Testimony of Greg Autry
Senior Economist, Coalition for a Prosperous America, American Jobs Alliance

On

Cyber Attacks: An Unprecedented Threat to U.S. National Security

Before the

Subcommittee on Europe, Eurasia, and Emerging Threats

Committee on Foreign Affairs

U.S. House of Representatives

March 21, 2013

Good afternoon Mr. Chairman and members of the Subcommittee. My name is Greg Autry. I am the co-author, with Peter Navarro, of the book *Death by China*. I also serve as Senior Economist for the Coalition for a Prosperous America and the American Jobs Alliance. I teach macroeconomics at Argyros School of Business at Chapman University in Orange, California. I have previously worked as a software and network engineer and have earned certifications from Novell (CNE), Cisco (CCNA) and Microsoft (MCSE).

I am testifying on my own behalf and the views expressed here are not necessarily the views of any organization.

My testimony will focus on the economic consequences of China's persistent cyber assault against America's citizens, firms, government and critical infrastructure.

The recent report from Mandiant Corporation has made perfectly clear what everyone in the cyber security community already knows – there is a giant sucking sound in the world economy and it is coming from China. The government of that nation has long been engaged in a massive hacking campaign aimed at Western firms, governments and infrastructure. The military origin of these attacks, the obvious economic cost, and the threat implied by intrusions into our critical infrastructure, mark this as a 21st century act of war.

These attacks are not an isolated case of industrial espionage but rather part of an integrated military-economic-cultural assault on America, a nation that China views not as a benefactor and valued trading partner, but rather as an ideological adversary who must be subdued by any means necessary. Chinese senior military strategists have discussed such multidimensional warfare for years[1]. While the Chinese economic assault on the U.S. manufacturing base is painfully visible to our unemployed, the Mandiant report shows that China views this as a military operation. In the process China has debased the Internet, a gift to the world developed at U.S. taxpayer expense.

As a former software and network engineer, I am undeniably impressed by the skill, thoroughness and audacity of several private sector organizations whose counterintelligence work has brought the Chinese hacking threat into the light. Canada's Information Warfare Monitor report on the Gh0st RAT threat, McAfee's work on Aurora, Dell Secure works investigations into Chinese military connections and now Mandiant's brilliant demonstration that Unit 61398 of the People's Liberation Army is APT1 have done our nation and the world a great service.

However, it is reasonable to assume that our national security, military, and government officials have aware of this for sometime. Why is the Chinese regime never held accountable for of any manner of bad behavior? If 61398 were an Iranian Republican Guard unit located in Tehran the U.S. military would have reduced their HQ to a smoldering pile of rubble long before I presented this testimony.

[1] i.g. Liang and Xiangsui, *Unrestricted Warfare*, 1999.

How does an economist estimate the cost of Chinese cyber warfare? The evidence suggests these revelations are merely the tip of the iceberg. The FBI admits, "As a result of the inability to define and calculate losses, the best that the government and private sector can offer are estimates."[2] A full accounting of the damage done to the U.S. is impossible to compile, because most of the victims will never detect the Chinese intrusions or will decline to admit to their losses.

The discrepancy between expert estimates and the value of crimes actually reported makes this under reporting obvious. For instance, Symantec estimated 2011 individual and small business cybercrime losses at $388Billion[3], while the FBI's IC3 summary of actual reports that totaled a mere $485million[4]. McAfee even tossed out a $1Trillion estimate a few years ago. Using the more conservative number only a little more than a tenth of one percent (0.0125%) of these crimes by cost were reported. Even if Symantec overstated the problem by an order of magnitude we still have more than 98% of cybercrimes going unreported.

In any case, how do we place a value on something like Google's source code? The firm trades at 25 times its annual earnings, suggesting most of its value is in future revenues. Conservatively assuming that half of Google's market capitalization of $248 billion reflects the value of its technology (other factors might be labor force, brand equity and assets) this implies a property worth $124 billion has been compromised. While assessing the total cost over time has too many unknowns to model, Google has clearly suffered at the hands of its Chinese competitor Baidu. Google has lost $ billions in the Chinese market alone prompting Google's co-founder Eric Schmidt to brand the Chinese government a "menace." He has wisely noted that "The disparity between American and Chinese firms and their tactics will put both the government and the companies of the United States at a distinct disadvantage." In other words we don't cheat and steal well.

Assuming that most American firms are less savvy than Google when it comes to cyber security, it is easy to justify some very large losses. If Mandiant was able to identify 141

[2] http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism
[3] http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/
[4] http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf

victims, there are thousands of compromised firms. If we set Google's losses at just $10 billion and assume that to be fifty times larger than the average of two thousand major victims we end up with a $400 billion figure. In any case, the losses are clearly in the hundreds of billions of dollars. Putting an exact number on the damages should be no more important to our reaction than calculating the precise losses from Al Qaeda attacks. The point is that *the Chinese government is currently using its military to intentionally inflict enormous damage on the American economy.*

Consider that the economic costs of the September 11 attacks (excluding the military reaction) have been estimated at around $175Billion[5]. The *annual* cost of Chinese military hacking to the US economy is therefore in the same range as 9/11. Every $100 billion implies a loss of about one million American jobs[6]. *Chinese military hacking has left millions of American workers unemployed.* And although we've been spared the specter of horrible televised deaths, the suicide and death rates for the unemployed are substantially higher than the national average[7]. The statistics would suggest that over the years, *Chinese military hacking has killed thousands of Americans.*

The membrane between the black-hat hacker community and the professional security services of China is very permeable. Internet trolls with handles like "UglyGorilla" have access to millions of American emails and passwords via their PLA connection. American workers often use their business computers and email for personal financial transactions. Many of them use the same password at work as they do on their bank. The American public should be in an uproar.

Technical protections against cyber intrusion have consistently proven to be insufficient because most initial system compromises are achieved via exploitation of human beings with "social engineering" tricks like spear phishing. The criminal

---

[5] The New York times suggest $55billion in physical damage and $123billion in attenuated economic impact. The cost of invading Afgahnistan and Iraq in reaction are separate and larger; though they are surely much less than the cost of using a traditional military response to China – something that is probably not a wise option. http://www.nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html?_r=0

[6] Estimating revenue of $100,000 per job

[7] http://www.nytimes.com/2012/11/05/health/us-suicide-rate-rose-during-recession-study-finds.html, http://news.yale.edu/2002/05/23/rising-unemployment-causes-higher-death-rates-new-study-yale-researcher-shows

consequences of getting caught are minimal. A report from Cambridge recently suggested, "we should spend less on anticipation of cybercrime (antivirus, firewall, etc.) and more in response . . . hunting down cyber-criminals and throwing them in jail."[8] Internet crimes must have punishments, even when the criminal is the Chinese government, or there is no rule of law online. As an analogy consider that if the police don't respond and the courts don't enforce the law, all the alarm systems and locks on Earth could not keep your home safe.

When businesses in lawless regions are left at the mercy of criminal elements they must: fail, relocate or reach an accommodation with the criminals. Consequently, victims of Chinese cyber attacks are actually helping to conceal the extent of this problem. They wish to avoid public humiliation, negative stock market reaction and the liability associated with the loss of customer data. What makes the silence more worrisome is that most large American corporations have been, for all practical purposes, coopted by the Chinese government. They are so dependent on low-cost production in China and strategically committed to the promise of the "world's largest market" that exposing the criminal behavior of their notoriously vindictive host is unthinkable. With the noble exceptions of Google and the New York Times, an American Corporation is no more likely to "call the cops" on China than are the victims of abusive relationships likely to testify against their spouses.

Remedies proposed by the administration suggest that nothing will happen until a victim proves exactly what China took it and how they used it. What CEO wants to take another beating from China's state manipulated economy and the stock market while trying to convince the U.S. government and the WTO of their victimhood?

Worse, many officials in the departments of State, Treasury and Commerce upon whom we depend to make China play fair come straight from doing business with China or proceed to do so as soon as they leave government.

---

[8] Measuring the Cost of Cybercrime:
http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

What is most important is recognizing the systemic nature of the China problem. None of China's offenses, including cyber attacks, occur in isolation. They are part of an integrated, asymmetric *war by other means* policy. Yet, America deals with trade cheating, space debris, and espionage as though each were a completely disconnected phenomena.

We are executing an "Asian Pivot" strategy to confront China's increasingly belligerent military posture in the Western Pacific, while our consumption of Chinese goods finances a massive PLA arms build up. The administration promises to tackle PLA cyber assaults in a similarly schizophrenic manner. Nothing could possibly make China's master strategists happier.

The fundamental problem is that the Chinese government is not a normal government but an immoral regime conducting an *active and planned assault* against our political and economic institutions. These cyber attack revelations are simply the latest manifestation of that war in progress.

Do we believe that China's corrupt, state dominated economy is actually beating American private enterprise in a fair contest? While Shanghai booms and Chinese billionaires sprout up like rice in the spring, 25% of Americans are unemployed or underemployed. This is the root of our intractable fiscal dilemma. While we cut and tax, the Chinese government can hardly think of enough new things to do with the vast wealth our consumers and corporations transfer to them – from maglev trains and moon missions to a frightening military buildup. This is what losing a 21st century war looks like.

I propose the following remedies.

Get Real about China: It is time to publicly admit that our engagement policy has completely failed to produce a democratic, peaceful China and is empowering an aggressive dictatorship. We must engage our allies in this new approach.

Systemic Penalties for a Systemic Problem: Take the burden off demonstrating damages off the victims and put the pressure on the perpetrator to stop. The PLA has been proven guilty of intending to undermine American firms and it does not enjoy constitutional rights in the US. A significant tariff should be placed on Chinese manufactured technological goods until there is no further evidence of these activities.

Technology Sanctions: The import of any Chinese computer and telecom networking hardware or software into the U.S. should be restricted. Specifically: Huawei, a technology firm founded by a Chinese military officer and routinely implicated in intelligence work.

Recover Costs of Defense from China: An import tariff equal to America's cyber defense costs should be attached to Chinese imports. (A similar tariff should be assessed for our expense of missile defense and the "Asian Pivot" costs.)

Return Costs to Multinational Corps: It is time to stop rewarding American corporations for transferring capital, technology and jobs to an enemy state by modifying our corporate tax system to favor American based manufacturing.

Stop Conflicts of Interest: Halt the flow of US officials to and from engagement in business with China. Encourage the Senate to make the investigation of Chinese business dealings a priority in confirmation hearings for officials at State, Treasury, and Commerce.

Stop Educating Our Adversaries in Military Technology: Ban the admission of computer science student to the U.S. from nations whose militaries engage in cyber attacks against America and her allies. We are educating a massive pool of Chinese talent in our computer science and engineering schools, where they displace tens of thousand of American citizens and allies.

Encourage U.S. Education in Computer Science: Direct the majority of student aid to STEM majors and specifically graduate degrees in computer science and engineering.

Protect and Reclaim The Internet: The Internet is an invention of the American government funded by U.S. taxpayers. The U.S. government and the U.S. armed forces are reasonably entitled to demand special privileges in its use. Any attempt to transfer further administrative oversight of the Internet to international regulatory bodies must be most strongly opposed. Any opportunity to *regain* U.S. control of the Internet would be in the interest of all people, most notably the citizens of China. Specifically ICANN and control of the DNS root must remain in the U.S. Root servers currently in the U.S. must remain there. The location of anycast servers should be restricted to friendly nations.

Closing Note: I want to be clear that my remarks are in no way meant to disparage the admirable nation of China nor its hardworking people. My criticisms are aimed entirely at the corrupt, nominally communist plutocracy that is repressing them and at the failed American policy of engagement, which has enriched and empowered that loathsome regime a thousand fold.