Red-Handed: Assessing the Depths of Chinese Economic Espionage

Alexander Hoskins

It is no secret that China is a hotbed of Intellectual Property (IP) theft. Tourists around the world flock to China's markets for high quality counterfeit goods, streets abound with peddlers of DVDs of movies that have not even hit theaters, and Chinese hackers consistently make international news for targeting and exploiting databases of the US government and major international firms. Despite this popularly held belief indicting China as the world's largest IP thief, the indictment gets messy when we try to separate Chinese actors from China. While it is clear that a fair amount of IP theft is conducted in China, the picture gets muddled when we try to see who exactly is pulling the strings behind these criminal acts. Is the Chinese government waging the same war as the international community against perpetrators of IP theft, or does the evidence catch China red-handed?

What is Economic Espionage?

Before we can understand the evidence pointing to the Chinese government's (herein referred to as "China's") involvement in these activities, we need to set our definitions straight. The term "economic espionage" (EE) conjures images of high-tech gadgets and spy craft; but in actuality, the practice has been around for centuries. EE, despite the modern connotations of its latter half, is just "covert actions intended to eliminate market advantages," a technique familiar to any business owner facing stiff competition from an innovative counterpart.[1] Strictly speaking, EE carries a somewhat more severe connotation; beyond the

1. Anthony Crescenzi and Herbert Snyder, "Intellectual Capital and Economic Espionage: New Crimes and New Protections," *Journal of Financial Crime* 16, no. 3 (2009): 246.

act of simply stealing trade secrets or undercutting the competition, EE is the systematic misappropriation of "trade secrets belonging to citizens of one country in order to benefit another country, to include the unlawful taking [and use] of proprietary information by anyone not lawfully entitled to it."[2] Beyond mere theft of trade secrets, EE pits one country against the business of another country (i.e. China targeting IBM), unlawfully acquiring proprietary information for the explicit purpose of furthering the "strategic initiatives of a sovereign state," or harm the victimized nation.[3]

EE is on the rise. The United States recently equated the threat of EE to US companies to the threat of nuclear war with North Korea. [4]Globalization is proving to be the accelerant on the fires of EE, with the digital and communication revolutions bringing American corporations into a new plane of vulnerability. Chief among the dangers globalization has brought to victims of EE is the ability to access company data networks and computer systems remotely. Economic spies used to have to physically engage their target to acquire the proprietary information sought` but that physical requirement has been almost completely removed with remote access to these networks, such as through the Internet.[5]

Furthermore, as companies have become more successful, they have made themselves bigger targets for competitor nations.[6] Given the central role that innovation and IP have played in the rise of many of these corporate giants, foreign demand has skyrocketed for their secrets of success. [7]Of equal importance is the growing role that IP and proprietary information plays in the current corporate landscape. As IP becomes more and more crucial to corporate success, foreign nations increase their EE efforts to seize those properties and remove the competitive advantage of the innovator.[8] As globalization brings the world closer

2. Crescenzi and Snyder. "Intellectual Capital and Economic Espionage," 246.

3. Crescenzi and Snyder. "Intellectual Capital and Economic Espionage," 246.

4. Lee, John, "Cyber Kleptomaniacs: Why China Steals Our Secrets," *World Affairs* 176, no. 3 (2013): 73.

5. Crescenzi and Snyder, "Intellectual Capital and Economic Espionage," 247.

6. Crescenzi and Snyder. "Intellectual Capital and Economic Espionage," 247.

7. Stephen A. Carlton, "Industrial Espionage: Reality of the Information Age," *Research Technology Management* 35, no. 6 (1992): 19.

8. Crescenzi and Snyder, "Intellectual Capital and Economic Espionage," 246.

together and breaks down physical barriers to communication and access, the rising success of IP provides foreign competitor nations with an easily-targetable assets to steal a share of the profits.

EE, IE, and Competitive Intelligence Gathering

Two important distinctions must be made when considering EE. The first is between economic and industrial espionage (IE), with the primary difference being the aggressing agent. With EE, the aggressor is a state. States often have access to tremendous resources that vastly enhance the effectiveness of their espionage efforts (which is why it is so common). Unlike independent actors, a state has the authority and resources to conduct activities such as wiretapping, searching public/private properties, inspecting materials entering and exiting the state, and concealing measures of espionage implementation.[9] IE, on the other hand, is aggression by an independent actor, such as a business competitor. If Samsung were to spy on Apple to steal some type of trade secret, that would be an instance of IE; however if China were to spy on Apple (an American company) to acquire trade secrets that would somehow benefit China as a state, then that would constitute EE.

The second important distinction to make is between EE and competitive intelligence gathering (CIG). CIG is the lawful acquisition of proprietary information or any other information/materials, which might garner a market advantage. CIG is a viable market practice and used by almost all corporations.[10] When many people hear EE, they often confuse it with CIG, but unlike EE, CIG's collection methods are entirely legal (although the ethics can sometimes be questionable). CIG utilizes legitimate sources and inferences to acquire corporate intelligence, whereas EE violates clear legal boundaries to acquire a competitive advantage.[11]

The Crater of EE

EE can have a major impact on the international community in a myriad of ways. In the most immediate sense, Chinese counterfeiting of legitimate goods hurts the companies who own those intellectual properties. When Chinese demand for those legitimate properties

9. Carlton, "Industrial Espionage," 20.

10. Andrew Crane, "In the Company of Spies: When Competitive Intelligence Gathering Becomes Industrial Espionage," *Business Horizons* 48, no. 3 (2005): 233-234.

11. Crescenzi and Snyder, "Intellectual Capital and Economic Espionage," 246.

is satisfied internally with counterfeit goods, those companies lose substantial potential profits. However, that illegally satisfied demand is not confined to China. Chinese counterfeits and pirated materials are consumed globally, illegitimately satisfying an international demand and stealing the profits from the legitimate supplier. [12]As profits decline, companies are less able to employ the citizens of their host country. This was the case of Solarworld, which had to shut down one of its plants in response to Chinese competitors acquiring its IP through EE then flooding the markets with cheaper versions of their product.[13] EE has a direct effect on the companies from which IP is illegally seized.

Regarding international effects, a major trade deficit currently exists between China and the US. Many argue that the mass consumption of counterfeit goods by the Chinese population satiates the demand that would otherwise legitimately be supplied by the US. In other words, the trade deficit could be greatly assuaged if China purchased legitimate goods from its trading partners, rather than counterfeiting the products domestically.[14] Not only are trade deficits a major source of ire for the host countries of targeted industries, but by the very nature of EE the victimized company ultimately loses a productive and competitive asset.[15] For countries like the US, who derive an increasing percentage of their GDP from companies whose competitiveness and strength are substantially based on intellectual properties, EE can be potentially devastating to domestic economies, altering the international (economic) power balance.[16] In 2013, the United States reported $300 billion in lost profit from Chinese IP theft, claiming that 80% of the total IP theft from US firms originated in China.[17] EE may seem as trivial is an off-brand handbag, but its cumulative effects can be internationally shattering.

---

12. Omario Kanji, "Paper Dragon: Inadequate Protection of Intellectual Property Rights in China," *Michigan Journal of International Law* 27, no. 4 (2006): 1266.

13. "U.S. Filed Economic Espionage Charges Against Chinese Military Hackers." *CBS,* May 18, 2014, accessed October 16, 2014, http://www.cbsnews.com/news/u-s-government-files-economic-espionage-charges-against-chinese-hack

14. Kanji, "Paper Dragon," 1264.

15. Crescenzi and Snyder, "Intellectual Capital and Economic Espionage," 252.

16. Jeffrey S. McIllwain, "Intellectual Property Theft and Organized Crime: The Case of Film Piracy," *Trends in Organized Crime* 8, no. 4 (2005): 16.

17. Andreas Schotter and Mary Teagarden, "Protecting Intellectual Property in China," *MIT Sloan Management Review* 55, no. 4 (2014): 41.

The Motivation to Spy

Before delving into the specific methods and practices of China's EE, we first need to understand why China would engage in such a globally harmful practice. What is it about China that motivates them to so rampantly engage in EE? First and foremost, China is extremely unsatisfied with its current economic position: an international supply of cheap manual labor and rampant industrialism.[18] The population issues, suicides (associated with working conditions and low quality of life), and the debilitating pollution have pushed China to make a drastic course correction regarding its economic place in the world. China is attempting to solidify itself as an international technological powerhouse and leader in technology by investing heavily in its State-Owned Enterprises (SOEs).[19] It hopes to achieve this in part by drastically reducing its dependence on foreign technologies by replacing foreign supply with domestic supply (making foreign technology into Chinese technology).[20] Of course, there is no better way to replace foreign technologies than to replicate them. And there is no faster, and more efficient, way to replicate these technologies than to seize them (EE). The Chinese hope that by stealing Western intellectual properties and innovations and injecting them with state funding via their SOEs, they can eliminate the West's primary advantage of IP holdings.[21]

The desire (and methodology) to acquire Western intellectual properties and use them in SOEs is only part of the picture. The obvious question is "why does China not simply come up with its own popular inventions?" There are a number of factors at play that prevent the Chinese from doing exactly this sort of innovation which has led to so much strength and success in the West. Chinese society places a far greater emphasis on "practical utility" than the vital type of abstract thinking critical to the innovative process.

The majority of China's educational system is focused on a standardized exam taken in high-school (高考), the results of which

18. Adam Segal, "The Code Not Taken: China, the United States, and the Future of Cyber Espionage," *Bulletin of the Atomic Scientists* 69, no. 5 (2013): 40.

19. Schotter and Teagarden, "Protecting Intellectual Property in China," 42.

20. Schotter and Teagarden, "Protecting Intellectual Property in China," 42.

21. William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Asian Security Studies : Chinese Industrial Espionage : Technology Acquisition and Military Modernisation,* Kentucky: Routledge, 2013, 241.

determine a student's college and academic major. Starting in high school, the curriculum almost exclusively stresses rote memorization in preparation for this exam (over the creative and analytical thinking stressed in Western education systems). This pattern begins as early as Kindergarten, where one student describes how her teacher scolded a student for drawing the sun slightly different than other students. Adhering to common standards, thinking inside the box, rote memorization, and a lack of exploration are the hallmarks of the Chinese education system.[22] Far more value is placed on concrete achievements and results than paradigm shifts and unique perspectives.[23] This is a major motivator behind the Chinese push to send its students to Western schools and universities, with the hopes that they will return and bring with them the kind of Western creative and analytical thinking that produce the valuable innovation China so desperately needs.

This aversion to creative, abstract thinking is reflected in neuropsychological comparisons of Westerners and Chinese populations. Studies show that not only do Westerners view things substantially more holistically than the far more analytical than their Chinese counterparts, but that there may in fact be a genetic predisposition for narrower thinking and a cognitive conformity bias in Chinese people (as opposed to Western genetic predispositions to the opposite). Without individualism, creativity is unlikely to flourish. This issue of creativity may be linked to the Chinese language, which maps ideas onto specific characters and words. This is significantly different than Western languages, which stress a seemingly unending number combination of syllables and letters. This Western style of speech and writing is far more conducive to abstract expression and creativity than the limited and rigorously structured system of Chinese communication.[24]

Whatever the cause for this lack of domestic innovation may be, the bottom line is that economic growth is not moving fast enough without it. It seems that China is resorting to the fastest methods of competitive-asset-acquisition possible (a trend reflected in increased activity of EE originating from China). By seizing intellectual properties through EE as rapidly as possible, particularly in the technology and manufacturing sector, China hopes to take as many shortcuts as possible to modernize

22. Yajian Zhao, interview by author, Dallas, TX, November 24, 2014.

23. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 239.

24. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 240.

its economy and catch up with the West.[25] "If you can steal rather than innovate, you save years."[26]

Types of EE: A Litany of Chinese Activity

Chinese pirated goods constitute a roughly $20 billion industry, securing China's position as "one of the world's largest producers of counterfeit goods."[27] US Customs and Border patrols seize more counterfeits produced in China than from any other country, with Chinese counterfeits alone making up 53% of all seizures in 2010. The practice is so rampant than an estimated 15-20% of all products made in China are counterfeits (8% of China's total GDP).[28]

EE is one type of transnational crime, but there are many types of EE to exploit the many types of IP. These intellectual properties can be copyrights, trademarks, patents, or trade secrets, and the theft of any of these by a foreign government constitutes EE.[29] Following an examination of Chinese theft of these properties, we will proceed to a more general overview of the methods the Chinese government employs to execute these seizures

Copyrights

A copyright is any "original work of authorship," the ownership of which translates to the exclusive rights to "reproduce, distribute, and publicly display or perform the copyrighted work, as well as to prepare derivative pieces based on the original copyrighted work."[30,31] The majority of the street-level Chinese EE is copyright theft, with the largest copyright market being movies and software.

The Motion Picture Association recognizes multiple methods of film piracy, ranging from optical disc piracy (termed "hard goods") to internet film piracy ("soft goods), and the full realm of possible piracy

25. Segal, "The Code Not Taken," 39-40.

26. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 187.

27. Kanji, "Paper Dragon," 1264.

28. Edward I. Chen, "U.S.-China Trade Relations and Economic Distrust," *The Chinese Economy* 47, no. 3 (2014): 58.

29. McIllwain, "Intellectual Property Theft and Organized Crime," 16.

30. Haiyan Liu, "The Criminal Enforcement of Intellectual Property Rights in China: Recent Developments and Implications," *Asian Criminology* 5, no. 2 (2010): 138.

31. Liu, "The Criminal Enforcement of Intellectual Property Rights in China," 138.

in between.[32] 85-90% of all media sold in China is pirated, resulting in losses exceeding $2.5 billion to the authors of the copyright. The factories producing the optical discs used as a medium of pirated copyright sale are all licensed by the Chinese government and operated in close cooperation with the street vendors selling the pirated copies.[33] Chinese Triad groups derive a substantial portion of their profits from the transnational sale of these pirated films.[34] This rampant film piracy comes as no surprise, however, given that current World Trade Organization (WTO) terms only allow 20 foreign films to be legally imported into China every year.[35] This digital piracy is not limited to films, however, as the optical disc factories also support the piracy of computer software, with pirated software constituting roughly 78% of all software sold in China (losses of $7.8 billion to the copyright authors).[36]

Trademarks

A trademark, another type of IP targeted by EE, is "any symbol, word, name, device, or combination used to identify products, services, or their producers in order for consumers to distinguish their sources."[37] Unlike other intellectual properties, which require relatively great effort to acquire, trademarks are the easiest IP to acquire and exploit. Street vendors and illicit markets are lined with counterfeited products all bearing famous trademarks like "Nike" and "Apple," many of which may have come from those companies' actual factories. In China, given that trademarks are published and so widely available and advertised, it would seem like trademark theft is a victimless crime. The trademark, however, is a carefully cultivated symbol of quality and brand identity. The company holding that trademark invested vast resources into cultivating that trademark. As such, it is a valuable commodity that can offer a market advantage over competitors. In the the Beijing Silk Market, a prime example of trademark theft, Chinese counterfeiters produce purses, wallets, scarves, and other visually similar/identical products to their designer counterparts, then sell them for drastically

32. McIllwain, "Intellectual Property Theft and Organized Crime," 18-21.

33. Kanji, "Paper Dragon," 1265.

34. McIllwain, "Intellectual Property Theft and Organized Crime," 19

35. Kanji, "Paper Dragon," 1265.

36. Chen, "U.S.-China Trade Relations and Economic Distrust," 58-59.

37. Liu, "The Criminal Enforcement of Intellectual Property Rights in China," 138.

reduced prices than their counterparts. While the consumer may be well aware that it is a counterfeit, their demand is largely driven by the trademark designer logos.

Patents

Patents are another type of IP, and they introduce a lethal element to EE. A patent is any protected "product, process, composition of matter, or improvement."[38] Patent theft feeds two major counterfeit markets: pharmaceuticals and automobile/aircraft parts. Considering the pharmaceutical market, Chinese counterfeits account for 30% of global counterfeit/unofficial pharmaceuticals. While some of the pharmaceuticals counterfeited in Chinese markets are morally negligible (a placebo Viagra is not going to kill you), Chinese counterfeit pharmaceuticals accounted for roughly 200,000 deaths in China in 2001.[39] Unlike counterfeit scarves or movies, consumers of counterfeit pharmaceuticals often need the genuine products to survive. As these counterfeits have no regulation or testing, there is nothing stopping counterfeiters from selling rat poison as aspirin, or powdered sugar as diabetes medicine.

Not only do counterfeit pharmaceuticals raise serious public health questions from Chinese EE, but so do counterfeit automobile and aircraft parts. China often reverse-engineers these parts domestically: a practice costing the automobile industry $12 billion annually. Similarly with the danger of counterfeit pharmaceuticals, there is no channels of regulation or testing of counterfeit automobile parts, and consumers sometimes find that their black market brake pads are, in fact, filled with grass or sawdust. In 1989, a Norwegian airline crashed as a result of faulty equipment—which was later discovered to be counterfeited—and this was not the first time. With an estimated 2% of the aircraft parts sold annually believed to be counterfeit and China being the US's 5th largest supplier of aircraft parts, the issue of counterfeits and IP theft is very much a matter of life and death.[40]

Trade Secrets

The final type of IP targeted by EE is also the most broad: trade secrets. Trade secrets are widely defined as anything with "independent

38. Liu, "The Criminal Enforcement of Intellectual Property Rights in China," 139.

39. Kanji, "Paper Dragon," 1267-1268.

40. Kanji, "Paper Dragon," 1266-1267.

economic value" that companies keep secret, covering a wide range of intellectual properties and assets that confer a substantial market advantage.[41] Trade secrets can include client databases, general business practices, trade agreement (both actual and planned), and anything else that a company derives value from that it protects as secret. One particular target of Chinese EE has been information on negotiations of business and political firms. Often operating as reporters, Chinese hackers commonly target negotiation tactics and plans of major corporations in an effort to exploit their strategies in future negotiations and business deals. Chinese spies have also attacked institutions that are known to influence both political and economic policy regarding China.[42] For every type of IP, there is a niche of Chinese EE to target and exploit it.

41. Liu, "The Criminal Enforcement of Intellectual Property Rights in China," 139.

42. Segal, "The Code Not Taken," 38-41.

Table 1 – IP Categorization

Type of IP	Definition[43]	Examples	IPC
Copyright	*Any original work of authorship*	*- Movies* *- Software*	*The majority of small-scale IPC is the sale of counterfeit DVDs and software*
Trademark	*Any symbol, word, name, device, or combination used to identify products, services, or their producers in order for consumers to distinguish their sources*	*- Apple's apple* *- Nike's swoosh* *- Louis Vuitton's LV* *- Burberry's tartan*	*Production of counterfeit products bearing a trademark, either as a knockoff (low-quality) or super-copy (virtually indistinguishable from original)*
Patent	*Any protected product, process, composition of matter, or improvement*	*- Pharmaceuticals* *- Aircraft parts* *- Automobile parts*	*Production of counterfeit pharmaceuticals and automobile/ aircraft parts of drastically varying quality*
Trade Secret	*Anything with independent economic value that companies keep secret*	*- Client databases* *- Business practices* *- Negotiation tactics*	*Chinese hackers routinely target and exploit negotiation strategies and potential business deals and contracts*

Tools of the Trade

While it is clear that China is after IP, their methodology is not so apparent. Not all EE is conducted through cyber attacks, and there is no black market warehouse off the coast of coast of Hong Kong where Chinese officials can fill moneybags with documents. There is an ideology and a methodology behind Chinese EE, and understanding of the big picture is critical to understanding China's full role in all of its IP activities.

"Buckets of Sand"

The initial school of thought examining Chinese espionage activities assumed that China took an approach referred to as the "thousand grains of sand." This assumption held that while other nations conducted espionage by sneaking "onto the beach" under cover of darkness and scooping up buckets of "sand" (IP and associated data) for later analysis, the Chinese instead brought thousands of its citizens to the beach in broad daylight. Instead of scooping up buckets and sand and sneaking off with them for later analysis, the Chinese would simply roll up their towels after a day of sunbathing and return home. When they did, they would shake out their towels, resulting in thousands of grains of sand from *all over the beach*, resulting in far more knowledge than any covert buckets ever would. The general assumption with this school of thought would be that China was deploying hundreds of thousands of citizens to the United States and other Western countries, with each citizen gathering a small piece (or "grain") of information (seemingly harmlessly so) that would contribute to a vast "sand pile" when they returned to China (and "shook out the towel"). Not only did this approach steal the same about of sand in broad daylight, but it gather a far broader sample of sand, thus providing a better picture of the "beach." This approach implied a general lack of intent, rather focusing on random selection, seeing every Chinese citizen abroad as an asset.[43]

While this approach fits with the widespread distribution of Chinese citizens in technological and manufacturing firms abroad, it ultimately neglected the intelligence-driven aspect of Chinese EE we have observed. For example, Dongfang Chung, who was charged with taking the trade secrets he had learned from his employment at Boeing and providing them to China, was in fact tasked by China ahead of time to collect these trade secrets; he did not just haphazardly shake out his towel from his trip to Boeing beach on China's doorstep. In the case of Chi Mak (another Chinese economic spy convicted of attempted IP theft) documents were found in his home that showed China's direct instruction to immerse himself in certain areas of expertise and return that knowledge for the Chinese government. China does not just solicit its citizens with a general request to return home with IP, it actively

43. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 188-192.

seeks out anyone who may be a valuable asset and directs them to conduct EE.[44]

Institutions

The Chinese government accomplishes this EE utilizing a number of methodologies, the first of which is institutions. China maintains roughly one hundred various institutions with a collective aim of acquiring foreign IP and returning it to China through a variety of means. The first of these such institutions are the Foreign Talent Recruitment Offices, which maintain databases of individuals who may be exploitable to some degree for IP seizure. One such office, the State Administration for Foreign Experts Affairs (SAFEA), exports native talent and imports foreign talent for the purposes of foreign IP collection. The focus of these efforts is not to increase China's understanding of science and technology or bring new creativity and ways of thinking (as is the case with sending Chinese students to universities abroad), but the direct acquisition of practical results and technologies. One of these recruitment offices reached out to US citizens Noshir Gowadia, a former employee of Northrop Grumman, and brought him to China to provide his knowledge of intellectual properties regarding military technologies. These programs and offices specialize in seeking out these foreign and domestic experts and deploying/collecting them to serve as EE agents.[45]

Another example of one of these institutions is the Ministry of Science and Technology (MOST), which is dedicated to increasing China's scientific and technological resources and investments, specifically via the transfer for foreign technology to China. They accomplish this through the hundreds of Technology Transfer Centers located throughout China, such as the Shanghai new High Technology Service Center, whose mission it is to convert acquired foreign "technologies" into Chinese technologies, often via recreation.[46]

The Ministry of Education is another such institution furthering the Chinese practice of EE, though not nearly as directly as SAFEA or MOST. The Ministry operates programs such as "Spring Light," which offers substantial bonuses and incentive programs to Chinese citizens

44. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 191-198.

45. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 79-83.

46. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 85-94.

employed in the science, technology, engineering, and mathematics sectors to return to China and "render services to the country."[47] Through these various institutions, China directly conducts EE through its careful management of human resources, expertise, and IP acquisition.

Blackmail

A second method the Chinese use to conduct EE is blackmail. Chinese officials will often target experts in a certain field or employees they know will possess a critical degree of IP and blackmail them in order to force them to surrender said expertise or property. A common tactic employed by the Chinese is the "honey trap," in which Chinese officials will directly trick targeted individuals into engaging in affairs and other illicit activities while being recorded. Officials then threaten to expose the individuals unless they help the Chinese government. This was the case with US citizen Gregg Bergersen, whom the Chinese government threatened with the exposition of his affair and gambling problem. Often Chinese officials will employ or recruit prostitutes in Western hotels in China to trap these targets, or just have the prostitutes drug the targets then go through their things. Surveillance isn't difficult, as it is not unusual for hotel rooms to be thoroughly bugged.[48]

Bribery

Beyond elaborate schemes like honey traps, Chinese officials are not above bribery (as was the case with US citizens Glenn Duffie Shriver, whom the Chinese paid to be a mole at the CIA or department of state).[49] Where bribery isn't necessary, officials will often appeal to the nationalism of US-employed Chinese citizens and their families, who often have ties to parts of companies full of invaluable trade secrets.[50]

Deception & Disguise

Targets do not always know when they are being targeted. Chinese officials can approach targets under the auspices of professors or admirers and ask seemingly harmless questions, as was the case with Peter Lee.

---

47. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 86.

48. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 202.

49. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 199.

50. Souvik Saha, "CFIUS Now Made in China: Dueling National Security Review Frameworks as a Countermeasure to Economic Espionage in the Age of Globalization," *Northwestern Journal of International Law & Business* 33, no. 1 (2012): 207.

In 1985, Lee was approached by a man claiming to be from the Chinese Academy of Engineering Physics, lamenting over how few resources his department had and how difficult it was for him to conduct research. Lee opened up to the man about his research on nuclear detonation simulations without even realizing what he was doing, leaving no trace of espionage.[51] In other instances, officials can pose as employees or actually take positions at companies with the sole intent of infiltrating social networks and exploiting "co-workers" without them having any idea. Once these officials get the information they want, they publish it and completely disappear, destroying the competitive value of the information before the company has any idea it was stolen.[52]

Cyber

These methods of deception and disguise are especially prevalent in the last Chinese method of EE: cyber espionage. Cyber espionage confers the unique advantages of increased anonymity, remote access, and reduced costs (no need to maintain a network of spies and handlers, just a single hacker).[53] Cyber EE attacks are unique in that they can occur both internally (as is required with the aforementioned methods) and externally. Internal examples usually involve an insider gaining access to an electronic database containing IP and copying the information onto a removable storage device or remote server (as was the case with David Lee and Valspar paints in 2008, Meng Hong and DuPont Chemicals's OLEDs in 2009, and Xiangdong Yu and 4,000 of Ford Motors's documents in 2009).[54]

Remote cyber attacks are a growing trend in Chinese cyber EE. The most publicized of these attacks was the January 2010 attack on Google (and about twenty others), which resulted in the theft of numerous intellectual properties to which Google attributed significant economic advantage.[55] Security firms like McAfee have reported thousands of computers and networks of major oil, gas, petrochemical, and infrastructural companies infected by Chinese actors.[56] These

51. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 193-194.

52. Carlton, "Industrial Espiaonage," 19.

53. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 219.

54. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 221.

55. Segal, "The Code Not Taken," 41.

56. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 221.

attacks often originate using the same principles of deception in previous methods. Often a hacker will access the employee database of a company and pick one member of a department. The hacker will then create an email address using that member's name (i.e. "smith@rmaill.com") and send a "phishing" email, which contains a seemingly innocuous invitation to click some link or open some program. That program (often a disguised executable program file), when opened, will then give the hacker access to the member's computer, and potentially the company's entire network of IP.[57] These operations are often highly unsophisticated and sloppy, but are incredibly effective to the untrained and curious.[58] Cyber espionage is a growing threat to companies given its anonymity, ease, and potential destruction.

57. *APT1: Exposing One of China's Cyber Espionage Units*. Washington D.C.: Mandiant, 2013. Accessed October 18, 2014. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, 28-31.

58. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 227.

Table 2 – Chinese IPC Methods

Method	Use	Examples
Institutions	*Utilizing existing government institutions to support the exploitation of foreign IP*	*- SAFEA* *- MOST* *- MOE*
Blackmail	*Obtaining damaging information about foreigners and using the potential disclosure of that information as leverage to reveal secreted IP or open vulnerabilities to attack and exploitation*	*- Filming foreigners with prostitutes*
Deception/ Disguise	*Purposely concealing identity/intent in order to trick foreigners into revealing secreted IP or open vulnerabilities to attack and exploitation*	*- Pretending to be a professor to disarm foreigners into revealing research*
Cyber Attack	*Remote computer-based attacks designed to infiltrate foreign computer networks with the intent to gather IP or harm those networks*	*- Phishing emails with malware links* *- PLA Unit 61398*

Why EE is so Hard to Stop

EE is unlike other transnational crimes in both the scope and nature of the attacker and the stolen property. We will be begin with an examination how IP makes EE so hard to stop, and then turn to the specific Chinese impediments to stamping out EE.

Intangible IP

Arguably the biggest difficulty with combatting IP theft is the nature of IP itself. Unlike other properties, such as physical money or a piece of art, IP is intangible information. As such, it can be copied an unlimited

amount of times, often without the owner ever knowing.[59] For example, logging onto your boss's computer and copying the file containing the secret recipe to the company's best-selling product can be done in a matter of seconds, and it leaves virtually no indication that a copy was ever made. Even beyond digital copying and information theft, the very nature of information makes it incredibly easy to steal; once an individual possesses the information, that individual theoretically can never give it back. Once that information is out in the open, it can't be reclaimed.[60] This was the case with Lucent Technologies: Once the FBI moved on three Chinese citizens suspected of stealing information to sell to PathStar, a Chinese company, they had already sent the information off, and it could never be retrieved without PathStar having it.[61]

Anonymity

Anonymity is another major hurdle in stopping IP theft. As is especially the case with cyber EE, the attacker can almost completely hide their trail.[62] If your company's servers are hit by a Chinese attacker and millions in IP are stolen, but you don't even know the identity of the hacker, you don't even have the name of someone to extradite to try to build a case against. Remote access has amplified the benefits of anonymity to hackers, particularly across international borders.[63] Attackers therefore have a huge advantage, as its incredibly easy for them to get in and out of a company's network, but relatively impossible to track them, especially if the investigation is after the fact.[64] Usually these attacks occur so quickly that by the time we even realize something is gone, the IP is already being put to use elsewhere.

Technological Innovation

While EE may not be new to companies, the contemporary methods certainly are. With the ever-advancing evolution of technology, the development of new methods to infiltrate and exploit companies is

59. Crescenzi and Snyder. "Intellectual Capital and Economic Espionage," 249-250.

60. Crescenzi and Snyder. "Intellectual Capital and Economic Espionage," 250.

61. Susan W. Brenner, and Anthony C. Crescenzi, "State-Sponsored Crime: The Futility of the Economic Espionage Act," *Houston Journal of International Law* 28, no. 2 (2006): 408.

62. Segal, "The Code Not Taken," 41.

63. Crescenzi and Snyder. "Intellectual Capital and Economic Espionage," 247-248.

64. Segal, "The Code Not Taken," 41.

evolving beyond the capacity of those companies to deal with the threat.[65] Especially when that development is funded by a state like China, the pace of development simply obliterates any potential escalated response by companies. Further hindering IP protection, companies stand a far better chance defending themselves than relying on legislation, as the law is far slower than business in catching up with new technologies.[66] The pace of technology is simply too fast, especially with state funding, for either individual companies or the law to keep up.

Chinese Legislative Ineptitude

Beyond the inherent difficulties of blocking EE, China's legislative system creates nightmares for foreign firms. Despite its strong SOE-focused agenda and its engagement in EE, China does possess and (to some extent) uphold anti-EE legislation. The most up-front obstacle to eradicating EE and IP theft in China is its lack of transparency, making any substantial or informed criticisms into China's legislative process extremely difficult.[67] This is no surprise given that the majority of China's IP legislation was basically transplanted from the West without much consideration for existing Chinese infrastructure or society. As such, there is a dire lack of societal willingness and administrative support to enforce any actual violation of IP rights or conduct of EE.[68]

Looking more closely at the legislation in place, what exists is fraught with problems. The Chinese Trademark Law does not even consider most IP theft to be a crime; copyright and patent infringements are not regarded as criminal offenses. Article 59 of the Law differentiates between trademark infringement and crimes, referring to instances in which "the case is so serious *as to constitute a crime."*[69] In other words, IP theft is only a crime when it is serious, and then really only when it is a trademark. None of this is helped by the fact that the seriousness of these infringements (the measures of whether or not they are crimes) are based off of profit: If the offender profits less than $6,000 from the infringement, it is not a crime.[70] This stipulation allowing those who show less than $6,000 in profit from IP theft reflects the general attitude

65. Crescenzi and Snyder. "Intellectual Capital and Economic Espionage," 247.
66. Crane, "In the Company of Spies," 138.
67. Kanji, "Paper Dragon," 1272.
68. Liu, "The Criminal Enforcement of Intellectual Property Rights in China," 142.
69. Kanji, "Paper Dragon," 1275.
70. Kanji, "Paper Dragon," 1274-1275.

that IP theft is not even a crime.

For those whose IP thefts are serious enough to constitute criminal activity, the trial process further aids them in resuming their illicit practices. Most of the judicial personnel in China's legal system are not educated enough to deal with the often complex and technical cases of IP theft, so they can be thrown out or tried without any comprehensive understanding of the facts of the case.[71] For those who are actually sentenced, the penalty is rarely more than three years in prison, with more lenient sentences for individuals (over companies) and strict restrictions on how much these thieves can be fined.[72] While China does, in fact, have legislative measures to hide behind when accused of allowing IP theft, they are totally ineffective and reflect a society that totally disagrees with and refuses to support them.

Denial

As if this weren't enough evidence of China's engagement in and support of EE, their responses to accusations of EE border on melodramatic, with officials often nearly indicting themselves in their grand counter-accusations and outright denials of anything ever having to do with EE. The general policy of the government in response to these accusations is threefold: "Admit nothing, Deny everything, Make vigorous counter-accusations."[73] When anyone accuses the Chinese government of such activity, they denounce those accusations as "irresponsible speculation without a shred of evidence," insist that they have never engaged in anything remotely related to "cybertheft of trade secrets," then accuse the US of EE, claiming to have "mountains of data" against us.[74, 75, 76] The overly-dramatic denials and swift counter-accusations indicate an overly-defensive response, suggesting guilt. These denials prove nothing, while over-the-top denials raise suspicion.

71. Liu, "The Criminal Enforcement of Intellectual Property Rights in China," 153.
72. Kanji, "Paper Dragon," 1273-1275.
73. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 225.
74. Hannas, Mulvenon, and Puglisi. *Asian Security Studies,* 225.
75. "U.S. Filed Economic Espionage Charges Against Chinese Military Hackers."
76. Segal, "The Code Not Taken," 41.

Table 3 – Barriers to Stopping EE in China

Barrier	Explanation
Nature of IP	*- IP is not a physical entity that can be guarded and kept, but is rather intangible, infinitely replicable, and nearly impossible to "get back."* *- Globalization has made international IP more and more available and vulnerable*
Anonymity	*- Chinese Cyber attacks are notoriously difficult to track and prosecute*
Technological Innovation	*- Technology is evolving too quickly for foreign firms to adapt to China's technological evolution and dynamism*
Legislative Ineptitude	*- Judges and courts are unable to comprehend or deal with IPC* *- Punitive measures against IPCs are insufficient deterrents*
Denial	*- China refuses to acknowledge or discuss their involvement in EE*

So How Messy Does China Get?

Having detailed the state of EE and China's activities therein, we are presented with some conflicting data. On the one hand, we have a country desperate to strengthen its SOEs in pursuit of international strength, with repeated instances of EE and overly-suspicious denials of such activity. On the other hand, China does maintain legislation against IP theft, which it does sometimes enforce, and the instances of EE for which we have evidence only make up a portion of the counterfeit market. Given the evidence for and against China's involvement in EE and theft of foreign IP, how messy do China's hands really get?

The overall picture of Chinese activity in this field of transnational crime points to a gradient of Chinese involvement, proportional to the scale and industry of the crime. For small-scale IP infringements (movies and scarves) that primarily benefit local communities, Chinese involvement is distant but supportive (a sort of IE supported, but not directed, by China). For large-scale IP violations targeting major foreign corporations and military equipment, Chinese involvement is full-scale EE, with the Chinese government not only directing, but running the operation.

Large-Scale IPC – Chinese EE

We begin with the obvious latter – the clear-cut, no-questions examples of Chinese EE. The general trend observed with these instances is the scope and content: anything large-scale or applicable to the military demonstrates pretty damning evidence against China. These cases are almost all conducted by the People's Liberation Army (PLA) in the cyber EE realm. The PLA's cyber commander is under the full control and has access to the full resources of the Chinese Communist Party, which, unlike in the US, calls the shots of the entire country.[77]

According to reports by security firms, there are more than twenty Advanced, Persistent Threat (APT) groups operating under Chinese support and funding.[78] The report finds ample data suggesting that the most prominent of these groups, APT1, is actually PLA Unit 61398, a cyber espionage unit. Two of APT1's four networks are housed in PLA compounds, which are believed to be the compounds of 61398.[79] Moving down the list of evidence, any searches on Chinese government networks for "61398" yield absolutely no results, pointing strongly to government efforts to keep the unit's operations a secret. If the unit truly didn't exist, the government would have no reason to erase all entries on the government network and some of the speculation regarding the network would show up. Seized memos from the network supplier of the supposed 61398 compound, China Telecom, reveal that the facilities are outfitted with unusually state-of-the-art fiber optic networks and other features commonly associated with national defense. According to Li Bingbing, a claimed former operative of 61398, has confirmed that the personnel classification requirements for assignment to 61398 include expertise in operating systems, digital signals, network security, covert communications, and the English language, all in fitting with the operations of APT1.[80]

The vast majority of APT1's data were stolen from the United States, with over 100TB from American firms. The type of data included product development specifications, systems designs, products manuals, trade agreements, business strategies, and partnership details

77. *APT1: Exposing One of China's Cyber Espionage Units*, 7.

78. Lee, "Cyber Kleptomaniacs," 74.

79. Lee, "Cyber Kleptomaniacs," 74.

80. *APT1: Exposing One of China's Cyber Espionage Units*, 7-16.

– a smorgasbord of IP.[81] While it's not clear as to everything APT1 has stolen, as the degree of anonymity is heightened by the fact that most of these attacks occurred after the report began its investigation, the parallels between APT1 and 61398 suggest beyond a reasonable doubt that the two are one in the same.[82] Beyond the 61398 example (arguably the most publicized example), the catalog of cases against agents of Chinese EE in seizure of missile schematics, jet blueprints, naval ship development plans, and other military and advanced technologies is endless.[83] With such strong evidence convicting China is EE aimed at military and advanced technologies, we move to the other areas of EE to get to the puzzle of the extent of Chinese involvement.

Small-Scale IPC – Chinese-Supported IE

Given the clear involvement of the Chinese government in EE targeting military technologies and other intellectual properties aimed at major corporations (such as energy and high technology), what exactly is the Chinese government's involvement in other areas of EE? Areas of IP theft and EE on a smaller scale (in terms of contribution to China's strength, as opposed to military and advanced technological might), include the Beijing Silk Markets (trademark/patent theft) and film piracy (copyright theft). In the case of these smaller-scale markets, the involvement of the Chinese government is far less evident. We don't have examples of Chinese officials approaching movie editors in hotels to blackmail them, or bribing fashion designers with millions to learn how the new Hermes scarves are made, yet those markets still exist and thrive in China. Ultimately, the following factors point to Chinese support of these small-scale IPCs.

China cannot/does not produce it's own IP

As is mentioned above, an examination of Chinese culture indicates that the Chinese population places far greater value on conformity and copying at critical developmental stages, hampering creative thinking and the critical innovative "outside-the-box" thinking required for IP generation. While this trend in thinking is likely decreasing with increase youth exposure to a greater variety of culture and ways of looking at the world (an effort bolstered by China's push to send its students abroad), they have not had the luxury of such creativity that results in

81. Lee, "Cyber Kleptomaniacs," 74-75.

82. *APT1: Exposing One of China's Cyber Espionage Units*, 25.

83. Segal, "The Code Not Taken," 38.

monumentally profitable IP in the past few decades. This creative deficit leaves China with no other option but to "emulate" such innovation, by legal and illegal means, to salvage itself from being a third-world factory.

IPC is the cheapest, easiest, and most harmless way to hurt foreign competition

Relatively speaking, small-scale IPC is incredibly cheap. In the realm of DVD piracy, the costs and risks are low, while the profits are high. Getting into the film piracy business is easier than getting into any legitimate business. With the global availability of technology in the modern world, virtually anybody can purchase a $100 DVD burner and a computer with internet access and, within an hour or two, have the means to set up a modest pirated film production line. With the movie companies themselves doing the advertising for the product, all a film pirate has to do is obtain a copy of the movie itself, which is remarkably easy given the simplicity of internet torrenting sites and DVD copiers. RAND illustrates the absurdly high profit margins by comparing the cost of a CD ($0.35) with the average selling price of that CD containing a pirated movie ($3.50). The profit margins of upwards of 1,000% of initial investment are criminally high. If the low entry costs and high profits weren't enough, the risks of engaging in film piracy are an even bigger selling point for entry into film piracy. In the US, for example, first-time film pirates usually receive probation as a reprimand, with prison sentencing rare. In France, film piracy punishments pale in comparison to other illicit activities such as drug sales, with prison sentences as low as 2 years (compared to drugs' 10 years) and fines as low as $150,000 (compared to drugs' $7.5 million).[84] RAND's examination of the factors promoting entry into the film piracy business are not only simple, logical, and compelling, but backed with real-world data illustrating the ease of this IPC industry.

IPC supports local communities

Looking to legislative evidence for EE in these markets, "companies recognized as good citizens may enjoy favorable treatment in IP protection enforcement."[85] In other words, foreigners who complain that counterfeiters are stealing their IP are, in theory, less likely to

84. Gregory F. Treverton, et al, "Film Piracy, Organized Crime, and Terrorism," *RAND Corporation* (2009): 27-30.

85. Schotter and Teagarden, "Protecting Intellectual Property in China," 44.

receive support than someone who goes to the government and says that their business is less able to help the local community because of local counterfeiting operations.[86] It would seem that the Chinese government is willing to allow IP theft, only so long as it doesn't harm the community (and to a greater extent, China). Smaller-scale IPCs bring profits and tourism to the communities perpetrating the IPCs. To the Chinese government, that is a valuable source of international revenue and bolsters the local community. As such, China has little incentive to destroy (rather it has the incentive to support) small-scale IPCs that bolster their communities.

China own many of the factories that produce products of IPC

Some evidence does point to Chinese involvement in these smaller-scale markets. Beyond their blatantly ineffective legislation, one example is Chinese ownership of many of the factories that manufacture the pirated optical discs used for movies and software. What exactly constitutes ownership and the extent of the manufacturing is unclear. A major hit against China is that what counterfeit goods they do seize in their crackdowns against IP theft are later auctioned off, and the destination of those profits is unknown. While China has a point in its assertion that destroying the counterfeit goods would be wanton destruction of valuable resources, the secrecy surrounding the destination of the profits of these goods raises justified suspicion against the government.[87] To further explore this factor, more information is needed regarding the relationship between the owners of these factories and their knowledge/complicity of the goings-on in terms of IPC operations.

China has not taken effective measures against perpetrators of IPCs

While China has adopted some measures against IPC, enforcement and effectiveness is weak at best. Not only are IPC perpetrators rarely sought out by Chinese authorities, but the mechanisms in place to deal with those perpetrators are inadequate. The judges that hear the majority of these cases have little to no understanding of the actual crimes being considered and the sentences levied against these criminals are hardly a deterrent (when they're levied at all).

86. Schotter and Teagarden, "Protecting Intellectual Property in China," 45.

87. Kanji, "Paper Dragon," 1278.

There is also evidence that points to China's condemnation of IP theft in these markets. Regarding legislation, for instance, ineffective practices may suggest a desire by the government for legislation to fail, but that is not a certainty. There have actually been numerous instances of government crackdowns on these markets. In November of 2002, the government shut down a number of counterfeit pharmaceutical companies (though that may have been due to the harm the pharmaceuticals were doing), the government did shut down the Beijing Silk Market (though a new market opened up practically the next day).[88] As of July 2013, the US and China have officially entered into a "US-China cyber security working group," with Beijing signaling its willingness to apply international legal principles to the internet.[89]

Based on the above factors, however, it is plausible to conclude that China is at the very least complicit in the range of IPCs conducted within its borders. Their direct involvement in EE through the activities of PLA Unit 61398 signal their willingness to rely on IP theft as a means to their end. Had China the ability to generate its own IP, it certainly would, but a lack of such generation, and evidence against such generation, indicate that China may only look outward for IP and innovation. The Chinese educational system is so focused on rote memorization and conformity towards test preparation that an individual's childhood and adolescent education are practically devoid of creative and analytical thinking. This lack of development critically hinders the Chinese population from the type of IP development generated in the West.

IPC on a smaller-scale is not only an incredibly cheap and easy way to undercut competition and bring in foreign revenue, but it does so with a degree of anonymity that keeps China relatively insulated from international reprisals. Given the benefits that IPC revenue brings local communities and the high likelihood of local factory collaboration in IPC endeavors, it seems an almost certainty that China is behind IPC, both great and small. While the legislative measures taken against IPC may indicate otherwise, the extreme ineffectiveness of such legislation, and clear incentive for such ineffectiveness, relegates such legislation to lip-service. It is in China's interest to give off the appearance of trying to combat IPCs to maintain its position within international trading organizations while simultaneously garnering profit from

88. Kanji, "Paper Dragon," 1267-1279.

89. Segal, "The Code Not Taken," 43.

illegal activities. China is intentionally shooting at its own criminals with blanks. While the Chinese government may not direct this small-scale crime, the evidence pointing to messy hands in its support of these crimes is potentially damning.

Proposed Action

Given the rampancy of Chinese EE, what actions is the international community taking to curtail this practice? The most noteworthy international effort to combat EE is the WTO's TRIPS agreement, which governs IP policy of the WTO members. Article 41 of this agreement explicitly calls for "action against any act of infringement of IP rights covered by this agreement…applied in such a manner to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse."[90] Herein are guaranteed so-called "DEER Rights" (Deterrence, Enforcement, and Expeditious Remedies), which guarantee owners of IP that the justice systems of the WTO will uphold their rights to that IP. Article 61 similarly calls for criminal penalties for violators of those rights.[91]

Since China joined the WTO in 2001, the TRIPS agreement and its articles apply to China. After joining, China agreed to hold annual Transitional Review Mechanisms (TRMs) in which WTO members could question China regarding its IP policies. While these are very promising in theory, the resulting arrests of IP violation have no resulted in any actual criminal liability.[92] Other than the WTO, there are no major international efforts currently being undertaken by the US to combat China's EE practices. The 1996 Economic Espionage Act is a federal piece of legislation, with any extradition next to impossible given the anonymous nature of the cyber attacks, so the last line of defense as of now is the "US-China cyber security working group."[93] In other words, our international measures against EE are slim to nil.

What we can control, however, regardless of China's involvement in EE at any market level, is develop strategies within companies to strengthen their defenses against IP theft. These policies include explicitly outlining what your IP is and implementing company-wide

90. Kanji, "Paper Dragon,"1268-1269.

91. Kanji, "Paper Dragon," 1269-1270.

92. Kanji, "Paper Dragon," 1277.

93. Crescenzi and Snyder. "Intellectual Capital and Economic Espionage," 250.

measures to protect it, conducting thorough research into the regional culture and legislation of any Chinese citizen or official you do business with, breaking up the production process so that no single entity possesses all aspects of intellectual properties, increasing security with any and all individuals with possible ties to China, and conducting as much intelligence on your counterparts as possible.[94] Implementing these simple tactics into the business model of a company can provide the last, and strongest line of defense against IP theft. Companies can no longer rely on federal or international legislation to protect them. While these measures should certainly not be the last lines of defense, they must form the fundamental bulwark against the onslaught of Chinese IPC.

94. Schotter and Teagarden, "Protecting Intellectual Property in China," 44-46.