Chinese Cyber Espionage: The #1 Threat to Economic Security? (And other tall tales)

PART-1 Introduction

SLIDE-01: Hello, my name is Bill and I'm from Below Gotham.

SLIDE-02: Let's talk about the nature of the threat posed to the United States by Chinese cyber espionage.

SLIDE-03: In 2013 the Department of Defense noted that China has been actively engaged in economic espionage (quelle surprise!).

SLIDE-04: Former National Security advisor Richard Clark warned that this espionage is costing American jobs. Note there are those who would view this as a clever ploy to align the interests of the average person with those of elite policy planners.

SLIDE-05: Mike Rogers, chair of the House Intelligence Committee, claims that Chinese cyber espionage is the number one threat to U.S. economic security.

SLIDE-06: General Keith Alexander went for full-throttle, claiming that Chinese cyber espionage is the greatest wealth transfer in history!

SLIDE-07: Let's break down Mike Roger's observation into two general impressions.

PART-2 Is the Chinese Government Responsible For All Attacks Emanating from China?

SLIDE-08: We'll start by tackling the impression that the Chinese government is behind all of the attacks emanating from China.

SLIDE-09: During the era of Mao Zedong, China leveraged strong central control in conjunction with a household registration system known as Hukou.

SLIDE-10: Hukou tied people down geographically. It was required to receive services (e.g. education, medical, employment) and was not recognized in other cities. Everything that you needed (e.g. cloth, rice, meat) you had to purchase with Liangpiao rationing stamps which were issued in the city where your Hukou was registered.

SLIDE-11: Combines these means of control with pervasive neighborhood monitoring and there was very little room to break the law. If these systems were still in place, then only the Chinese government would have the ability to launch large-scale cyber campaigns.

SLIDE-12: But the reforms launched by Deng Xiaoping weakened Mao's tools. He let people move around, enabled the emergence of economic inequality, and delegated a substantial amount of authority to local officials.

SLIDE-13: Travel restrictions have gradually loosened over the years. Oversight of foreign visitors is so lax that there's ample opportunity for foreign spies.

SLIDE-14: Another result of Deng Xiaoping's reforms is growing inequality and intense economic pressure. Other than the United States, China has the most billionaires in the world. But someone trying to buy a house struggles like a part-time waiter in Denver.

SLIDE-15: This kind of economic pressure incites crime, people are desperate to find ways to make money. Hence the resurgence of organized crime.

SLIDE-16: There are strong incentives for finding outside work. Government hackers are so poorly paid that many of them moonlight, hiring themselves out to whomever can pay.

SLIDE-17: The transfer of power to local officials resulted in extensive abuse. In fact, people even question the extent to which the central leadership can exercise their authority to reform their system and impose rule of law.

SLIDE-18: To give you an idea of the scope of the corruption, the Chinese government seized assets from relatives and associates of the former security chief Zhou Yongkang which amounted to over $14 billion.

SLIDE-19: Party officials have become a law unto themselves. Bo Xilai monitored his political opponents.

SLIDE-20: The government is riddled with crooks involved in their own illegal schemes.

SLIDE-21: In light of this kind of systemic corruption, China struggles just to provide basic services to its population and this failing is reflected by reflected by a flood of dissent (what the government refers to as “mass incidents”). The pollution in cities like Beijing is one driving factor.

SLIDE-22: The ability of the Chinese government to regulate food quality is so poor that in terms of sheer volume the black market for baby milk powder in Hong Kong is bigger than the market for heroine.

SLIDE-23: Though China has established an extensive censorship and monitoring system called Golden Shield (which relies on IP blocking, DNS filtering, URL filtering, packet filtering, etc.) it’s not that hard for a technically knowledgeable user to sidestep it.

SLIDE-24: Piracy is another problem, one which makes Chinese networks vulnerable because it means there’s a veritable sea of unpatched systems sitting out there on the internet waiting to be hacked.

SLIDE-25: Rule of law is so dodgy in China’s networks that Russian cyber criminals have shown a proclivity for using Chinese bullet-proof hosting services.

SLIDE-26: The idea that all of the cyber-attacks coming out of China are the sole work of the Chinese government is the result of what’s known as out-group homogeneity bias. The common tendency to see other groups as more homogeneous than they really are.

SLIDE-27: The attacks coming out of China aren’t the result of some 1000-year plan, but rather are a function of the government’s waning control over its networks.

SLIDE-28: There are a broad spectrum of actors operating out of China’s relatively lawless networks: organized crime, foreign spies, moonlighting agents, rogue officials, and corporate spies.

ASIDE: Foreigners in China’s Networks

SLIDE-29: But not all of the attackers are Chinese. There are also attackers outside of China using Chinese networks as a staging area.

SLIDE-30: I can attest that anti-forensics is a thriving field. Bytes are bytes and they can be manipulated, along with operational signatures, to tell any story you want.

SLIDE-31: Technologies like onion routing were created so that U.S. intelligence services could spy on people anonymously. The TOR project was originally funded by the military.

SLIDE-32: And, guess what? The TOR project still receives money from the Pentagon. Almost half of its funding.

SLIDE-33: The private sector has also created solutions that allow users to spy anonymously. Ntrepid has a service known as the Internet Operations Network that enables "operational" non-attribution.

SLIDE-34: Thanks to Ed Snowden: it is part of the public record that the NSA uses fronts in other countries to launch attacks.

SLIDE-35: Intelligence agencies like GCHQ have also admitted to conducting false flag operations. These are standard techniques, so you can be certain that the NSA is involved in false flag operations.

SLIDE-36: But deception isn't just limited to covert operations. The very same security professionals who investigate incidents are in a unique position to fabricate evidence to manipulate public perception.

PART-3 Are Losses Dues to Cyber Espionage the #1 Threat to U.S. Economic Security

SLIDE-37: Now let's tackle the 2nd impression, that Chinese cyber-espionage is the number one threat to our economic security.

SLIDE-38: The problem with answering this question is that there aren't a lot of statistics available.

SLIDE-39: Mainly due to the fact that investigators often don't know what was taken. This is true even in high-security environments.

SLIDE-40: For example, when computers storing documents on Lockheed's F-35 Joint Strike Fighter were compromised the Dept. of Defense had no idea what they made off with.

SLIDE-41: And the NSA has no idea which documents Ed Snowden took with him…

SLIDE-42: For all the resources that get poured into the NSA's budget, they're completely clueless.

ASIDE: Government Secrecy and So-Called Credible Officials

SLIDE-43: Officials usually respond to the scarcity of data by claiming that they do indeed have the facts, but they just can't share them with us. Because it's all classified.

SLIDE-44: This creates a convenient pretext to exclude normal people from engaging in policy discussions. You don' have access to secrets like we do so you can't help shape policy. This was a stated reason why the review board at DEFCON rejected this presentation.

SLIDE-45: This is also how CIA Station Chief Larry Devlin convinced a fellow spy named John Stockwell not to ask questions. "There are people who have all the information, making tough decisions. Leave the decision making to them…"

SLIDE-46: When John Stockwell rose through the ranks and garnered enough clout to actually sit on NSC sub-committee meetings, he found fat old men who slept through meetings, and high-level officials (i.e. Henry Kissinger) arguing over who sat in what seat…

SLIDE-47: The universal apologia that we're given is that secrecy is needed to protect national security. On the other hand, if you know where to look, there's an overwhelming amount of evidence that suggests that secrecy is a common mechanism to conceal illegal behavior (the CIA's operation Mockingbird, the Watergate scandal, operation CHAOS, MKULTRA, the FBIs' COINTELPRO program, the Iran-Contra scandal, etc.).

SLIDE-48: A functioning democracy requires that people have access to accurate information and exercise sound judgment.

SLIDE-49: Propaganda undermines this by obscuring facts and encouraging people to respond emotionally.

SLIDE-50: Secrecy also undermines democracy because people can't debate policies that they aren't aware of. Note Obama's penchant for secrecy and his hostile stance towards anyone who violates it.

SLIDE-51: This raises a question. If someone is a current, or former, government official, does this ensure that their information is reliable?

SLIDE-52: For example, an NSA spokesman stridently told the Washington Post that the NSA isn't engaged in economic espionage.

SLIDE-53: Thanks to Ed Snowden, we know that this is not true.

SLIDE-54: The United States has a long and storied history of being heavily involved economic espionage.

SLIDE-55: According to Beatrice Edwards, these economic espionage operations benefit narrow private sector interests, not the general public.

SLIDE-56: Let's look at another example: Director of National Intelligence James Clapper claimed on camera (under oath, no less) that the NSA doesn't collect any data on millions of Americans.

SLIDE-57: It turns out that this was not true, per the telecom industry's release of telephone metadata.

SLIDE-58: Likewise Keith Alexander stated that the NSA doesn't intercept American e-mails or cellphone conversations.

SLIDE-59: Obama claimed on Charlie Rose that any monitoring of American emails or telephone calls would require a warrant.

SLIDE-60: Of course, anyone who's familiar with Section 702 of the Foreign Intelligence surveillance act knows that this isn't true.

SLIDE-61: As Daniel Ellsberg can tell you, Presidents lie all the time. This definitely undermines any guarantee of executive credibility…

ASIDE: Losses Due to Cyber Crime

SLIDE-62: Given that we have very little useful data on cyber espionage losses, let's look at a related category to provide us with a frame of reference: cybercrime.

SLIDE-63: According to the Internet Crime Complaint Center, which is a partnership between the FBI and the National White Collar Crime Center, their recorded losses are close to $800 million.

SLIDE-64: This figure is in the same basic ballpark of findings published by Cambridge where researchers stated that England spent approximately a billion dollars trying to protect against cybercrime and clean up after incidents.

SLIDE-65: Is there an upper bound for losses due to cybercrime?

SLIDE-66: In 2009 McAfee claimed that worldwide losses were on the order of a trillion dollars.

SLIDE-67: Does this seem a little bit much?

SLIDE-68: A year or two later, McAfee admitted that this was a flawed unscientific extrapolation that had very little basis in reality.

SLIDE-69: McAfee then hired another think tank, which scaled back the statistic to $100 billion.

SLIDE-70: Assuming this is correct, it's clear that cybercrime is not an existential threat as far as the United States economy is concerned. This lends weight to the conclusion that economic espionage is also not the gravest threat to U.S. economic security.

PART-4 There Is an Existential Threat to U.S. Economic Security

SLIDE-71: But… This doesn't mean that there aren't existential threats to U.S. economic security.

SLIDE-72: History shows that society faces a threat from banks that have gotten too big to fail. (I'm talking about financial institutions like Goldman Sachs, Morgan Stanley, JP Morgan Chase, Citigroup, Bank of America and Wells Fargo)

SLIDE-73: According to former Treasury Secretary Hank Paulson the 2008 financial collapse threatened to melt down the entire global economy.

SLIDE-74: This slide offers a fairly terse synopsis of what happened in 2008. I don't have time to go through the specifics but you can go back when you have time and parse through this. For a more detailed rundown, see *Griftopia* by Matt Taibbi or Robert Scheer's *The Great American Stickup*.

SLIDE-75: Researchers at the Dallas Federal Reserve Bank calculated that the recession resulting from the financial meltdown in 2008 cost the American economy between $6 and $14 trillion.

SLIDE-76: The Financial Crisis Inquiry Commission (FCIC), a group of ten people selected by congress to investigate the 2008 collapse, placed particular responsibility on the shoulders of politicians, regulators, and banking executives.

SLIDE-77: In many instances banks cared very little about the actual quality of the loans they used to create their mortgage securities because once they sold them (the Collateralized Debt Obligations) they had no interest in whether the underlying loans defaulted. See Frontline's *The Untouchables* for more on this.

SLIDE-78: The Rating Agencies (Moody's, Standard & Poor's, and Fitch Ratings) failed because the companies they regulated were also their customers. Tell me there isn't a little room for conflict of interest in this scenario.

SLIDE-79: According to former SEC attorney James Kidney, regulators (like the SEC) failed because high-ranking officials were hoping to work in private sector once they retired from government. Regulators have been anything by aggressive, as a report by the OIG of the DoJ detailed in March of 2014.

SLIDE-80: Politicians failed us because, well, because the banks are in a position to reward them once they leave office.

SLIDE-81: With the bankers gaining widespread influence (rating agencies, regulators, and politicians) it's not surprising that the banks which were too big to fail are even bigger, and that society has been set up for another catastrophe. This, my friends, is an existential threat to U.S. economic security: **a small group of powerful rent-seeking plutocrats in the banking sector**.

PART-5 Other Tall Tales

SLIDE-82: Mike Rogers has also claimed that Ed Snowden is a Russian spy.

SLIDE-83: Of course, the only reason Ed Snowden is in Russia is because the State Department revoked his visa. He was originally aiming for Latin America.

SLIDE-84: Mike also called Glenn Greenwald a thief.

SLIDE-85: Glenn Greenwald is a journalist. Just like other journalists (e.g. Bob Woodward) he makes a living writing stories based on disclosed government secrets.

SLIDE-86: And now, for the final tall tale. Mike Rogers claims that the United States is involved in a (gasp!) cyber war.

SLIDE-87: I don't have the bandwidth to address this sort of idiocy herein. But my coauthor and I wrote a book to refute pundits like Rogers.

PART-6 Epilogue

SLIDE-88: And now: a bonus track.

SLIDE-89: Did I mention that Mike Rogers was a former FBI agent whose campaign was funded heavily by the defense industry?

SLIDE-90: After all these tall tales it might not surprise you that Mike has taken up in the AM band as radio show host.

SLIDE-91: As for General Alexander, he moved on to greener pastures and started a consulting firm that targets the financial sector.

SLIDE-92: As you can see, he's probably made lots of new friends at the 2014 Bilderberg conference.

SLIDE-93: Thank you.