say, "Prove it".

[13] Robert Marquand and Ben Arnoldy, *China's hacking skills in spotlight*, Christian Science Monitor, 16 September 2007.

[14] Nick Hopkins, *Hackers have breached top secret MoD systems, cyber-security chief admits,* The Guardian, 3 May 2012

[15] George Chen et.al. *China's Great Firewall Is Rising*, Foreign Policy, 3 February 2015

We can do better.

We have business leaders who think we can “out innovate” China no matter what they do. I’m not sure I want to bet on them being right.

We manage our health, reading materials, news, banking, home security, supply chains, travel, taxes, and a range of astounding new vehicles that may drive themselves on an Internet of Things – on an Internet that we can’t trust. We need to devise better ways to separate ourselves from it, keep foreign governments from using it against us, while still allowing for us to use it as a communications and information medium.

Industry and government both have roles to play. They can focus much better together, than working on their own. Our own National Security depends upon that cooperation.

This statement has been approved for public release by the Office of the Director of National Intelligence. The views expressed in answers to questions are solely my own personal opinions, and not those of the Intelligence Community or United States Government.