China's Cyberespionage: The National Security Distinction and U.S. Diplomacy

Greg Austin[1]

In January 2011, the United States and China agreed for the first time at head of state level to include cybersecurity as an important bilateral agenda item, albeit one of around two dozen identified in a "laundry list" well into the body of a joint communiqué. It was also that year when the United States issued its *International Strategy for Cyberspace*. These two events held out the promise that U.S. diplomacy towards China on cyberspace issues would begin to benefit from a clear focus and an articulated strategy. There have been other glimmers of hope, especially the bilateral agreement in June 2013 to open an official working group on the subject of cybersecurity.

This new working group was not however in all respects a sign of positive improvement. It resulted in part from the issuing in March 2013 of unprecedented public demands on China by U.S. National Security Adviser, Thomas Donilon, that it "should take serious steps to investigate and put a stop to" "sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale".[2] The demands capped an escalating rhetorical campaign from senior Administration figures that this cyber espionage by China represented "the greatest transfer of wealth in human history".[3] China responded to this pressure by agreeing in June 2013 to set up the bilateral working group.

Any hope springing from the creation of this group was dashed on 19 May 2014 when the Justice Department, not normally a significant player in U.S. diplomacy, announced grand jury

indictments in a U.S. District Court of five Chinese military personnel for cyber-enabled industrial espionage undertaken from their home base in China.

China reacted angrily to the indictments, which were unprecedented in international diplomatic practice, by suspending the bilateral cyber dialogue. However, the sense of outrage in China was deeper than that one symbolic and limited act. After all, the United States itself had long practiced remote surveillance of China by myriad electronic means. Chinese officials noted that since June 2013 world newspapers had been full of reports of large scale cyber espionage by the United States and its closest allies against China and many other countries.

This article concentrates on the distinction being made by the U.S. Administration between China's national security espionage (which the United States does not challenge in principle, even as it tries to stop it) and China's industrial espionage (that benefits the non-military or civil sector enterprises in China). This is the main claim used at the diplomatic level by the U.S. Administration to justify the damage to U.S. diplomacy arising from the indictments: that China's government condones the practice of cyber espionage by its armed forces, the People's Liberation Army (PLA), to the benefit of China's civil sector businesses. U.S. officials have made clear that any economic information it collects is for national security purposes only and that such activity is a legitimate or normal activity for any state. The distinction the United States is making is between the end–use of the intelligence collected: that they are being applied in civil sector commerce (as opposed to the national security sector which includes defense industry). The article concludes that the U.S. Administration has failed to make a convincing case in the public domain but has incurred a considerable diplomatic cost.

This article was completed prior to the unsealing of indictments on 18 May 2015 against six Chinese defendants for commercial espionage undertaken largely by having personal access to the trade secrets through two defendants employed at the two victim companies. In this case, the allegation appears to be that defendants copied the files to computer memory devices directly rather than remotely. This May 2015 indictment alleges that the secrets were stolen "for the benefit of the government" of China and for a Chinese civil sector company, with the Department of Justice publicly alleging that the actions were "sponsored" by the Chinese government.[4] There is a short section towards the end of this article on how this news might be read relative to the article's conclusions.

The article is published as a discussion paper in an effort to stimulate comments and to surface additional evidence in the public domain that is relevant, perhaps even contradictory, to its conclusions.

Counts of the May 2014 Indictment

The indictment alleges, inter alia, that the five officials breached Section §1832 of Title 18 of the U.S. Code (18 USC), that they took commercially sensitive information from Westinghouse without authorization "with intent to convert a trade secret" about a product "intended for use in interstate or foreign commerce, to the economic benefit" of someone other than the legal owner of the information.[5] This "trade secret theft" intended for commercial benefit and covered by §1832 is distinguished from a separate offence covered under §1831, which criminalizes acts

where the perpetrator knows they "will benefit any foreign government, foreign instrumentality, or foreign agent". The indictment brought only one count under §1831 and one count under §1832 and each was for the theft of Westinghouse information. The remaining 29 counts were for other offenses, such as identity theft, damaging a computer, and computer fraud and abuse, and involved as victims four other corporations and a labor union. The alleged offenses were said to have occurred sometime between 2006 and 2014. Of 31 counts in the indictments, only one related to the activity that the United States government had identified as a high policy priority in diplomacy with China: stopping the conversion of U.S. trade secrets to the benefit of Chinese civil sector firms. As a domestic law enforcement problem, the United States is fully committed to using its own security and law enforcement agencies to stop Chinese espionage for national security purposes but concedes that this is not something that it would normally demand through diplomatic channels that China stop.

The U.S. Standard

In a background briefing in July 2014, a State Department official repeated the well-known position of the United States government: "one of the fundamental differences is on this question of the acceptability of cyber-enabled economic espionage, which the United States Government does not conduct, and we need to come to a clear understanding with the Chinese about that norm".[6] This norm was expressed by Assistant Attorney General, John Carlin, on May 22 2014 as follows: "as a general rule, as the president has stated in his Presidential Policy Directive, we do not take information from other people's companies to provide it to our own companies."[7]

The statements made by the Department of Justice (DoJ) at the time of the indictments are silent on the fact that in the case of trade secret theft or economic espionage, 18 USC, in §1833 provides an exclusion for "any otherwise lawful activity conducted by a governmental entity of the United States". The desire to protect U.S. officials in this way is a part of long-standing U.S. policy on mutual recognition of sovereign immunity in espionage cases. This approach has been expressed on numerous occasions, of which one example is this: "refusal by US courts to grant immunity to foreign officials for their official acts could seriously harm US interests, by straining diplomatic relations and possibly leading foreign nations to refuse to recognize the same immunity for American officials".[8] Of special note, the United States has previously set a standard that what it does in its own courts in respect of non-recognition of sovereign immunity is the test for its view of whether it can claim sovereign immunity in the jurisdiction of a foreign state.[9] Yet, as noted by an authoritative legal scholar, the May 2014 indictments do not seem to allow for this consideration of sovereign immunity and they sit as part of an intensifying tendency in U.S. policy, visible also she said in targeted sanctions, "towards focusing pressure on individuals associated with undesirable state policies".[10] This commentator observed that "The full implications of this trend for international law and international relations remain to be seen".

The Indictments and the U.S. Legal Policy Framework

In announcing the indictments in May 2014, the DoJ, with the Attorney General Eric Holder in the lead, laid out at length the arguments for the action. Though well known, the statements need to be summarized here for completeness. Holder noted that the indictments were the "first ever charges against a state actor for this type of hacking".[11] He asserted that "the range of trade

secrets and other sensitive business information stolen in this case is significant and demands an aggressive response". He suggested that the espionage was having a material effect on the ability of the affected companies "to innovate and compete" because their Chinese competitors benefited from their government's ability to steal business secrets. He further suggested that the indictments were necessary to deter or punish efforts by any state (including obviously China) "to illegally sabotage American companies and undermine the integrity of fair competition in the operation of the free market."

The Attorney General was explicitly asserting that China undertakes as state policy the cyber-enabled theft of industry secrets in order to convert them to the commercial benefit of Chinese civil sector firms on a significant scale, implying there was no clear national security purpose in stealing the secrets and exploiting them.

The victim companies named in the indictment came from several industries: solar, nuclear, aluminum and steel. In respect of a US-based subsidiary of the German company, SolarWorld AV, the grand jury indictment includes the charge that one of the named defendants "stole thousands of files including information about SolarWorld's cash flow, manufacturing metrics, production line information, costs, and privileged attorney-client communications relating to ongoing trade litigation, among other things". The indictment alleges that "such information would have enabled a Chinese competitor to target SolarWorld's business operations aggressively from a variety of angles". But, for some reason, the indictment did not charge the defendants with industrial espionage against SolarWorld under §1832 (or even under §1831).

To achieve a conviction under §1832, if defendants ever came to court, it would seem sufficient for the U.S. federal prosecutor to prove that the Chinese military officers took the information with the intent of converting it the economic benefit of any entity apart from the victim company. Since collection of data by China's Unit 61398 might have various purposes which the U.S. government concedes may be legitimate (national security interests), then to meet the diplomatic test implied by U.S. policy and to pre-empt a defense of sovereign immunity, the prosecutor would have to provide evidence of an intent over and above a national security or political impulse.

Proving this distinction would be complicated by the fact that all victim manufacturers companies were in fact suppliers to the U.S. armed forces and would therefore be a legitimate target of national security espionage. In the case of Westinghouse, which supplies military reactors to the United States, its main Chinese counterpart, with whom it does big business, is the China National Nuclear Corporation, the absolute epicenter of all China's military and civil nuclear power research and policy. Westinghouse itself, like its main Chinese competitor, is so deeply involved in the national security sector (supplying naval nuclear reactors) that it appears to be a poor choice for action by the United States as part of a ground-breaking diplomatic strategy that relies at its core on a clear distinction between the civil and national security sectors.

To prove this additional intent under §1832, compared with §1831, the prosecutor might need several pieces of evidence. It might include a secret Chinese document, if one exists, that directs PLA staff to collect such information in order to pass it on to Chinese civil sector manufacturers.

It might include secret U.S. intelligence showing that the collecting agency involved, Unit 61398 of the Third Department of the PLA, had passed the specific information on to a specific civil sector manufacturer or had consistently passed similar information on to a range of manufacturers, or intermediaries. The indictment specifically claims the latter – a secret deal between SOE1 and officers of Unit 61398 in the case of the theft of civil nuclear information from Westinghouse and SOE2 in the case of the steel sector, involving United States Steel (USS). The indictment mentions no similar deal in respect of the solar sector and that may be the reason why no count under §1832 has been brought in respect of SolarWorld's trade secrets. There is a question as to why no count under §1832 was brought in respect of USS.

It is of some note that the U.S. strategy for combatting trade secret theft which was released in February 2013 placed most emphasis on diplomatic persuasion of U.S. trade partners to monitor and control trade secret theft, backed up where appropriate by domestic law enforcement action by the FBI and DoJ.[12] Even so, one of the methodologies for the DoJ and FBI was supposed to be to "encourage cooperation with their foreign counterparts"[13] alongside enforcement action. Deterrence of foreign states from industrial espionage by bringing court cases against their foreign intelligence officials operating from home base was not mentioned.

On 22 May, Assistant Attorney Carlin claimed that a more direct motivation for the Administration in bringing the indictments was to respond to the Chinese government which had denied such activities were occurring: "the Chinese said, bring us hard evidence, evidence that could stand up in a court of this criminal activity". One can presume that the indictments were the result of a judgment by some in the Administration that China had been given ample time

(one year since the Donilon demands) to respond but had failed to do so. Carlin expressed the hope that such public action as the indictments would lead the Chinese government to bring about a stop the criminal activity (without distinguishing between normal military intelligence collection and commercial espionage).

Evidence against China for "Civil" Sector Economic Espionage prior to the Indictments

To undertake such an unprecedented diplomatic act against China, a strong public case would appear to be essential. One part of the story is publicly available and credible – the charge that Chinese military agencies were collecting industrial secrets on a massive and unprecedented scale by cyber means.[14] In 2011 the U.S. National Counter Intelligence Executive (NCIX), issued a report on foreign industrial espionage against the United States.[15] It concluded that China was the most aggressive collector, ahead of Russia, Israel and France. It was the 14th annual report which NCIX delivers under a requirement levied by Congress, and which in its public versions had been identifying China as an aggressive collector of U.S. economic or technical intelligence since 1998.

The NCIX annual reporting addresses two problems: theft of economic information for national security purposes and theft of similar to benefit the civil sector and undercut the competitiveness of U.S. civil companies. That is the NCIX brief: its mission is to stop both, as it is law enforcement's responsibility to stop both. At the same time, in pressing China, the U.S. government has said repeatedly the two are distinct, can be distinguished in operational terms and has been calling on China to observe a norm that the latter collections (for benefiting the

civilian sector) is unlawful. But the DoJ had brought charges relating to on the former class of activity too.

The unclassified versions of the NCIX annual report on economic espionage began to call out China as a major offender around 1998. The report for the year 2000 relied on a survey by the NCIX of Fortune 500 companies to identify the following countries as the most active: China, Japan, Israel, France, Korea, Taiwan and India.[16] It was in its 2000 annual report that NCIX observed the first case of a successful prosecution under §1832 of USC 18 (inserted by the Economic Espionage Act 1996), and it was against a Taiwan firm and two Taiwanese executives. This annual report noted that collectors included "non-state-sponsored companies and individuals". The 2001 report included five cases involving China (four were for military related items, and involved breaches of export licensing, not theft of civil sector trade secrets), two cases involving Pakistan and one case involving Iran. The 2004 report cites three cases, involving Singaporean, China and Indian entities. The Chinese case was military.

The 2005 report makes up for lack of attention to China by reviewing the previous seven years: "a relatively small number of countries, though—including China and Russia—were the most aggressive and accounted for much of the targeting, just as they have since the CI Community first began systematically tracking foreign technology collection efforts in 1997". It is not clear whether the reference to China means the Chinese government, since the 2005 report also concludes that the bulk of foreign industrial espionage in the United States was conducted by individuals without prior assignments from their governments … and to "satisfy their desire for profits, for academic or scientific acclaim, or out of a sense of patriotism to their home

countries".[17] The 2005 report is also noteworthy because at that time it saw "suspicious internet activity" as one of the least popular methods of collecting trade secrets, and the most popular form being a direct person to person request. That said, the report devotes a short section to the "Internet—Coming into its Own as a Source of Technology Collection", citing a private sector Israeli case. The report observed that the "real concern for the CI Community is how many such attacks may have gone undetected".[18]

It was not until the report for 2007 that NCIX came out strongly against China on the cyber front.[19] The report reserved its judgment on whether these cyber attacks were all China-originated (the attribution problem) or originated in other countries. But it stated categorically that the "most of those convicted in FY 2007 of stealing US technologies or trade secrets for transfer abroad came from the private sector".

The data cited in a Table of "Arrests and Convictions for Economic Collection and Industrial Espionage Cases in FY 2007" starts with six cases from China, five of which are for military related breach of export controls, and one of which deals with commercially oriented trade secret theft. The table includes examples involving entities from Pakistan, the United Arab Emirates, Cuba, India, Indonesia, Iraq, Taiwan and a set of twelve examples involving Iran.[20] In the 2008 report, the similar table cites seven cases from China, all with military-related end uses.[21]

The NCIX report for 2009-2011, the first since the report for 2008, singled out Chinese actors as the most persistent collectors.[22] It was careful not to put all of the blame at the feet of the Chinese government, and it remained uncertain that all of the action from China-connected

computers was even undertaken by Chinese actors. It concluded that "Increasingly, economic collection and industrial espionage occur in cyberspace, reflecting dramatic technological, economic, and social changes".[23] For that reason, the 2009-2011 report concentrates on cyber espionage, while keeping up past practice of reporting on other means. The report cites one China-related example from the military sector and one from the civil sector on trade secret theft, and reports that six of the seven cases prosecuted under the Economic Espionage Act in 2010 involved Chinese entities. The report alluded to an "onslaught" of China-related cyber attacks but noted that the U.S. intelligence community "has not been able to attribute many of these private sector data breaches to a state sponsor".[24] It noted that some private sector companies it had consulted reported Chinese attacks, asserting a variety of differing private or governmental purposes.

The Chinese government's role in economic espionage for civil sector companies

In the indictments, the United States says it has evidence of transfer of trade secrets to civil sector companies in the cases of Westinghouse and USS, but while other instances have been asserted, few have been evidenced. It is axiomatic that loss of a trade secret does not automatically convert to damaging competition any more than theft of credit card details translates into losses for all of the victims. In fact, very few people suffer personal financial losses as result of the theft and illegal sale of millions of credit card details.

The 2013 strategy mentioned document above ("Whitehouse Strategy for Mitigating Theft of Trade Secrets") is the most extensive compilation by the U.S. Administration of specific cases of

Chinese industrial espionage. The body of the report contains seven very short case studies in just a few lines each. Each of these has an estimate of commercial damage, but the document does not give any explanation of how the figures were arrived at, how any competitive damage was estimated, and whether there was direct Chinese government involvement. In all of the seven cases, the Strategy notes a visible motivation of a personal kind by people who were not employed by the Chinese government rather than evidence of action on behalf of any government. The first six of the seven cases involve people of Chinese origin or ethnicity seeking to create a benefit for themselves and for Chinese firms, but there is no indication of direct Chinese government involvement in any of these cases. The perpetrators in these six cases were not commissioned in advance to steal the secrets but, on the contrary, actually tried to find buyers for them only after the fact. See Tables 1 and 2 below based on the case summaries.

TABLE 1 *Seven Highlighted Case Studies In Body Of The Whitehouse Strategy*

Company	*Estimated loss based on variable sources*	*Competitive damage evidenced by USG*	*Chinese government involvement evidenced by USG*
Ford Motor Co	$50m	No	No
DuPont	$400m	No	No
General Motors	$40m	No	No
Dow and Cargill	$7m to $20m	No	No, maybe[25]
Valspar	$7m to $20m	No	No[26]
Motorola	$0 (no secrets passed)	No	No, but[27]
Goldman Sachs	$500m	No	No[28]

In one of several annexes, the strategy document provides a summary of twenty Department of Justice cases of economic espionage from January 2009 to February 2013, including the first six above. Two of the cases are repeated with a slightly different summary (the case affecting L-3 Communications and the case affecting General Motors).[29] Table 2 summarizes the remaining twelve in the same way as Table 1.

TABLE 2 *Additional 12 DoJ Cases in Annex of the Whitehouse Study*

Company Affected	*Estimated loss based on variable sources*	*Competitive damage evidenced by USG*	*Chinese government involvement evidenced by USG*
DuPont and Teijin[30]	No	No	No[31]
L-3 Communication (M)	No	No	No
CME Group	$50m to $100m	No	No
Pittsburgh Coring	No	No	No
Orbit Irrigation Products	No	No	No
DuPont	No	No	No
Sanofi-Aventis	No	No	No
Dow	No	No	No
Frontier Scientific	No	No	No
Akamai	No	No	No[32]
Company A	No	No	No
Boeing	No	No[33]	Yes – "spy"

In 2013, a bipartisan Commission on IP Theft made several key conclusions.[34] One of the three items in its terms of reference was to "document and assess the role of China in international intellectual property theft". It accepted numerous sources of evidence that China (as a geography) accounted for between 50 per cent and 80 per cent of all theft of American IP. It concluded that:

- "National industrial policy goals in China encourage IP theft
- and an extraordinary number of Chinese in business and government entities are engaged in this practice"
- Companies in China which benefit from IP theft are immune from consequences and can only be deterred if they face sanctions in the market place (since the legal system was not by themselves delivering the needed results).

The Commission's recommendations for new policy are wide-ranging, balanced and well thought out. They give considerable emphasis to diplomacy, to legal and institutional reform inside the United States, and help to China to become a "self-innovating economy" rather than one that focuses on "indigenous innovation". Sadly, these recommendations see little light of day in the Administration's strategy for mitigating IP theft issued only three months earlier. From the legal point of view, several recommendations speak to the role of the Department of Justice. The Commission recommended that the National Security Adviser coordinate all national policy in this area and that the Secretary of the Department of Commerce be empowered to serve as the "principal official to manage all aspects of IP protection" and to guide punitive measures against corporations under the sequestration powers of the international Trade Commission and by the Secretary of Treasury in respect of access to the U.S. banking system. It recommended that the DoJ and FBI get increased resources to investigate and prosecute IP theft, especially that enabled by cyber means.

While recognizing that China as a geography was the worst source of IP theft, the Commission acknowledged that "Much of this theft stems from the undirected, uncoordinated actions of Chinese citizens and entities who see within a permissive domestic legal environment an opportunity to advance their own commercial interests".[35] The report noted that these privateers were encouraged by relative impunity for offenses and large profits available.

The most substantial scholarly effort to address the scale of China's state-sponsored industrial espionage is probably a 2013 study, titled *Chinese Industrial Espionage*.[36] Yet seven of its ten chapters address what are largely lawful methods of technology transfer, such as use of open

sources, student exchange programs, joint ventures and licensing. That is essential context, but a number of key distinctions and linkages are not addressed in the book as fully as they might have been. For example, in an appendix listing 33 "Cases Histories of Chinese Industrial Espionage", only five appear to have been prosecuted under the economic espionage provisions. The other 28 involved breaches of export control acts affecting military or dual use technology, or simply military technical espionage. The study documents the lawful and covert (unlawful) methods of technology acquisition, and asserts a threat to the United States (and the world) in China's policies because it is able to acquire technology without paying for it and "without compensating its owners". The book is impressive, but it does not offer any effort to quantify the balance between lawfully obtained technology and stolen technology, nor does it compare in any meaningful way, the practices of China and other states. Its charge that China is the biggest cheater in the global economy may be true but that is not evidenced in the book. The section in the book on "Managing cheaters in a global society" appears to want to address the international political economy of technological innovation but is in fact about U.S. policy for control of classified or controlled information.

The 2012 report by Mandiant, prefaced by assertions of officially sponsored cyber espionage for civil sector benefit on a massive scale ("piracy", "trade war", "scourge"), reminds us that in 2010, the company concluded that "The Chinese government may authorize this activity, but there's no way to determine the extent of its involvement."[37] It then went on to report a changed assessment, convinced "that the groups conducting these activities are based primarily in China and that the Chinese Government is aware of them". But these statements refer only to "computer security breaches at hundreds of organizations around the world", not to evidence

industrial espionage being converted to commercial civil sector profit. The report said that since 2006, Mandiant had tracked breaches against "141 companies spanning 20 major industries" – around the world, of which 115 were in the United States. It identified 20 sectors, as diverse as high tech electronics and media and advertising. But beyond this, it provided almost no evidence on the claims of state-sponsored economic espionage intended for conversion to the benefit of civil sector companies. Its claim that "targeted at least four of the seven strategic emerging industries that China identified in its 12th Five Year Plan" is entirely credible (as it would be normal for the United States to do the same), but this is not evidence that supports a claim of piracy and trade war in the civil sector. The main contribution of the Mandiant report was to establish that the Chinese PLA was the source of cyber espionage attacks that had previously not been attributable to China. It did not offer any confirmation as to the purpose (military or civil) or the commercial result of the espionage.

S&T Intelligence Priorities: Military Interests and Defense Industry Customers

Chinese military signals intelligence units which collect the commercial data have a brief to support the country's wider intelligence community in its scientific and technical intelligence collection and analysis (S&T intelligence or S&TI).

In the case of the United States, the purpose of S&TI is to "to provide a comprehensive picture of global scientific and technological advancements."[38] A 2013 U.S. report on U.S. S&TI called out the high priority to be attached to this: "Failure to properly resource and use our own R&D to appraise, exploit, and counter the scientific and technical developments of our adversaries—

including both state and non-state actors—may have more immediate and catastrophic consequences than failure in any other field of intelligence."[39] The report opens with the statement that "The global spread of scientific and technical knowledge challenges U.S. national security." The United States officially acknowledges that it pursues S&TI to "counter" the scientific advances of other countries.

This then is the policy environment in which Chinese and other countries' intelligence agencies must operate. China's leaders must have similar motives as U.S. leaders to undertake national security espionage that collects industrial secrets. For countries like China subject to export controls on certain technologies by the United States, having no intelligence allies, and almost certainly less adept at intelligence than the United States, the challenges must be enormous.

It should be noted that in both countries it would be illegal for an intelligence official to pass a trade secret obtained by espionage to a commercial entity for its commercial benefit. Assistant Attorney General, John Carlin, conceded on May 22: "we know of no nation that stands up publicly to defend corporate theft for the profit of state-owned enterprises".[40] He went on to say that "in the shadows, there may be some who encourage and support it". This is almost certainly what is happening in China. More about those shadows later.

There are five important steps in the intelligence cycle (prioritize, collect, process, analyze, disseminate). The evidence placed in the public domain by the U.S. Administration about China's activities provides only the briefest of glimpses of official dissemination, and then to

firms that may well be military related. But the body of evidence ignores important questions about the intelligence cycle that it might have been expected to comment on.

Priorities

The first is the priority attached to different pieces of information received by the PLA. Assuming, as I think we can, that the Chinese PLA exfiltrated all data from the files of the most victim companies that they accessed. For example, if we take the case of solar panels, the PLA would see access to technological secrets on solar panel development among their high priorities for national security purposes. The victim company, Solarworld, has been a supplier to the Pentagon, at least since 2009. There are many military uses of solar energy and the Chinese armed forces have been struggling to keep up. Solar technologies are used in many ways by the U.S. armed forces and intelligence agencies:

- to power satellites involved in ballistic missile launch detection and surveillance[41]
- as an essential component of tactical network warfare[42]
- electric plants for important bases, such as Nellis Air Force base[43] and Fort Bliss,[44] the latter being home to theater missile defense units that have been forward deployed in the Western Pacific
- R&D on solar energy
- to power forward operating bases in Afghanistan.[45]

China's armed forces are investing in solar technology research but on nothing like the scale of the U.S. armed forces and Department of Defense. Chinese military intelligence customers at the operational level would want to know all about military applications of the technology and about military procurement arrangements for the technology, including price.

The proposition that the GSD Third Department may be supported (funded) directly by commercial enterprises which help to set its intelligence collection priorities is not one that, as a general rule, appears credible in the light of the decommercialization of the PLA in the past twenty years. I would agree with the analysis that "The classified intelligence collected by PLA intelligence agencies are likely to be only available for the military component of the IAD system, which is centralized under the China Defense Science and Technology Information Center (CDSTIC) that is affiliated with the GAD."[46]

Collect

There is no doubt that millions of documents obtained by cyber espionage containing valuable IP and other business secrets now sit inside Chinese military databases. The public case against the Chinese government as IP thief by cyber means is premised on the assumption that in the cases of cyber espionage mentioned, the main purpose of the physical collection of the information was to steal commercial intelligence that can be used in a contemporaneous, commercially relevant fashion, either relating to current business negotiations or to a the start-up of a new manufacturing process, or to the adaptation of an existing manufactured product. There is also an implication that the outside observer can exclude other, equally plausible motivations

for the collection. Another way of understanding this proposition is to ask: what else apart from market-influencing trade secrets was being collected and why? One answer is given above: the IP information is intended for China's military S&TI, including recipients who have a dual civil-military profile. A second answer is that some of the information, concerning international trade negotiations (price and positions), is intended to inform contemporaneous decision-making by government agencies.

This is a large unanswered question about the collection process. How can observation of cyber espionage (hacking into a computer and siphoning up all data) reveal anything about which pieces of the data had the highest priority? There would need to be evidence on the collection priority.

Analyze

This is the biggest gap in U.S. official complaints about China's cyber espionage for civil sector companies. The terabytes of data collected every week from the United States are mostly in English, and sit in documents as varied as emails, letters, contracts, technical plans and drawings, personnel files, maintenance plans, and strategy documents. Some folders may contain several if not hundreds of drafts rather than final versions. A careless analyst may in fact pick up an earlier cost estimate or technical specification that has been superseded. The final version of a technical plan may be stored in a different folder from experimental versions. For each raid by one hacker, the volume of material that would need to be sifted by an English speaking analyst with the requisite superficial knowledge to be passed to the translator could take a month to sort through.

As a comparator, when a group of Western journalists gained physical access to a single hard drive of financial data from the British Virgin Islands and Cook Islands, with most documents in the analysts' native language, alongside thousands of spreadsheets, it took a team of more than sixty experts a year to exploit a fraction of the documents. The subsequent report on Chinese citizens named in the files took over a year to research and compile. As another comparator, more than a year after Edward Snowden leaked large volumes of documents from NSA, only a small percentage of them have been exploited. The same problem of volume applies to public exploitation of the Wikileaks cables posted to the web in 2010. It seems wildly improbable that China's PLA translates more than a tiny fraction of the intelligence its scoops up. It would follow highest priorities first and foremost: those of national security.

Dissemination

Which Chinese corporations are involved? The indictment does refer to beneficiary companies in China -- SOE 1(in the nuclear sector) and SOE2 (in the steel sector) -- but does not offer further details on the identity of these. In respect of the solar industry, the documentation from the DoJ makes clear that they are those companies, or at least one of them, exporting solar energy products to the United States. Since there are some 400 firms which may be in that category, including many contracted to U.S. solar industry firms, is it the U.S. government's contention that the PLA is broadcasting its secret intelligence to all of the 400 companies in the solar energy sector in China, many with foreign employees and some with foreign directors, spread throughout China and with subsidiaries in other countries, including the United States? Or are only certain Chinese companies, favored? The latter seems more likely. How would a

manufacturer in China win this lottery and be favored to be the recipient of such secret intelligence?

There are two main possibilities. Either the PLA has an office whose function is to identify selected companies and routinely supply one or two handpicked employees with secret intelligence of military or dual use character; or the activity is not sanctioned by the government and it involves corrupt payments by one or more corporations or individuals to a small number of PLA intelligence collectors or analysts, or those with access to the information. The indictment says that in the case of the nuclear industry, one SOE "hired" Unit 61938 to "build a 'secret' database to hold corporate 'intelligence'."[47] That would almost certainly be a corrupt and criminal act under Chinese law.

There is strong evidence of a dissemination chain from China's PLA intelligence community to China's defense industry,[48] as we might expect. As far as I can tell, there is no public domain information on a PLA industrial espionage liaison department set up for the purpose of feeding selected Chinese manufacturers outside the defense sector the market data obtained by cyber means. In the United States, information collected by NSA is usually classified Secret or Top Secret and circulated on a tight need to know basis. But it is interesting to explore the second option. Are there are Chinese companies which have improper links to the PLA intelligence agencies, or those with access to the information? Well, it appears that there may be such links. Has there been high level corruption in China's intelligence agencies? Yes, all the way to the top, including the country's most senior Party leader responsible for intelligence and security, Zhou Yongkang, who would have had been able to gain access to commercially sensitive intelligence

product. The Chinese security and intelligence services are riddled with corruption, as recent cases demonstrate.

In China, there are several legal and regulatory obstacles (non-transfer of state secrets) but the most important barrier is a political one, not a legal one. The Chinese Communist Party (CCP) has spent two decades getting the PLA out of commercial activities. Perhaps it can turn a blind eye to Chinese civilian companies getting illegal access to trade secrets, but it is opposed 100 per cent opposed to corrupt relationships between PLA personnel and powerful commercial actors. It would be extremely unhappy about non-official uses of the cyber espionage capabilities of the PLA, since these could be turned against the leaders. As in the United States, but more so in China, it is in the nature of the work that intelligence officials can do many things with little accountability. There is so little scrutiny of day to day activity. If in the U.S. system, against the wishes of the government, Edward Snowden could steal what he did over an extended period and leave the country, then one can imagine a similar room for maneuver for the average Chinese intelligence operative has for simple theft of information without legal authorization from his/her superiors. The picture painted by the 2013 Mandiant report of the lack of professionalism of some of the officers of Unit 61398, including security breaches by them, paints the PLA in a less than impressive light.

Open-sourced collusion

One source of evidence for the case that espionage was not critical to the pricing outcomes comes from the solar panel industry. It is the allegation that the price of Chinese solar products

was set by collusion between Chinese companies, themselves competitors against each but working under the proposition that they could collude to establish a "Chinese" cartel. Details of one such allegation can be found in civil proceedings involving three Chinese-owned U.S. corporations (Suntech, Trina and Yingli) as the cause of bankruptcy of a U.S. corporation, the case of Solyndra v. Suntech.[49] The case documentation identifies the instigator of the collusion as the companies themselves, not the Chinese government.

Implications for U.S./China Relations

The conduct of effective diplomacy requires pragmatism, predictability, diplomats in control of the policy making who know the technical issues well, and a high degree of national unity on the issue at hand. These characteristics have rarely been present simultaneously in the conduct of U.S. diplomacy toward China on cyberspace issues. The main reason is that the big destabilizer to pragmatic American diplomacy across the board – its passionate and principled support to defense of human rights – is so strongly in play on a daily basis because of China's censorship of the internet and persecution of people who use it to support human rights. One example both of the defense of human right but a disturbing lack of consistency emerged within months of the now famous speech by Hilary Clinton, then Secretary of State, on internet freedom in January 2010. The speech was seen by many as an attack on China. She said that "Countries or individuals that engage in cyber attacks should face consequences and international condemnation".[50] In July that year, she was confronted with the publication of news of the Stuxnet attack by the United States on Iran – an unlawful act of cyber sabotage under

international law. The United States had done what she said should result in consequences and international condemnation.

This sort of experience suggests not only that the art of cyber diplomacy, like the epistemic community around it, is quite new and still in learning mode. My analysis for this article suggests that the diplomacy for managing cyber espionage is of even more recent provenance and probably even more challenging for that. In both the United States and China, important institutions to handle the twin diplomatic challenges (cyberspace policy and cyberespionage) have been set up in the last two to five years. In the United States, there is visible evidence, as this article suggests, that officials engaged in the diplomacy of managing cyberespionage, especially that targeted at sensitive information for commercial gain, do not have a consensus view of where the practice sits in overarching taxonomies of diplomatic practice, espionage or trade secret theft.[51] The most damning consideration for the United States is related to the absence of various taxonomies. It (like its allies) has been engaged in a policy for the lawful transfer of technology to China on a massive scale for three decades. This represents a very large transfer of wealth. It is simply not credible superficially, and certainly not without evidence and some effort at quantitative analysis, to say that that China's cyber espionage represents the "largest transfer of wealth in human history". For example, Westinghouse has a lawful joint venture in China under which it has transferred 75,000 documents containing technical specifications.

My research suggests that the indictments signaled a return to contest among different arms of the U.S. government on cyber space issues and even on the big issues of the bilateral

relationships (“trust and trade” vs. “critique and contain”). The indictments for cyber espionage were undertaken by one arm of the United States government (the Attorney General and his Justice Department) pursuing its lawful remit but in a way that scuttled in one blow much hard work in bilateral diplomacy by the State Department and by others in the immediately preceding years. It is not apparent from the public record how much consultation there was between the DoJ and the State Department about the indictments, which were secret until unsealed. The move by the Justice Department set a new standard for unpredictability and surprise in U.S. diplomatic practice, as well as a precedent in international diplomatic practice.

Attorney General as a U.S. Foreign Policy Actor

The lead prosecutor in the indictments, John Carlin, held the post of Assistant Attorney General leading the National Security Division of the Justice Department. The circumstances of the emergence of this division raises some questions about how well integrated it is into the country’s diplomacy. It appears to have only commenced its work on cybersecurity in 2012, less than two years prior to announcing the grand jury indictments. According to Carlin, The Division, set up in 2006, was the department's “first new litigating section in half a century”. This is a very new American institution. He foreshadowed prosecutions against cyber criminals as the “new normal”, as the “threat we face is increasingly moving out of the physical world and into cyberspace”. Carlin saw the office as an important adjunct to U.S. diplomacy, particularly in helping officials to “lay out evidence of state-sponsored cyber theft to foreign government officials, and force them to answer for those actions”.[52] This last remark suggests that prior to his pursuit of the indictments against the five Chinese military personnel that Carlin at least shared

the basic intelligence with his State Department counterparts to help them persuade the Chinese government to act.

Yet as political scientists we probably should look to the consideration of institutional disarray as a major factor in the bringing of these unprecedented charges in such a way as to seriously disturb U.S. diplomacy with China. The National Security Division of the DoJ had been at the epicenter of grueling, but unpublicized battles in the Administration for more than a decade over the constitutionality of a range of NSA programs and other national security practices, including the illegal rendition, unlawful detention and extra-judicial killing of terrorist suspects. As a result of the review of NSA in the wake of the revelations by Edward Snowden, President Obama was highly critical of the agencies involved,[53] one of which was the National Security Division of DoJ, responsible for managing the applications for surveillance to the Foreign Intelligence Surveillance Act court.

May 2015 Indictment

The indictment unsealed on May 18 2015 in California alleges that six defendants and unnamed others conspired to and did steal trade secrets from two U.S.-based companies for the benefit of the Chinese government and other instrumentalities.[54] There are 32 counts, all brought under §1831 and §1832 (compared with only one count under each of the same sections in USC18 in the May 2014 indictment). There are other important differences between the two indictments. The 2015 indictment does not identify a specific Chinese government agency, such as the PLA, as either the perpetrator or beneficiary. It does identify the University of Tianjin, as a

government-funded university, and related organizations, as an arm of the Ministry of Education. For its allegation that the trade secret theft was to the "benefit of the PRC government", as opposed to simply a Chinese private corporation, the indictment appears to rely on several considerations: the status of Tianjin University as government-funded; that it receives government grants under a strategic investment program launched in the 1980s; that the technology stolen had a potential military application; that the defendants referred several times in their alleged communications that they were stealing the technology for China; and the fact that key people in the decision-making chain in the university held national level appointments, such as a role in the Chinese People's Political Consultative Committee. There is room for debate how a U.S. court would rule on the meaning of "benefit of the PRC government" but there is a considerable gap between the import of these considerations and the suggestion in the associated DoJ press release that the government of China directly "sponsored" the alleged crimes.[55] As a counter to that proposition, there are several indirect indicators in the indictment that the government of China did not sponsor the specific crimes. The most important is that the defendants are alleged to have been pursuing venture capital for the commercial entity they set up with the university. They probably would not need to do so if the Chines government were directly engaged in the trade secret theft. The U.S. government may have additional classified information on relationships between the defendants' crimes and other Chinese government agencies, but these linkages would not be seen by most China analysts as evidence that the central government sponsored (meaning "knew about and encouraged") the alleged crimes.

Conclusion

There can be no doubt that Chinese intelligence agencies are scooping up vast amounts of commercially sensitive information from U.S. companies that only has applications in the civil economy and that if converted to usable technology or commercial negotiations would undermine the competitiveness of U.S. firms. The United States must prosecute the universally acknowledge crime of commercial espionage wherever the trail of culpability lies, even if that be a foreign government. However, the U.S. claim that is Chinese government policy to direct its intelligence officials (or state funded universities) to hand over highly classified information to its civil sector firms on a mass scale is not proven by the U.S. Administration in the public record to date. There is no convincing evidence in the public domain that it is China's policy to undermine U.S. economic prosperity and business competiveness at a macro level through commercial espionage. The United States may have such evidence but there is considerable room to believe otherwise. U.S. government agencies have repeatedly indicated private citizen motivation as a powerful force in such activity. In any event, there is such significant blurring between R&D in the civil and military sectors, in China as in the United States, that a diplomatic or influencing strategy premised on this distinction and involving unprecedented legal action against Chinese military personnel was probably not a wise idea for the United States.

There is however a deeper issue. This is the belief being fostered by U.S. officials among elites in the United States and in other countries that China as a nation is a "cheater" country that arises from the unsubstantiated allegations about the commercial impact of its cyber espionage. It may be time for the Administration to recognize that, like the bomber gap (1950s), the division gap (1960s), the civil defense gap (1970s), the cyber espionage gap with China is simply not what

they say it is. Either that, or it needs a whole lot more evidence to make a public case to support the claims. Unless that happens, the indictments will go down in history as one of the strangest undertakings in U.S. diplomacy.

---

[1] Greg Austin is a Professorial Fellow with the EastWest Institute in New York and a Visiting Professor at the Australian Centre for Cyber Security in the University of New South Wales (Canberra) at the Australian Defence Force Academy. He is the author of *Cyber Policy in China* (Cambridge: Polity 2014).

[2] Remarks By Tom Donilon, National Security Advisor to the President: "The United States and the Asia-Pacific in 2013", The Asia Society, New York, NY, Monday, March 11, 2013, http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a.

[3] Lisa Daniel, "DOD Needs Industry's Help to Catch Cyber Attacks, Commander Says", General Keith Alexander, DoD News, March 27 2012, http://www.defense.gov/news/newsarticle.aspx?id=67713. The turn of phrase was used by General Keith Alexander, the commander of Cyber Command and Director of the National Security Agency before a Senate committee.

[4] Federal Attorney's Office, District of Southern California, Department of Justice, "Chinese Professors among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People's Republic of China", May 19 2015, http://www.justice.gov/usao-ndca/pr/chinese-professors-among-six-defendants-charged-economic-espionage-and-theft-trade

[5] The full text of the indictment can be found at United States v. Wang Dong et al, United States District Court Western District of Pennsylvania, filed May 1 2014 under seal, Criminal No. 14-118, http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.

[6] State Department, Background Briefing on the Strategic and Economic Dialogue, Special Briefing Senior Administration Officials En Route to Beijing, China, July 7, 2014, http://www.state.gov/r/pa/prs/ps/2014/07/228852.htm.

[7] "Remarks by Assistant Attorney General for National Security John Carlin at a Brookings Institution Discussion", Federal News Service, May 22 2014, Subject: "Tackling Emergency National Security Threats through Law Enforcement" Moderator: Benjamin Wittes, Senior Fellow in Governance, Brookings Institution Location: Brookings Institution", Thursday, May 22, 2014, source: Nexis.

[8] State Department, Statement of Interest of the United States of America in Ra'ed Mohamad Ibrahim Matar v. Avraham Dichter, 05 Civ.10270 (WHP), Southern District Court of New York, November 17 2006, http://www.state.gov/documents/organization/98806.pdf.

[9] "It is the consistent practice of the United States not to plead sovereign immunity in foreign courts for instances where, under United States law, the *United* States would not recognize a foreign state's immunity if it were sued in the United States." See Digest of United States Practice in International Law 1989–1990, Office of the legal Adviser, Department of State, International law Institute, Washington DC, 2003. p. 294; http://www.state.gov/documents/organization/139393.pdf

[10] Chimène Keitner, "Guest Post: Foreign Official Immunity and the Chinese Cyberespionage Indictments", opiniojuris website, http://opiniojuris.org/2014/05/21/guest-post-foreign-official-immunity-chinese-cyberespionage-indictments/.

[11] Department of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage, May 19 2014, http://www.justice.gov/opa/pr/2014/May/14-ag-528.html.

[12] The White House, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets", February 2013, http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

[13] Ibid. p.5.

[14] See National Counter Intelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011*, October 2011, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf; Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Feb. 2013),

http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf; See also Laura Saporito and James A. Lewis, "Hacking incidents attributed to China", http://csis.org/files/publication/130314_Chinese_hacking.pdf.
[15] National Counter Intelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011*, October 2011, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.
[16] NCIX, Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, http://www.ncix.gov/publications/reports/fecie_all/fecie_2000.pdf.
[17] P. 3. http://www.ncix.gov/publications/reports/fecie_all/FECIE_2005.pdf.
[18] P. 9.
[19] NCIX, "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY07", 10 September 2008, P. 4. http://www.ncix.gov/publications/reports/fecie_all/fecie_2007/FECIE_2007.pdf.
[20] Ibid. Pp. 9-14.
[21] NCIX, "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY 2008, 23 July 2009, pp. 9-11, "http://www.ncix.gov/publications/reports/fecie_all/fecie_2008/2008_FECIE_Blue.pdf.
[22] NCIX, *Annual Report 2009-2011*, p. i.
[23] Ibid. P. 1.
[24] Ibid. p. 5.
[25] The recipients were Chinese universities working on Chinese government contract.
[26] The receiving paint company in China is Japanese-owned.
[27] US Attorney's Office, Northern District of Illinois, "Suburban Chicago Woman Sentenced", August 29, 2012, http://www.fbi.gov/chicago/press-releases/2012/suburban-chicago-woman-sentenced-to-four-years-in-prison-for-stealing-motorola-trade-secrets-before-boarding-plane-to-china. PLA was alleged to be an intended recipient, but the court brought a not guilty verdict against charges relating to economic espionage on behalf of the government of China. The communications company in China for which the convicted felon was working was a contractor for the PLA and had provided the felon with secret Chinese military documents, which the FBI found in her possession. The explanation for this from the FBI was that the company had provided the documents so that she might better understand what to steal from Motorola.
[28] Not a single mention by the U.S. government of a foreign government involvement. Conviction for the alleged crime of economic espionage was overturned on Appeal.
[29] Another three cases (Boeing, DuPont and Valspar) had been reported in the NICX 2011 report.
[30] A Japanese company.
[31] Executives of a Korean firm were the perpetrators. No foreign government involved at all.
[32] FBI entrapment case, posing as Israeli official.
[33] It appears that the felon was an agent of the Chinese government for 30 years. http://www.fbi.gov/news/podcasts/gotcha/dongfan-greg-chung.mp3/view. His brief appears to have been military technology intelligence collection rather than enabling commercial competitors. According to the FBI, "he was sent to the United States in 1978 in order to obtain employment in the defense industry with the goal of stealing US defense secrets, which he did for over 20 years." http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat.
[34] *Report of the Commission on the Theft of American Intellectual Property*, May 2013.
[35] Ibid. p. 18.
[36] William G. Hannas, James Mulvenon and Anna B. Puglisi, *Chinese Industrial Espionage: Technology acquisition and military modernization*, London and New York, Routledge, 2013.
[37] Mandiant, APT1, p. 2.
[38] Report of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community, Unclassified Version, p. ii, http://www.fas.org/irp/eprint/ncrdic.pdf.
[39] P. iii.
[40] "Remarks by Assistant Attorney General for National Security John Carlin at a Brookings Institution Discussion", Federal News Service, May 22 2014, Subject: "Tackling Emergency National Security Threats through Law Enforcement" Moderator: Benjamin Wittes, Senior Fellow in Governance, Brookings Institution Location: Brookings Institution", Thursday, May 22, 2014, source: Nexis

[41] U.S. Department of Defense (News release), "DOD's Scarlet-II Successfully Launched on Deep Space 1", October 26 1998, http://www.fas.org/spp/starwars/program/news98/b10261998_bt550-98.html.
[42] Scott Gourley, "DARPA Advancements provide Alternative Energy and Power" in U.S. Defense Advanced Research Projects Agency, *DARPA: 50 Years of Bridging the Gap*, Faircount LLC, 2008, p. 170.
[43] Jim Garamone, "Obama Touts Solar Power at Air Power Hub", American Forces press Service, 27 May 2009, http://www.defense.gov/news/newsarticle.aspx?id=54526.
[44] Dona Miles, "Missile Defenders Trained, Ready for Deployment, General Says", U.S. American Forces Press Service, April 5, 2013, http://www.defense.gov/news/newsarticle.aspx?id=119714. "The THAAD system is a land-based missile defense system that includes a truck-mounted launcher, a complement of interceptor missiles, an AN/TPY-2 tracking radar and an integrated fire control system."
[45] Lisa Daniel, "Marines Prove Energy Efficiencies in Afghanistan", American Forces Press Service, May 5 2011, http://www.defense.gov/news/newsarticle.aspx?id=63841.
[46] Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application", in Jon Lindsay, Tai Ming Cheung, and Derek Reveron (eds), *China and Cybersecurity* (Oxford University Press, Forthcoming, 2014/15, available in draft at http://goo.gl/6VytNy.
[47] Mandiant, op. cit. p. 3.
[48] See Lindsay and Cheung, op. cit.
[49] The Solyndra Residual Trust vs. Suntech Power Holdings, Suntech America, Trina Solar Limited, Trina US, Yingli Green Energy Holding Ltd, Yingli Green Energy Americas Inc ("Solyndra v. Suntech"), http://www.jdsupra.com/legalnews/us-china-trade-war-developments-trade-41373/.
[50] State Department, Remarks on Internet Freedom, Hillary Rodham Clinton, Secretary of State, Washington, DC, January 21, 2010, http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.
[51] The importance and character of an overarching taxonomy in the case of trade secret theft is demonstrated in Arnold Reisman, "Illegal Transfer of Technologies: A Taxonomic View", September 8, 2004. Available at SSRN: http://ssrn.com/abstract=532522 or http://dx.doi.org/10.2139/ssrn.532522. A taxonomy allows policy makers and their agents to understand priorities and relationships.
[52] Remarks at Brookings, May 22, 2014.
[53] In his speech on the review he had ordered into NSA after the Snowden revelations, Obama said: "it is not enough for leaders to say: Trust us. We won't abuse the data we collect. For history has too many examples when that trust has been breached." White House, "Remarks by the President on Review of Signals Intelligence", January 17 2014, http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.
[54] United States District Court, Northern California District Court, San Jose Division, "The United States of America versus Wei Pang et al", April 1 2015, unsealed May 18 2015, https://s3.amazonaws.com/s3.documentcloud.org/documents/2083667/indictment-of-6-chinese-citizens-on-charges-of.pdf.
[55] Federal Attorney's Office, District of Southern California, Department of Justice, "Chinese Professors among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People's Republic of China", May 19 2015, http://www.justice.gov/usao-ndca/pr/chinese-professors-among-six-defendants-charged-economic-espionage-and-theft-trade.