TriCorner News
from The Lakeville Journal, The Millerton News and The Winsted Journal
Published on *TriCorner News* (http://tricornernews.com)

Charles R. Church is an attorney who devotes most of his efforts to human rights issues: detention, torture, the facility at Guantanamo Bay, habeas corpus, etc.
His website is: www.churchlawllc.com
Email him at: charleschurchllc@gmail.com

The quiet war few have heard of — until now

Thu, 06/06/2013 - 10:46am Field Notes From A Battleground [1] Opinion/Viewpoint [2]
By Charles R. Church

For years now, news articles, primarily at outlets devoted to national security, have told of massive quantities of intellectual property being looted by the Chinese (and others) through cyber attacks on major corporations in the U.S., though who specifically was doing the stealing was left unclear. But now alarms are blinking red, as mainstream media outlets blare headlines about cyber attacks on companies such as Apple, Microsoft, Citibank and Google, and on media giants such as the New York Times, the Washington Post and the Wall Street Journal. Even the Federal Reserve's computer services have been breached.

Ominously, these accounts also describe the looming military threat from targeting our infrastructure, power grids taken down and natural gas compressor stations blown up. One actual victim was Telvent, which designs software that gives oil and gas pipeline companies as well as power grid operators remote access to valves, switches and security systems. Cyberspies have targeted Washington journalists, lawyers and human rights workers with access to political actors, seeking insights into how our federal government works. Now, for the first time, a finger is being pointed directly, for the trade secrets pillaging at least, at China's Communist Party and the People's Liberation Army, with details being provided on how they do it. The Chinese are pushing back with expressions of incredulity and accusations of their own.

Why this sudden shift? For one thing, major corporations that never disclosed these attacks are now doing so. Also, a blockbuster Feb. 19 report by the private computer security firm Mandiant builds a robust, though circumstantial, case based on digital forensic evidence that China's People's Liberation Army for years has been running an extensive cyber espionage and data theft campaign against organizations around the world. It does this through what is called an Advanced Persistent Threat, or APT, which can overwhelm a cyber defense system by the sheer volume and duration of assaults. With what has been dubbed APT 1, the Army has systematically stolen hundreds of terabytes (each about a trillion bytes) of data from at least 141 organizations, spanning 20 major industries that match those China has identified as strategic to its growth. Through analyzing the group's intrusions over seven years, Mandiant tracked APT 1 to four large networks in Shanghai, two of which are in the Pudong New Area, where People's Liberation Army Unit 61398 has a large facility.

APT 1 swipes large volumes of intellectual property, including technology blueprints, manufacturing processes, test results, and business plans. Increasingly, its focus has been on companies involved in the critical infrastructure of the United States — the power grid, gas lines

and waterworks. Employing malicious software for “spearphishing,” APT 1 first establishes access by enticing a business leader to open a malicious file from an innocuous-seeming email, so a “backdoor” is established. APT 1 revisits every so often, all the while deploying custom digital weapons, then exports compressed bundles of files.

The January 2013 Defense Science Board’s Task Force Report on “Resilient Military Systems and the Advanced Cyber Threat,” like so many Department of Defense (DOD)reports, is chilling. In brief, it says the U.S. cannot be confident that our IT systems will work under attack from a “sophisticated and well-resourced opponent using cyber capabilities in combination with all of their military and intelligence capabilities.”

Adversaries have had success penetrating our networks. In war gaming, Red Teams (our people, pretending to attack us) have experienced “relative ease in disrupting, or completely beating, our forces in exercises using exploits (cyber attack tools) available on the Internet.” And, “DOD and its contractor base have already sustained staggering losses of system design information incorporating decades of combat knowledge and experience that provide adversaries (with) insight to technical designs and system use.”

An “existential cyber attack” is seen as possible. That’s an attack capable of causing sufficient widespread damage for the government potentially to lose control of the country. Naturally, there is a risk reduction strategy, and nuclear weapons “would remain the ultimate response.” Here’s the bottom line: “It will take time to build the capabilities necessary to prepare and protect our country from the cyber threat. We must start now!”

All of which makes this child of the 1940s-50s sigh, “Here we go again.” Can we keep our heads this time?

A little common sense helps. Given their enormous investments in the U.S., no one expects the Chinese to launch a cyber attack to inflict calamitous damage on our economy, for such an attack would damage Chinese investors severely. Russia, too, is deemed unlikely to attack. In both cases, however, a March 12, 2013, report to the Senate Select Committee on Intelligence notes this exception: “outside of a military conflict or crisis they believe threatens their vital interests.” Iran and North Korea present different stories, but lack the technical expertise and operational sophistication required for such an attack.

America has not been a quiet bystander. It has long been known that the U.S. and Israel deployed malware called Stuxnet to disrupt Iran’s uranium enrichment program. Thomson Reuters on March 10 told of China’s claim that the U.S. originated more than half the hacking attacks on China in the first two months of 2013. Who knows what else we have done secretly?

Another day in the life of this dangerous world.

Charles R. Church is an attorney practicing in Salisbury who focuses primarily on Guantanamo Bay, detention, torture, habeas corpus and related issues.

[1] http://tricornernews.com/category/opinion-author/field-notes-battleground
[2] http://tricornernews.com/category/articlead-category/lakeville-journal/opinionviewpoint