Is Our National Security Under an Ever Increasing Cyber Threat?

by Ira Wilsker

WEBSITES:

http://en.wikipedia.org/wiki/Edward\_Snowden

http://www.nydailynews.com/news/national/snowden-chinese-hackers-stole-f-35-fighter-jet-blueprints-article-1.2084888

http://abcnews.go.com/Blotter/major-us-weapons-compromised-chinese-hackers-report-warns/story?id=19271995

http://www.theepochtimes.com/n3/1207688-snowden-reveals-more-bad-news-for-the-400-billion-f-35/

http://www.spiegel.de/media/media-35687.pdf

http://time.com/3761786/5-facts-explain-iran-nuclear-talks-sanctions/

As many of you have seen firsthand, I have been doing a series of free presentations for local and national groups titled "Are We Under Cyber Attack?" With the constantly increasing volume of information that has indicated that we are indeed under an increasing level of cyber attack, it has been difficult for me to keep my presentation up-to-date without it becoming an excessively long presentation. Sadly, most of us are blissfully unaware of the degree and scope that our computer systems are being hacked and penetrated, with massive amounts of personal, technical, and other sensitive information being stolen. It is not just the massive theft of computer data that has been damaging our national security and economy, but the increasing number of cyber attacks that have threatened our critical infrastructure as well as jeopardized our collective personal safety.

Some of the previously rumored but denied digital intrusions into our most sensitive data systems important to the national security have been recently corroborated (if credible) by such questionable and controversial individuals as Edward Snowden and WikiLeaks infamous contributor, Julian Assange. As recently as January 20, 2015, Edward Snowden was quoted in an interview in the New York Daily News where he proclaimed that despite earlier news reports that were officially denied, some going back more than six years, that Chinese hackers stole the complete blueprints and other technical data for the U.S. F-35 stealth jet fighter and used that information to build a near clone of the F-35, the new Chinese J-31 stealth fighter. According to the Daily News, "Chinese hackers stole “many terabytes” of data about the American F-35 stealth fighter jet, new documents provided by NSA whistle-blower Edward Snowden contend. The stolen materials, taken from the Pentagon and contractor Lockheed Martin Corp., included radar designs and engine schematics used in the crown jewel of American military aircraft." On January 19, 2015, the international newspaper, Epoch Times in reporting the theft of F-35 data commented, "This is billions of dollars of combat advantage for China. They’ve just saved themselves 25 years of research and development. It’s nuts.”

Officially, the Chinese vehemently deny that they are engaged in any form of cyber espionage and hacking of any American facilities. Despite the fact (allegation?) that the Chinese military stole data developed by the U.S. at the cost of many billions of dollars, and used that purloined data to produce a highly competitive air superiority fighter in record time without the enormous expense and lengthy time for research and development, there is still much disbelief that it could have happened. In response, again quoted by the New York Daily News, China's Foreign Ministry spokesman Hong Lei told reporters, "The so-called evidence that has been used to launch groundless accusations against China is completely unjustified. According to the materials presented by the relevant person, some countries themselves have disgraceful records on cyber-security, Hong added." The Daily News also wrote in the January 20 article, "China, meanwhile, boasted of its Shenyang J-31 twin-engine fighter jet when the aircraft was unveiled late last year, prompting the aircraft’s maker to claim the jet could “take down” America’s F-35."

The documents released by Snowden also appeared to verify an earlier ABC News story on May 28, 2013, where ABC reported, "Among the more than two dozen major weapon systems listed in the report are the stealth F-35 Joint Strike Fighter aircraft program, the most expensive weapons program in history whose breach was previously reported; the Global Hawk long-range surveillance drone; aspects of the Patriot missile system; the Navy's Littoral Combat Ship and Black Hawk helicopters. Information on various U.S. government technologies was also siphoned by cyber spies including nanotechnology, directed energy, space surveillance telescopes, tactical data links and drone video systems." ABC also reported in this story, "The Chinese government has repeatedly called hacking accusations "groundless" and has claimed to be the victim of a widespread American cyber espionage campaign."

To show the depth of the "alleged" Chinese thefts of important and vital American national defense and security information, the German newspaper Der Spiegel published on January 18, 2015, some of the PowerPoint slides purloined by Snowden, and provided by him to the newspaper (http://www.spiegel.de/media/media-35687.pdf). These slides were also picked up by a British newspaper the Daily Mail, and distributed globally, then reposted by countless others. Clearly labeled as "Top Secret" and titled "Chinese Exfiltrate Sensitive Military Technology", and "Byzantine Hades Causes Serious Damage to DOD Interests", the PowerPoint slides state that the Chinese have stolen about 50 terabytes of data, which is the "Estimated equivalent of five Libraries of Congress". Some information on these slides indicates the details of some of the stolen technical data on the U.S. F-35 Lightning including the numbers and types of radar modules, detailed engine schematics, methods of cooling engine gases (important to minimize an infrared signature that can be used to track and shoot down an F-35), leading and trailing edge treatments, and other vital technical date that could be utilized to defeat the stealth technology engineered into the F-35, at a cost to the U.S. taxpayers of $400 billion.

Other statistical information disclosed in these "Top Secret" PowerPoint slides indicate that there were over 30,000 "Incidents", including over 500 "Significant Intrusions in DoD Systems"; over 1600 networked computers penetrated, and over 600,000 user accounts compromised. It cost the Defense Department over $100 million to access the damage, and rebuild the compromised networks.

Operational data on the PowerPoint slides consisted of compromised information which included air refueling schedules, the personal records of 33,000 Air Force generals and other field grade officers, over 300,000 user IDs and passwords used by Navy personnel; Navy missile navigation and tracking systems; and Navy nuclear submarine anti-aircraft missile designs. Other highly critical and sensitive data stolen also included International Traffic and Arms Restrictions (ITAR) data, information on defense contractors' research and development, and active defense industrial espionage on the B-2 bomber, F-22 Raptor fighter, F-35 Lightning stealth fighter, spaced based laser systems, and other valuable data. Snowden also provided "Top Secret" PowerPoint slides titled "Cyber Attack and Mitigation Timelines" which explains the "Adversary Malware Design Process", as well as the "SIGINT" (Signals Intelligence) enabled countermeasures used to mitigate the "Adversary Intrusion". Obviously, after these PowerPoint slides were published by major German and British newspapers, and then reposted countless times on other websites, the proverbial "Genie" is out of the bottle, as these slides are now readily available online.

On March 27, 2015, Time Magazine ran a story titled "These 5 Facts Explain the State of Iran". Fact #2 listed about Iran has to do with "splurge" of money being spent to make Iran what its Revolutionary Guard called “the fourth biggest cyber power among the world’s cyber armies.” In its domestic 2015/2016 budget, Iran is increasing its spending on cyber security by 1200%, but has increased spending on its offensive cyber capabilities to well over a billion dollars a year. In response to the mysterious Stuxnet virus (worm) that damaged many of the centrifuges producing nuclear material, Iran intensified its cyber attack capabilities. In 2012, Iran demonstrated its cyber attack capabilities by deleting critical data from about 30,000 computers in Saudi Arabia belonging to the oil company Aramco, in what is now call the infamous "Shamoon Attack." In the past, while the majority of cyber assaults on American assets were predominately from China, followed by Russia, and other mostly unfriendly countries, there is now evidence that the Iranians may also be contemplating significant cyber attacks on the U.S.

So, "Are we under cyber attack?" I end each of my hour long presentations with the statement, "Sleep well tonight!"