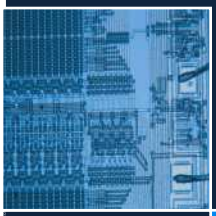
2009

The U.S. – China Economic and Security Review Commission



Opening Statement

of

Kevin G. Coleman, Senior Fellow at Technolytics

April 30th, 2009

The Technolytics Institute
4017 Washington Road
Mail Stop #348
McMurray, PA 15317
www.technolytics.com

The Technolytics Institute (TTI) has an international reputation for excellence in cyber security, cyber warfare and cyber terrorism that extends over the last decade. This program has included past and present thought leaders within the fields of computer hardware, computer software, networking and internet technology and supportive disciplines. TTI has sponsored and funded ground breaking research that has helped define the field of cyber aggression and continues to be at the forefront of investigation with our proprietary sources and methodologies.

U.S.-China Economic and Security Review Commission

About: The Commission was created on October 30, 2000 by the Floyd D. Spence National Defense Authorization Act for 2001 § 1238, Pub. L. No. 106-398, 114 STAT. 1654A-334 (2000) (codified at 22 U.S.C.§ 7002 (2001), as amended by the Consolidated Appropriations Act, 2008 (regarding changing the annual report due date from June to December), the Treasury and General Government Appropriations Act for 2002 § 645 (regarding employment status of staff) & § 648 Pub.L. No. 107-67, 115 STAT. 514 (Nov. 12, 2001); as amended by Division P of the "Consolidated Appropriations Resolution, 2003," Pub L. No. 108-7 (Feb. 20, 2003) (regarding Commission name change, terms of Commissioners, and responsibilities of Commission); as amended by Pub.L. No. 109-108 (enacted Nov. 22, 2005) (regarding responsibilities of Commission and applicability of FACA).

Purpose: To monitor, investigate, and submit to Congress an annual report on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China, and to provide recommendations, where appropriate, to Congress for legislative and administrative action.
Public Law 109-108 directs the Commission to focus its work and study on the following eight areas: proliferation practices, economic transfers, energy, U.S. capital markets, regional economic and security impacts, U.S.-China bilateral programs, WTO compliance, and the implications of restrictions on speech and access to information in the People's Republic of China.

Hearing: "China's Propaganda and Influence Operations, Its Intelligence Activities that Target the United States and the Resulting Impacts on U.S. National Security"

Co-Chairs: Commissioner William Reinsch and Commissioner Peter Brookes

Date: Thursday, April 30th, 2009
Location: Room 485, Russell Senate Office Building
Delaware and Constitution Avenues, NE
Washington, DC 20510

Panel V: China's Cyber Espionage Directed against the United States

This document provides a discussion of the employment of computer network exploitation by PRC state or state-affiliated entities to obtain information from the U.S. government, contractors, and industrial computer networks.

OPENING STATEMENT

It is both an honor and a privilege to be here today and address such a critical issue that is central to the national security interests of the United States. During the later stages of my tenure as Chief Strategist of Netscape, the company that pioneered the commercialization of the Internet, I became awakened to the darker side of what we were creating. From that point on I began my research and analysis efforts in the areas of cyber security, cyber espionage, cyber terrorism and cyber warfare which continues to this day. China's military strategists view our dependence on space assets and information technology as "soft ribs" and a strategic weakness. That begs the question –what are they basing their view on?

Less than a week ago I was to be face to face with my Chinese counterparts or cyber adversaries if you will, that I have researched and analyzed for years. The Chinese representatives included Mr. Hou Yinming, Delegation Leader and Former Director of the prestigious Zhang Ya Da Electronic Research Center, Major General Wang Baocun, PLA (ret), Professor Wang Xiangsui, Director of the Beijing University of Aeronautics & Astronautics Center for Strategic Studies and co-author of "Unrestricted Warfare" and finally Mr. Shen Weiguang, referred to as "the father of China's information warfare." At the last minute, only one Chinese panelist was allowed. The others were denied permission to attend by their government bosses. Clearly, they were concerned about the opposing panelists and there may have been other considerations as well. I might add timing was bad for them – given the disclosure of their scanning of the power grid and the discovery of a cyber spying network in 103 countries.

I'd like to start by discussing current observations before moving to ongoing initiatives. For far too long, cyber attacks, cyber terrorism and cyber warfare have been perceived as too complex an issue and a risk that could not be managed. Many others believe that until we experience the massive disruption that will surely follow a successful cyber attack, we do not possess the intestinal fortitude to take the actions necessary to help mitigate this risk. Another contingent believes reports of these threats are overblown and need not be addressed. It is my belief that this threat is real and we must take a proactive posture on acts of cyber aggression and espionage. For over two decades, China has been attempting to do what the Soviet Union never accomplished; covertly acquire western technology, then use it to move ahead of the west. I offer the following three observations that I feel are critical when discussing acts of cyber aggression and espionage.

1. Cyber espionage is a serious and evolving threat that demands immediate attention. In a report authored by Cambridge University it said that sophisticated computer attacks have been "devastatingly effective" and that "few organizations, outside the defense and intelligence sector, could withstand such an attack." We have all heard the comments and warnings from Dennis C. Blair - Director of National Intelligence, General Kevin Chilton - Commander of U.S. Strategic Command, MI5 – the Intelligence Service in the United Kingdom and many others throughout the world have even warned of successful cyber espionage activities against hardened systems that are said to have been traced to China. Perhaps the most troubling acknowledgement came when the

Wall Street Journal broke the story about the Chinese and Russians conducting cyber intelligence reconnaissance and mapping the nation's electrical power grid.

There are other reports of malicious code being found in the computer systems of oil and gas distributors, telecommunications companies, financial services industries and other pieces of our infrastructure. In February of this year I warned of acts of cyber terrorism against our water treatment and distribution systems in my presentation at the United Nations. Former CIA operative Robert Baer has publically stated that the "foreign intelligence service has been probing our computers, our defense computers, our defense contractors, our power grids, and the telephone system. ... I just came from a speech at the National Defense University and they were hit by the Chinese trying to get into their systems." What will it take before we realize the serious nature of these acts of espionage and again I must ask – What constitutes an act of cyber war? I asked that question a long time ago, former DHS Secretary Chertoff asked that question again in November of 2008 and we still do not have an answer!

2. At the 10th National People's Congress in 2003, the Chinese army announced the creation of "information warfare units." General Dai Qingmin said internet attacks would run in advance of any military operation to cripple enemies. Clearly cyber intelligence is a critical component of China's military arsenal. Cyber espionage officially arrived on Capitol Hill when two Republican congressmen, Rep. Frank Wolf of Virginia and Rep. Christopher Smith of New Jersey, went public with the news that in 2006 and 2007 their office computer networks had been breached by Chinese hackers. And also when Commerce Secretary Carlos Gutierrez, who was in China on a trip with a U.S. trade delegation last December, had his laptop slurped by Chinese cyber operatives. Not much happened after those two events. It was seen as just two of the many covert acts that take place in networks that connect the billions of computers and related devices globally. Perhaps the recent discovery of a vast Chinese cyber espionage network (code named GhostNet) that penetrated 103 countries, infected nearly 1,300 computers, and continued to infect at least a dozen new computers every week, will provide the wake-up call. I ask Solutionary, a security advisory client of ours and top ranked managed security services provider (MSSP) to pull some data about acts of cyber aggression that were tied to China. In March of this year, their security operations center (SOC) identified 128 acts of cyber aggression against their clients every minute that were tracked back to IP addresses in China. These acts should serve as a warning that clearly indicates just how far along China's cyber intelligence collection capabilities are.

3. Hardware is just as susceptible as software is to hackers through the inclusion of malicious logic; and the consequences of such an attack could be serious! One year ago this month, I wrote on a blog site (DefenseTech's Cyber-Warfare) about the growing number of concerns over backdoors and malicious code or circuitry hidden inside of counterfeit hardware and software -- all the way down to the BIOS and instruction set inside of integrated circuit chips. Last month we saw a flurry of articles about vulnerability in the BIOS of microprocessors that could be exploited to gain control over the computer. Hidden malicious circuits provide an attacker with a stealthy attack vector.

Commercial suppliers are increasingly moving the design, manufacturing, and testing stages of Integrated Circuit (IC) production to a diverse set of countries, which is making the securing of the IC supply chain infeasible. Together, commercial off-the-shelf (COTS) procurement and global production lead to an increasing risk of covert hardware/firmware based cyber attacks.

The extraordinary effort required to uncover such high-tech covert acts combined with the massive number of chips we would have to test and validate from a circuitry and microcode perspective, as well as the need to scan through tens of millions of lines of code and validate each software instance on billions of devices come together to make ensuring the integrity of our systems nearly impossible. Security must be designed and built in, not tested for after the fact. In support of that statement, researchers at the University of Illinois at Urbana-Champaign demonstrated how they altered a computer chip to grant attackers backdoor access to a computer. This is not the casual attacker! The level of effort would make this a tool for intelligence services of nation states.

If we are to ensure the integrity of our critical systems and information infrastructure, status quo is not good enough. Many organizations do not have the technical capabilities to evaluate the threat of cyber espionage or the budget to implement the advanced defensive measures needed to protect their information assets. You would think that the fact that IP and data theft cost businesses an estimated $1 trillion in 2008 would be a call to action. However, at this point the call to action has been unanswered. Based on the sum of my experience, research and our analysis I would offer the following three suggestions to help mitigate the risks associated with acts of cyber aggression and espionage. Given this is a public hearing, I will leave my recommendations vague as not to risk any compromise to the security these measures could provide.

1. We need to examine in detail and further quantify the risk that the global supply of components, sub-assemblies, assemblies, sub-systems and systems pose to the integrity of our critical information infrastructure and our highly computerized military. It would be extremely difficult for the United States to create the computer and related equipment necessary to build and support our critical information infrastructure and our technologically advanced military. If we are not going to build everything we need here at home, then we need to advance the current testing and validation tools and techniques as well as our system covert compromise monitoring and detection capabilities. Refer to our report - Cyber Threat Analysis Report on the Global Supply Chain National Security Issues.

2. We need to take any and all actions necessary to ensure our military has access to a continuing supply of new offensive and defensive cyber capabilities that are required and will continue to be required to defend our nation. This is not a one-time investment. Continuous investment will be necessary to respond to the ever changing global supply of computer technology. Chinese authors believe the United States already is carrying out offensive cyber espionage and exploitation against China. China therefore must protect its own assets first in order to preserve the capability to go on the offensive. While this is a highly unpopular statement, WE ARE IN THE EARLY STAGES OF A CYBER ARMS RACE AND NEED TO RESPOND ACCORDINGLY!

This race was intensified when China created Kylin, their own hardened server operating system and began to convert their systems back in 2007. This action also made our offensive cyber capabilities ineffective against them given the cyber weapons were designed to be used against Linux, UNIX and Windows. Refer to our report - RED SOS.

3. Cloaking capabilities, pass-through servers, compromise web sites and remotely controlled zombie computers make tracking and identifying the source of attacks and those behind them an extremely difficult task. We need to develop and advance the concept of Digital DNA. This concept catalogs the characteristic signatures associated with the cyber attack artifacts (code). In addition to these technical capabilities, we need to establish a framework for international cooperation for the investigation of cyber attack.

In Conclusion

We top the global chart of military spending, with China and Russia ranking second and third. China's strategists believe the United States is dependent on information technology and that this dependency constitutes an exploitable weakness. There are reasons to believe that China and Russia's militaries are collaborating and cyber warfare is one area that not only lends itself to remote collaboration, but there is soft and medium intelligence that this has and is occurring. Last year Col. Gary McAlum, chief of staff of the command's Joint Task Force for Global Network Operations at U.S, Strategic Command, quoted approvingly from a new report Technolytics had produced saying, "China aims to achieve global electronic dominance by 2050." This conclusion was drawn prior to the massive decline in the U.S. economy. As the U.S. funding for research and development has slowed substantially, China's has increased. We are in the process of updating the report referenced by Col. McAlum and at this time it appears the new projected date for China's goal of electronic dominance is in the late 2020s or early 2030s. They will simply be able to outspend the United States and the rest of the world much as we outspent the Soviet Union in the cold war.

At this time, the United States is the most technologically sophisticated country in the world. It is that distinction that makes acts of cyber aggression so dangerous. It is critical to our nation's future to take any and all actions necessary to ensure the integrity of our critical information infrastructure and our sensitive systems. I struggled with the best way to summarize over a decade of learning and the best way to communicate how real the threat of cyber aggression is, as well as the severity of these types of threats without sounding like an alarmist. The nature of this threat is such that this is not a one-time fix. The continued advancements of cyber attack techniques coupled with the rapid evolution of cyber weaponry requires continuous vigilance and the real-time creation of innovative defensive mechanisms. China is laser-focused on dual-use technology that caters to military and public use at the same time. President Hu Jintao has promised to "blaze a path of development with Chinese characteristics featuring military and civilian integration." The USCC 2008 report stated that "The U.S. government has not established any effective policies or mechanisms at the federal level to retain research and development facilities within its borders." I believe what I have presented here is the result of that shortcoming. The issue that China is behind

acts of cyber aggression against the United States is not the most concerning. It is the fact that we currently do not know how extensive the problem of cyber espionage is today and where this will lead to tomorrow!

Thank you for the opportunity to provide my perspective on the many challenges facing our nation from acts of cyber aggression. In doing so, I tried to be mindful that this administration has only been in place for a few months and new or changing policies surrounding cyber security will likely arise in coming months. I look forward to answering your questions and working with you in the future.

Appendix A Question from USCC

Q. As best as can be determined from unclassified sources, what is the extent of computer hacking and computer network exploitation (CNE) that originates in China and is directed against the systems of the U.S. government and/or U.S. firms? Do you have personal experience of cyber espionage activity that you could discuss?

The accurate response to this question is WE DON'T REALLY KNOW! While there have been reports, some highly publicized, a vast quantity of these are not officially reported. A former US special agent with over 20 years of service stated he saw over 100,000 systems completely compromised and hundreds of thousands of files infiltrated." One study suggests that open acknowledgement of a breach results in between 1% and 5% decline in stock price for a corporation. That in and of itself is one reason why many of these events are not reported. One troubling attack was when hackers were able to glean the sensitive information of up to 12,000 visitors to the Oak Ridge National Laboratory. In a recent conversation about this and other cyber attacks with Gary Clayton, CEO of Privacy Compliance Group, he stated "Recent reports from Australia, Canada and the United States regarding the coordinated efforts of the Chinese to target key infrastructure, throw into sharp focus the necessity for better coordination among the government, industry and individuals to protect our infrastructure and our personally identifiable information. Today, the Chinese are targeting the Pentagon and the Dalai Lama. Tomorrow, the targets will be ordinary citizens, their personal data and the businesses upon which we rely. Unfortunately, most Americans are simply unprepared for the chaos and financial disaster that such attacks will cause." We need to address security awareness!

Q. Who/what are the entities in China involved in cyber espionage? What evidence, if any, exists to link such activity to Chinese state and/or state-sponsored entities? What are the major Chinese institutions involved in the development of Chinese cyber espionage capabilities?

The PLA has cyber warfare capabilities that in my opinion equal that of the United States and Russia. This is a three horse race (U.S. plus China plus Russia) and it is a dead heat. While at Netscape I became aware that China had a group that reviewed, monitored and filtered content based on guidelines set by the Chinese government. I have posted on my cyber warfare blog that this group has possibly been redeployed as a cyber militia. I also worked with U.S. Strategic Command's working group on cyber militias. In addition, the National University of China has Defense Technology advanced programs in place and is the strategic advisor to the PLA on Cyber Warfare. The Ministry of Science and Technology (MOST) is the lead organization in

defining science and technology plans and policies, drafting related laws, regulations and department rules, and guaranteeing the implementation for China. Part of their initiatives deal directly with cyber capabilities.

Q. What are the primary targets of such hacking and CNE activities? What government, infrastructure, economic, and scientific institutions and/or interests are being targeted by such activity? What are the implications for U.S. national security and economic competitiveness resulting from the loss of data and intellectual property in these areas?

I struggle to identify any computer that is not a target or potential target for cyber attack. Individuals are attacked for personal information and their computers become an unwilling participant in a botnet. A bot is a type of malicious software which allows an attacker to gain control over the affected computer. The affected computer is then referred to as a zombie because it is not under the complete control of the owner/user. A botnet is a collection of zombie computers under the control of the attacker. Corporate computers are attacked for Intellectual Property and customer lists. One study I saw suggests that around 80 percent of an organization's value now rests in its information. The Director of National Intelligence reported before Congress that Intellectual Property and data theft in 2008 totaled $1 Trillion Dollars. It is all tied together.

The ability for foreign companies to advantageously compete against U.S. companies through cyber espionage impact our economy and our ability to support research and development and investment in defending our nation. Critical infrastructure control computers are compromised and mapped for possible attacks by terrorist groups or rogue nation states. A computer is a cyber weapon waiting to be loaded and used. Based on over a decade of work in their area without legislative standards for computer and systems security, our national security is at great risk and will remain so!

Q. Can you identify and explicate past case studies of PRC cyber espionage that would serve to illuminate Chinese intelligence operations within the United States?

Just look in the recent press and you will find plenty of examples. I was contacted by a security consulting company for advice when they uncovered a bot attached to an Oracle data base of a U.S. Company. Based on the information I was provided, the bot was said to have collected what I would categorize as competitive information and send it to an IP address in China. I ask Solutionary, a top ranked managed security services provider (MSSP) to pull some data about acts of cyber aggression against their clients that were tied to China. Their security operations center (SOC) on average, identified 128 acts of cyber aggression per minute that were traced back to IP addresses in China.

Q. Are you able to identify particular U.S. vulnerabilities (networks, infrastructure, etc.) that you believe need to be addressed? Are there any practices or policies that you could recommend to the U.S. Government to improve cyber security?

With the continuous discovery of vulnerabilities, the opportunity to compromise systems is always present. April 14, 2009 (Computerworld) Microsoft today released eight security updates that patch 23 vulnerabilities in Windows, Internet Explorer, Excel and other software in the company's portfolio -- a collection of fixes one researcher called "insane." You can prove a computer has been hacked and compromised. It is nearly impossible to prove a computer has not been compromised. We do not know how bad the problem is because many organizations do not disclose these security events. Mandatory reporting along with a classification of event type is required to properly track these malicious attacks and see if our preventative measures are working.

About Technolytics

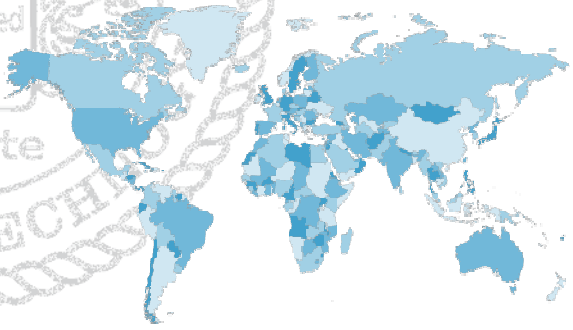
The Technolytics Institute (TTI) was established in 2000 as an independent executive think tank. Our primary purpose is to undertake original research and develop substantive points of view on strategic issues facing executives in businesses and industries around the world. Our strategic goals focus on improving business performance, creating sustainable competitive advantage, delivering innovation and technology, and managing security and risk.

Technolytics helps guide business executives, industry leaders and government policy makers in shaping the economic, regulatory and risk environment of tomorrow. One of the hallmarks of our service offering is our security and risk scenario planning. Our approach is called Trans-disciplinary Intelligence Engineering (TIE). This approach has been used to develop scenarios for Homeland Security, Corporate Event Planning, Corporate Espionage and Security and for other entities. This technique has been applied to strategic planning, product strategy, competitive strategy and marketing strategy as well as security and risk management.

Our technology framework methodology is based upon 1997 Malcolm Baldrige strategic planning and reporting guidelines. We believe these guidelines (as implemented in the Technolytics models and tools) represent some of the best strategy and management models available anywhere in the world. The knowledge repository, benchmark data, and best practices used to create these Technolytics models have evolved from detailed research and analysis and are updated regularly to reflect changes in the global market.

CONTACT INFORMATION

The Technolytics Institute
4017 Washington Road
Mail Stop #348
McMurray, PA 15317
P 888-650-0800
F 412-291-1193
I www.technolytics.com
E info@technolytics.com



The following is a list of research that will be published in the near future.

1. *International Policy on Cyber Aggression*
2. *Advanced Cyber Counter Intelligence*
3. *Advanced Cyber Counter Measures*
4. *Cyber Intelligence Acquisition Infrastructure*
5. *Cyber Threat Assessment 2009*