CYBER WAR AND THEFT OF INTELLECTUAL PROPERTY:

The threat that China poses to the United States

Name

Institution

CYBER WAR AND THEFT OF INTELLECTUAL PROPERTY

Abstract

Over the recent past, there have been massive developments concerning the use of computer technology and the internet to conduct surveillance upon enemy nations or rival countries by other opposing powers. This paper discusses the recent developments in cyber space warfare and the role of china in the current threats that have placed the United States of America and the world as a whole on high alerts. The paper posits that there are steps the Chinese government has refused to take regarding the level of internet usage to access foreign intellectual content. Instead of working together with the USA and other governments to reach an agreement on the way they can exchange military intelligence, for example, the Chinese have reportedly hacked into the systems of other governments and helped themselves with this intellectual property. This paper discusses some of the most prevalent issues regarding Chinese IP theft as well as the characteristics of these thefts. The paper also analyzes the factors that will facilitate success and collaboration relative to China IP threats.

Introduction

In the recent past, there have been various threats as well as successful attempts by the Chinese to hack into the Computer intelligence systems of the United States government with the aim of stealing highly classified information regarding some of the core US operation schema. These recent threats are not the first of their kind, since the first IP theft cases can be traced back to as early as the 1970s. However, many researchers and scholars have given their opinions concerning the increasing cases of cyber attacks, with divergent opinions being brought into light. While some hold that theft of intellectual property of high value like military operations are acts of war, others argue that these are necessary evil that a country may indulge in to get trade secrets for the sole purposes of economic development.

Consistent research into the issue has revealed some cases of intellectual property thefts across history, and especially involving the US. What these researchers have failed to give the much deserved attention is the reasons why these IP thefts occur. Similarly, researchers have given only a small deal of research into the role of China in IP theft and its driving factor towards cyber war. The aim of this research paper, therefore, is to fill this information gap by offering an in-depth analysis on China's case. In order to achieve this, the paper will corroborate information from both primary and secondary sources on the topic of discussion so as to offer balanced arguments. The writer holds the position that the degree of involvement of China in IP theft has reached the extent that it can no longer be ignored or wished away. China is becoming a threat to the security of data in the computer achieves of the US, and by extension, the entire world.

This paper is divided into various sections for ease of analysis or perusal in the following manner. This section, which is the first section, is the introduction, which offer insight into the content of the paper and the objective of study the second section outlines some of the most important issues that have so far come into play regarding the formulation of China IP threats. The third section analyses some of the most fundamental characteristics of China IP threats, and the fourth section discusses the factors that will facilitate success and collaboration relative to China IP/threats. The paper winds up in a conclusive summary which offers a preview of the discussion and the author's thoughts on the same.

Global issues associated with formulating China IP/threats

The prosecution problem

Intellectual property refers to anything that is uniquely created by someone largely by the use of their mind (intellect) and, as such, has exclusive ownership rights. These rights are protected by the law and they extend to items such as music, art, literary content, inventions and discoveries, and symbols among others. In the computer world, they include programs, software, hardware, firmware and certain pieces of information that are otherwise classified to the owner(s). Today, most countries own huge archives of information regarding important functionalities of the government. The information can include anything from personal data of citizens, criminals, government, employees; to profiles of business organizations, their historical or criminal activities; to the country's military and defense strategies.

Chinese hackers continue to plague the world with their persistent intrusion into foreign computer systems in search of secrets and other things known only to them. As General Keith Alexander testified during his Senate confirmation hearing as the first leader of US Cyber

Command, the top government institutions are probed hundreds of thousands of times daily (Senate Armed Services Committee, 2010). These include the White House, CIA, FBI and Pentagon, among others, all of which are known for their huge banks of data. In 2006, Chinese hackers extracted an estimated 20 terabytes of data from government computers (Morozov, 2010). Private companies also are not immune from attacks. Earlier this year, Google moved from China to Hong Kong after tracing threatening cyber activity which affected at least 20 other U.S. corporations, to servers in China. As the Air Force takes on an expanding role in deterring and defending against foreign cyber threats, judge advocates find themselves increasingly responsible for providing cyber law expertise (Huntley, 2010).

To address this growing need, The Judge Advocate General's School recently launched its first cyber-law course. The three-day curriculum included lectures on computer and network basics, cyber operations law, and current threats in cyber warfare. Air Force JAGs can now earn cyber law LLM's. The Air Force Law Review likewise tackled the issue by publishing a master edition on a range of cutting edge cyber law issues

To provide context to the rapidly expanding field of cyber law, it is helpful to look more closely at the cultural environments in which hackers operate. It has been foldout that the hackers in china belong to organized groups with private communication channels. Understanding what might be called the "culture of Chinese hacking" enables scholars to contextually understand the threat of hacking as well as clarify some of the most crucial legal issues confronted in cyberspace.

Current Events

In recent years, American cyber attack victims have included an illustrious group: the U.S. State Department (2005), the Pentagon's NIPRNET (2006), the US Naval War College (2006), a nuclear weapons laboratory at Oak Ridge National Lab in Tennessee (2007), the White House (2008), and NASA (2008) (Huntley, 2010). In one instance, hackers linked to China reportedly acquired information on NATO troop movements in Afghanistan; in another, the Joint Strike Fighter program was reportedly compromised (Sullivan, 2009)

While individual hackers can and do pose a threat to U.S. security, recent reports suggest a substantial organization within the Chinese hacker community. Last year, researchers discovered a cyber espionage network called Ghostnet, which was targeting computers in the foreign ministries and embassies of many Asian countries, as well as news media and non-governmental organizations. A virus linked to Ghostnet was able to spread to some 1300 computers in over 100 countries. To make the situation worse, the Ghostnet hackers, most of whom are based in China, were able to posses the control of the victimized computers temporarily (Morozov, 2010).

More recently, researchers have uncovered a cyber espionage network that compromised systems primarily based in India (Sullivan, 2009). This network, originating in Chengdu, China, acquired information from the Indian government, the United Nations, and the office of the Dalai Lama, including access to his personal e-mail. One of the most historical hacking of all time is attributed to the operation in which Indian hackers stole the information regarding NATO troop movements in Afghanistan. These breaches of security reflect the global effect of such attacks.

The rapid increase in cyber threats present judge advocates with numerous novel legal issues, such as the definition of a cyber "weapon" and whether harmful cyber activities constitute

"attacks" under the law of armed conflict (Sullivan, 2009). Likewise, traditional JAG work in communications law, intelligence oversight, and information security law has been complicated by related cyber issues. One issue that is most significantly discussed currently is the issue of attribution in which the biggest question is whether the hacker can attribute his (or her) hacking activities to the government.

Attribution

In 2008, the U.S.-China Economic and Security Review Commission held a hearing on Chinese cyber threats, bringing together experts from throughout the national security community. The Commission's report from the event concluded that "determining the origin of cyber operations, and attributing them to the Chinese government or any other operator, are difficult. Computer network operations provide a high degree of plausible deniability to the Chinese government (Sullivan, 2009). To the extent that uncertainty obscures questions of attribution in the cyber world, how are legal advisors to proceed?

Under international law, a state can be held responsible for the actions of a non-state actor if it can "effectively control" the non-state actor.12 Officers with the People's Liberation Army Academy of Military Sciences elaborated on this point in 2007, explaining to an American delegation that attribution of hackers to the Chinese government would require that "the source… be clearly identified" (Goldsmith, 2009).

In the The Air Force Law Review, Major Arie J. Schaap argued that a more appropriate attribution rule in the cyber realm would allow for attribution where a state merely acquiesces to cyber attacks on foreign targets, despite having the means to prohibit and prevent such activity14

So conceived, if the Chinese government were to take a purely permissive stance on hacking, and if it demonstrated the capacity to prevent hacking originating within its sovereign territory, the argument might be made that the Chinese government could be held responsible for hacking originating in China. However, as discussed below, China has at least presented itself as neither purely permissive nor capable of preventing hacking (Sullivan, 2009).

Steps to criminalize hacking and publicize the prosecution of high-profile hackers creates at least a colorable argument that the Chinese government does not seek to permit hacking by non-governmental Internet users. Furthermore, reported attacks by Chinese hackers on Chinese business interests, many of which are closely connected to local government and party officials, suggests an inability to prevent some forms of non-governmental hacking (Sullivan, 2010).

It is perhaps too easy to argue that non-governmental hacking by private Chinese citizens cannot easily be attributed to the state, or that hacking by the People's Liberation Army can be attributed to the state. A more concrete and vexing attribution problem arises when one looks more closely at the gray area between state and non-state in China's sprawling military industrial complex. As part of its drive to modernize the PL A, the Chinese government has sought in recent years to draw on resources found in the civilian population. In 2003, for example, the Sixteenth Party Congress announced the policy of yujun yumin, or locating military potential in civilian capabilities. As a result, determining where the Chinese government ends and the civilian sector begin is an increasingly imprecise undertaking (Barboza, 2009).

Chinese universities are a case in point. Recently, researchers affiliated with major Chinese universities have published a number of articles on cyber security, including several examining vulnerabilities in U.S. infrastructure. One article, entitled "Cascade-Based Attack on

the U.S. Power Grid," looks at how an attacker might cause power grid failures in the United States. (Goldsmith, 2010). Another article, "Research of Attack Taxonomy Based on Network Attack Platform," introduced a network attack platform capable of launching virus, Trojan Horse, and other cyber attacks (Goldsmith, 2010).

The status of personnel at universities is likewise a complicating factor. The Information Security Engineering Institute at the Shanghai Jiaotong University (SJU) is currently headed by Mr. Peng Dequan, former Director of the Science and Technology Commission of the Ministry of State Security, one of China's principal foreign intelligence services Arie (2009). Through the revolving door between the academic and military communities is by no means unique to China, it does demonstrate the difficulties one would have clearly identified the source of Chinese cyber capabilities. Mr. Peng's position as head of SJU drives this point home, given that the recent hacker attacks on Google were traced to computers at SJU (Sawyer, 2010).

If the university system and military industrial complex were not complicated enough, perhaps the best example of the difficulties of accurate attribution in China is the eight million member militia spread throughout the country, which researchers call "an operational nexus" between Chinese military operations and civilian information security professionals (Barboza, 2009). Directly accountable to the State Council and Central Military Commission, militia units are comprised of civilians from commercial firms in fields critical to national defense, including software design and telecommunications (Mulvenon and Sam, 2010). Local militia units in Ningxia, Henan, and Guangdong provinces have published online material describing unit missions, which include network, information, electronic, and psychological warfare (Weinstein,

2009). These militia units have sought out individuals with foreign languages and cultural skills, suggesting a mission not limited to territorial China (Weinstein, 2009).

Attribution of Chinese cyber attacks likely will become increasingly difficult for US officials. As we have seen, there are no clear lines distinguishing military from non-military actors in China. While this blurry line plays a role in how hackers operate, cultural factors also influence the world of the Chinese hackers.

Chinese Hacker Culture

Hacker War, a novel published online in 2008 by a number of Chinese e-publishing websites, offers a window into the often inaccessible world of Chinese hacking (King, 2009). The protagonist, Chen Yonghao, hears the call to arms after the accidental NATO bombing of the Chinese embassy in Belgrade, Yugoslavia. Rather than taking up traditional weapons, however, Chen organizes a group of citizen hackers through an Internet chat room -- and the Chinese Hackers Union is born. The Union then launches a series of patriotic cyber attacks against those believed to be most responsible for the bombing: the United States government. The White House website is hit first. Chen hacks in and defaces the website, causing the site to be shut down as repairs are made. News of the hack quickly spreads, earning Chen and the Union respect and fame throughout the Chinese Internet community (Todd, 2009).

Scores of books similarly lionizing patriotic Chinese hackers have been published online in recent years, one indication that hackers increasingly enjoy an esteemed position in modern Chinese Internet culture. Hacker novels with names like Hacker Legend and I Am A Hacker are commonplace, putting Chinese citizens a click away from a fictional tour through the computer systems of the Pentagon, White House, and other popular U.S. targets. Perhaps recognizing the

emergence of the hacker hero phenomenon, the Chinese government has recently ramped up efforts to reframe the issue and brand hackers as mere criminals. Recent headlines - including those in publications closely monitored by the Chinese government - tell of prominent hackers brought to justice by an increasingly tech-savvy Public Security Bureau (Jie, 2009). But for all the efforts of the Chinese government, hacking continues to be a growth industry in China, and its reach is global.

A culture of underground hackers feeds off easy access to and continual encouragement from websites and hacker fiction. In China, hackers have remarkably easy access to information guiding their activities. Four major search engines in China, Baidu, Google China, Google US, and Yahoo!-China, all produce links to hacker websites with a simple search of "Multiple line equation cannot be converted into text." the most common Chinese term for "hacker." These hacker websites include discussion forums where hackers compare accomplishments and describe how to hack certain networks (Branigan, 2009). With easy access to such information, new hackers can learn how and what to hack and receive encouragement for doing so.

Online novels are a wildly popular phenomenon in China and a major growth industry (Branigan, 2009). At times earning $10 per thousand characters typed, online authors of hacker fiction can be expected to keep pumping out their product, and legends of heroic hackers storming the distant walls of American network infrastructure will proliferate.

Chinese Law

While China is not a member of the European Union Convention on Cybercrime, new laws passed in 2009 by the Chinese People's Congress do appear to reflect an effort by China to

adopt the core principles of the Convention (Branigan, 2009). The Convention requires that member states criminalize certain forms of cyber activity, including unlawful access, interfering with data or systems, unlawful interception, and computer fraud or forgery (Jie, 2009).

Two new Chinese laws criminalize illegal acquisition of computer system data or control of computer systems and prohibit supplying programs or tools for the purpose of illegal control of computer systems (Branigan, 2009). Conceivably, the new law prohibiting the supply tools for the purpose of intrusion into computer systems could be the tool used to shut down many of the easily accessible chat forums and hacker fiction websites that provide instructions on how to hack systems of foreign governments. There is some anecdotal evidence that the Chinese government could be in the early stages of a crackdown on certain types of unlawful cyber activity; (Branigan, 2009) the Chinese government, for its part, claims to have "nabbed" just over 1,000 hackers under the new criminal laws, though such reports are difficult to verify.

China's well known restrictions on free expression likewise permit the government to restrict hacker websites and literature. Under Article 225 of China's Criminal Law, Chinese publishers are prohibited from publishing materials without first acquiring a license through the General Administration on Press and Publication (GAPP) (Todd, 2009). In addition to licensing restrictions, GAPP works with the Central Propaganda Department to regulate the content of publications. The Regulation on the Administration of Publishing (2001) empowers officials to punish authors and publishers for a number of infractions, including the vague prohibition on published material that "harms national security or national interests." (Todd, 2009). A web search conducted from China for the Tiananmen Square Massacre produces a webpage with an error. Other taboo topics include the Dalai Lama, political independence of Taiwan, and ethnic

conflict in Muslim regions of China. The Chinese government censors this material in the name of national security and national interest. However, hacker websites and hacker fiction that glorifies cyber attacks of the U.S. government remain largely unfiltered.

Chinese law enforcement has used this regulation to crack down on Internet books with unapproved content in the past, such as the 2007 sting resulting in the removal of over 300 online books featuring pornographic content (Jie, 2009). Together, China's cybercrime and publishing laws equip law enforcement with strong tools to address hacking and other cyber threats. While the Chinese government possesses the legal tools to do so, it does so infrequently. One could argue that the smothering censorship applied to certain subject matter - such as the Dalai Lama or Taiwanese independence - and the relatively limited restrictions on hacker Internet discussion forums, websites, and even e-books, implies a tacit endorsement of Chinese hacker activities.

These uncertainties raise strategic questions of the first order: does China "harbor" hackers? Should the language of the War on Terror be applied in a future War on Cyber Terror? How could China demonstrate to U.S. satisfaction that it does not "harbor" hackers? Would an international organization tasked with cyber inspections – akin to the current nuclear watchdog regime – help resolve these issues?

The beginning of an answer may lie in what is known as the United States-China Joint Liaison Group (Liaison Group). Having evolved over the decade-plus since President Bill Clinton met with Chinese leaderships to establish stronger bilateral relations, the Liaison Group today serves as a primary vehicle by which the United States and China coordinate bilateral law enforcement operations on issues like transnational crime and intellectual property infringement. Headed by the U.S. Department of State and the Chinese Foreign Ministry, the Liaison Group

has helped the two sides resolve a number of cases, including an anti-intellectual piracy operation over $500 million (Jie, 2009).

The Liaison Group could help resolve one type of attribution problem in particular: where the United States has been cyber-attacked and China wants to avoid responsibility (e.g., war). Through the Liaison Group, China can help the United States verify that, though the attacks originated in China, they were done by rogue elements or otherwise non-state citizen hackers. The Chinese side of the Liaison Group could get the Public Security Bureau to arrest the hacker and hand him over to the FBI, thereby verifying that no "armed attack" justifying American retaliation had occurred. Whether it takes the form of the Liaison Group or some other vehicle of coordination, the United States and China would do well to take quick steps to institutionalize a joint fight on cyber threats, thereby reducing the types of uncertainties and suspicions that have been the prelude to conflict throughout history.

Conclusion

Hacking is now a popular sport in China. The hacker hero is alive and well in Chinese popular culture and fiction. How the emergence of a Chinese hacker culture will influence the frequency and severity of Chinese hacker attacks remains to be seen. At the very least, Chinese hackers have an increasingly rich library of hacker fiction from which to plot their next attacks. Recent cyber attacks worldwide reflect a need to understand where these attacks originate. As we continue to develop technology, organization, and skills necessary to combat cyber threats, it is ironic that we rely ultimately on the Chinese philosopher Sun Tzu, who counseled in The Art of War to "know your enemy" (Weinstein, 2009). Doing so will better enable the Air Force to win the fight in cyberspace.

As the Air Force takes on an expanding role in deterring and defending against foreign cyber threats, judge advocates find themselves increasingly responsible for providing cyber law expertise. One issue presenting a challenge is attribution: when, if ever, can the victim of a cyber attack attribute responsibility to the host government of the hacker? (Weinstein, 2009).

Characteristics of China IP/threats

There are many examples of China-based IPR breaches. Huawei Technologies, for example, China's leading telecoms-equipment maker, according to The Economist ("Special Report: China's Champions," 2005) was successfully sued by Cisco for IP theft in an American court. Huawei is one of the so-called state champions that the central government decided would be among the 30–50 of its best state firms to be built into globally competitive multinationals by 2010 ("Fear of China," 2005). At home, these companies enjoy tax breaks, cheap land, and virtually free funding via the state-owned banks. Abroad, the Chinese government helps these state champions to secure contracts or exploration rights ("Special Report: China's Champions," 2005). Chinese car firms are pervasive counterfeiters of foreign models: one local favorite is half Mercedes, half BMW ("Fear of China," 2005). So ahead of the game are the counterfeiters that Harry Potter books are published in China before J. K. Rowling, the author, has written them!

Amcham-China's president maintains that "the problem [of IP theft] is growing faster than the enforcement efforts . . . and this problem of growing exports is really one to watch because that is going to reverberate against China on the international stage" (AmericanThere are many examples of China-based IPR breaches. Huawei Technologies, for example, China's leading telecoms-equipment maker, according to The Economist ("Special Report: China's Champions," 2005) was successfully sued by Cisco for IP theft in an American court. Huawei is

one of the so-called state champions that the central government decided would be among the 30–50 of its best state firms to be built into globally competitive multinationals by 2010 (“Fear of China,” 2005). At home, these companies enjoy tax breaks, cheap land, and virtually free funding via the state-owned banks. Abroad, the Chinese government helps these state champions to secure contracts or exploration rights (“Special Report: China’s Champions,” 2005).

Chinese car firms are pervasive counterfeiters of foreign models: one local favorite is half Mercedes, half BMW (“Fear of China,” 2005). So ahead of the game are the counterfeiters that Harry Potter books are published in China before J. K. Rowling, the author, has written them! Amcham-China’s president maintains that “the problem [of IP theft] is growing faster than the enforcement efforts . . . and this problem of growing exports is really one to watch because that is going to reverberate against China on the international stage” (American Chamber of Commerce China, 2006). Some analysts, Yang (2005) for example, argue that some allowance for cultural impediments on the Chinese side is called for to establish a tighter IP protection regime. The argument for tolerance is predicated on history: during the Qing dynasty (1644–1912), China ruled almost a third of the world’s population and oversaw a third of the world’s GDP. It can look back on a history of innovation, spanning the inventions of paper money, explosives, the printed book, and professional civil service (Maddison, 2001). Today, there remains more than a vestige of resentment among the Chinese people that their inventions attracted none of the royalties that they are now exhorted to pay to others.

Perhaps this period of IP piracy is an intermediate phase on the road to development, just as the United States a century ago exhibited similar behaviors. For example, Charles Dickens complained bitterly about the theft of his rights by American publishers (Edwards, 2007). The Budweiser brand, it is claimed, was systematically deconstructed and stolen in the nineteenth

century from Czech brewer Budejovicky Budvar by a Czech émigré, and then reconstructed in the United States. As recently as 2009, the second largest court in the European Union confirmed a previous decision not allowing Anheuser Busch to register the trademark Budweiser in the European Union ("Court Has Supported Budvar," 2009).

It may be expected that China will become more compliant about protecting IP when it gauges that it has enough of its own IP to protect (Kirkpatrick, 2005). Indeed, China now has a National Intellectual Property Strategy that looks to "improve the intellectual property system, actively work to create a favorable legal environment, market environment and cultural environment for the development of intellectual property in order to greatly improve China's capacity to create, utilize, protect and administer intellectual property. This will provide strong support for the effort to make China an innovative country and develop a moderately prosperous society in all respects" (Outline of the National Intellectual Property Strategy, 2008). This phraseology disturbs other governments, as they expect China to use its IP portfolio to block entry and negotiate advantage in international markets. The potential is great. China is now a major source of innovation; for example, in 2008 there were 800,000 Chinese patent applications, 360,000 of which were for design patents.

Analysis of the China Cyber war situation

The research for this article involved a subset of 20 face-to-face interviews conducted in China, with a range of relevant players: CEOs of companies that hold multibillion-dollar asset portfolios based on heavy concentrations of IPRs, IP lawyers, IP consultants, management consultants, advertising agencies, branding consultants, and those who track down and prosecute

counterfeiters on behalf of the IP owners. These interviews comprised a subset of a larger study involving 150 interviews probing the experiences of foreign companies in China.

The analysis illustrates that the methodologies employed by many foreign companies to ensure the integrity of their IP in China are seriously flawed. It is estimated that over 70% of cases, IP theft in China occurs as a result of companies having failed to take effective action, or having executed only partially effective steps to protect their IPRs. The data analysis of the CEOs interviewed suggests that the majority of companies are not taking effective steps to protect their intellectual property.

It is paradoxical that these foreign-invested enterprises (FIEs) have a myriad of governance rules, ranging from the use of cash through to the issuance of stock options, yet the critical group of intellectual assets known as IP is left largely unguarded. Given that employees are the most vulnerable IP leakage point, human resources (HR) policies in the majority of cases appear lax from the outset as they fail to make provision, as part of the recruitment process, for striking tight agreements regarding IP protection. As an IP lawyer explained, IP has legs: What we normally see in China is the leg. Where do the legs come from? The legs come from your employees. They're the ones with access to the information.

They're the ones with the access to your intellectual property. It's not the patent office. It's not the government that's giving your secrets away. So once you've registered your IP, you need to go and take an approach which is employee based . . . you should get your employee's contracts, take a look at them, and try to assess whether or not your IP is protected in those agreements and whether or not you've signed employment 010 DOI: 10.1002/tie contracts which have valid clauses in them to protect intellectual property.

> Protection is a necessity. As a senior China-based Microsoft executive stated: When we hire people . . . people sign noncompete agreements [NCAs]. They sign nondisclosure agreements [NDAs]. . . . Just in case somehow our system got broken . . . there are always some recovery actions that we can make. For example, when something comes up [an innovation], we can patent it and whenever somebody comes up with something very similar to what we're doing . . . if we have a strong belief that this has leaked out, then as long as we can prove it, we can file a claim for that patent.

Several of the organizations surveyed were represented by those who appreciated the value of their firm's IP. They have the expertise to protect it, but rarely it seems do the parties work consensually to inhibit theft and leakage, largely due to the silo mentality referred to earlier. The present study found that IP losses were often attributable to failures by companies to effectively seal the leakage points. This porosity derives from a frequent absence of a single point of responsibility for IPR protection. FIEs frequently neglected to weave together the functions of IT, Security, HR, and engineering, each of which operates according to differing agendas with respect to IP protection.

As an IP protection consultant informed: We found that most companies have not managed IP well because it falls between different divisions.

> It could fall between research and development, labor, procurement, finance. . . . And unless those divisions cooperate and coordinate and bring it together, you have an ineffective strategy. . . . What we've found from our experience in the enforcement side is that most companies . . . have not pulled IP together. Because of a general failure to bring the strands of IP protection activity under a unitary command structure, the divided

> responsibility on IP protection often leaves enterprises susceptible to IP theft and, subsequently, the trying ordeal of dealing with China's legal process. The head of Boston Consulting Group stated, "In the past, companies thought of IP as something that the lawyer would handle . . . register your patents in China. But what we are learning is that it is a much broader topic."

IP leaks occur in a wide range of industries. In many cases, the loss of IP occurs because of a company's failure to understand the China IP environment and the flexibility it affords to shore up IP protection levels. Some lose IP as a result of the most fundamental omissions. For example, China patent law operates on a first-to-file basis. As a result, arbitragers in China may temporarily usurp mature technology rights and other IPRs by seizing public domain knowledge to register patents and trademarks in China, so as to subsequently inhibit the original IPR owners from developing their China market positions.

Regarding first to file, an IP lawyer interviewed stated: Patents for invention are examined for substance in China and undergo a thorough investigation by the examiner whereas design patents and utility models are granted after having passed preliminary examination. And that means that lots of rights, especially lots of technology that is already registered in Europe by other companies, are registered by Chinese enterprises as utility models. And later on, once you are in the market you will find out, well, that's my technology and someone else says, "I have a patent on that." You look further into the issue and you find, oh, utility model. Someone else took your technology and registered it as his own to later on use it in the Chinese market.

This does not mean, however, that the first to file will necessarily be awarded patent rights. In particular, China and almost all countries require absolute novelty as a basis for patent

rights to be awarded. Thus, if the invention was publicly known anywhere in the world prior to the patent application being filed, a patent will not be awarded. But critical market development delays may be inflicted and/or payments exacted to minimize their impact.

Regarding trademarks, an IP lawyer interviewed stated, “Trade names have to be registered locally. To protect your trade name in China, you need to have a [Chinese] trademark.” Trademark registration is another area where many foreign players are seriously remiss. Some fail even to establish Chinese versions of their brand names. Large and small players alike exhibit this trait. Pfizer, for example, according to Rouse, the IP consultancy, one of our interviewees, failed to appreciate the extent to which a Chinese name constitutes a critical part of a branding and trademark strategy.

To fail to provide a Chinese brand name in a timely fashion is to invite the Chinese population to invent one. And in the case of Viagra, they did so, even before Viagra had reached the China market. The local name, Weige, which became the everyday reference term for the product, remained beyond the control of Pfizer and under the aegis of Shenyang Feilong Health Products Co. Ltd. Our data analysis suggests that Chinese branding is one of several issues on the foreign investors’ report card that requires improvement.

In another case, an American consumer products vice president among the study’s interview set revealed that counterfeiting and piracy imposed a huge cost, “Our senior executive team, largely expatriate, devotes 70% of its time to dealing with IP infringement, counterfeiting, and pirating challenges.” Shortcomings in IPR protection strategies compound subsequent problems; technology is misappropriated and company performance is impacted; and management becomes distracted by legal issues.

Conversely, the study's data show that the most successful companies are those that take effective strategic and operational action to protect their IPRs a priori, thus lowering their litigation risks and improving the likelihood of keeping their IPRs secure in China. Based on our analysis of the data, we advance the following testable propositions:

Proposition 1: Companies frequently fail to learn from the mistakes pertaining to IP protection of others, even within their own organizations. They fail to make the most of the help that is available to them in trade associations or is accessible from other external sources.

Proposition 2: It is of no consequence where an IP leakage occurs in an organization; the damage may be equally severe whether it leaks in China or France. Companies invariably have no overriding coordination of IP matters and often do not adopt the best practice available in their own organizations or beyond.

Proposition 3: The typical absence of an IP czar in companies means that few attempts are made to hash out policies and practices that are acceptable and could be made to apply throughout the enterprise.

Proposition 4: Approaches to IP protection tend to be atomistic and parochial, not global. There is a need to develop IP protection strategies in a global context.

The bard model

In light of the ever-increasing volume of writing on IP in China, an important and surprising idea at the core of the BARD model is the finding that many foreign enterprises in China fail to make an adequate search for, and to keep up with, what is best practice in dealing with IP in China. This omission inhibits understanding of the issue and, consequently, restricts

the actions that might be taken to address the China IP situation. BARD meets the need, highlighted earlier as a literature gap, to map and define best IP practices in China including the identification of those intellectual assets that would be prudent and cost-effective to protect.

A second important idea inherent in the model is that in meeting the China IPR challenge, companies are required to act locally, in China, and globally. Making substantial progress in IPR protection in China necessitates addressing regional and global issues such as processes, organization structures, and working culture. These shifts represent a counterintuitive perspective from the one prevailing among many managers and organizations in our study. While the tendency is to recoil from or take only local action to limit China IPR problems, this study shows that effective action on China IPR issues requires proactive engagement with senior management and the head office.

The BARD model prompts companies to pose previously unasked questions of them. In addressing the questions, companies are required to think through and act, first, on a company's IPR protection in China, and then on a companywide basis. This will prompt some far-reaching examination of how a company organizes itself to deal with IPRs; the level of IP and information security protection each company wants and needs; the trade-offs and costs of achieving these improvements; and possible changes to the way work is done as a consequence of taking these decisions.

This will deliver two sets of benefits: (1) at the local level, improving a company's IPR protection in China, and (2) at the global level, bolstering a company's global IPR protection together with overall information security. The rationale and the design of the model will work well for companies across many industries with IPR and operations in China, such as trademark-

based businesses, software companies, firms with process technology, and those with proprietary patented products. It is relevant for MNEs, and the precepts apply also, with adaptation, to small to medium-sized enterprises (SMEs) that are expanding their scope internationally. It will not work well either for commodity-based trading businesses or for retail assortment, or much beyond trademark protection. Neither will it work well where the business model is based on a choreographed performance (Starbucks, for example). In those cases, protection is best achieved by differentiation via an emphasis on superior execution.

The BARD model is a four-stage framework evolved from our findings relating to common elements among initiatives taken by the minority of companies that have been observed to improve their IPR protection in China. Some of these companies have succeeded in reducing IP leakages and, thus, mollified concerns about this down-side of China investment. Importantly, they have also reduced the potential for leaks elsewhere in other parts of their global operations. BARD involves: best practice determined by benchmarking, audit, review, and design.

Stage One: Best Practice, Searching

The china experience Most CEOs of FIEs in China are dissatisfied with their levels of IPR protection. Yet, this discontent is counter pointed by their abject neglect of IP protection. At times it is akin to being trivialized as an “attractive nuisance,” where the keys to the house, full of valuables, are accessible to many. A glaring leadership failure was found by the study to exist in many IPR matters, the tendency being to devolve responsibility to legal, IT, or security functions.

An IP protection consultant explains: A business partner was ripping one of our clients off. We had to start with the legal agreements. Initially the legal people who walked away from it

signed these agreements. It becomes a question of who follows up on the agreements to protect the IP. Executives think about protecting IP primarily in legal terms, with few integrating the legal, operational, and strategic dimensions.

Stage two: audit

IP can be swung across frontiers overnight; for example, if protection practice is sloppy in France, the IP may be quickly exploited in China or Kazakhstan, or elsewhere. So, in this second stage, the best practices distillation may be operationalized by way of providing a brief to a team to report on policies, issues, problems, and gaps identified in a China business or global operation. What is required here is for enterprises to perform an audit of IP protection practice across divisions and geographical regions.

Stage three: Review

The limit of the audit team(s) overarching review is to recommend steps to be considered by individual divisions, related functional streams, and the head office. Typically, these recommendations will drive discussions about what levels of IP security are required, with inputs from the many stakeholders being essential. Some experts point to the differential costs in protecting different categories of IP (Dietz et al., 2005; Hulme, 2009). In one of the examples studied here, a U.S. high-tech manufacturer with extensive investments in China classified its at-risk IP into three categories: low value, medium value, and high value. Several interviewees indicated that to protect IP in each of these bands requires varying levels of sophistication and tolerance of differing levels of associated cost to do so.

Stage four: Design and Implement

When designing organizations, structures, and systems for a China venture, it is necessary to recognize the reality of IP exposure. The interviews undertaken for this study confirmed that employees are by far the most vulnerable leakage point as far as IP is concerned. An IP lawyer put it this way: “In China IP seems to grow legs and it often starts walking out of the door.” Nondisclosure agreements and noncompeting agreements may be deployed, but they are only as robust as the integrity of those whose signatures adorn them. NCAs, however, under the new labor laws may only be applied to corporate officers. It may be assumed that employees with valuable knowledge will ultimately walk. As a source of leakage frequency, suppliers closely rival employees. Given that much business is conducted by outsourcing, this is a particular risk.

Conclusion

IPRs are recognized as the jewels among corporate assets, yet their protection in China appears ineffectual in many companies. The need for a more comprehensive strategic approach to deal with IPR protection has been identified. What complicates the issue of IPR protection is the existence of countervailing forces: China’s rapid accumulation of IP, fueled in part by the NIPS, and the attraction of long-term market development opportunities in China that require good relationships to be developed with government at all levels. This requires strategic trade-offs to be made, as was the case with some of the companies interviewed for this study; with some difficulty, they tempered their immediate responses to IP theft in order to keep the government on their side.

The gargantuan role played by government in the China business environment is one of the salient distinguishing characteristics of the operating environment in China. Therefore, IPR strategy has to adapt to it and reflect the operating environment reality. Those companies that deal only on a local or regional basis with China IP challenges are missing opportunities to engage senior management; leverage head-office resources; and pass on important lessons learned by tackling some of the toughest questions dealing with IP anywhere in the world today.

References

Aaker, D. A. (2008). Marketing in a silo world: The new CMO challenge. California Management Review, 51(1), 144–156.

Agence France-Presse. (2007). China punishes nearly 350 porn websites, Aug.14. *Breaking news at inquiresrs.com*

Arai, H. (2000). Intellectual property policies for the twenty-first century: The Japanese experience in wealth creation

Branigan, T. (2010) China closes training website for hackers, THE GUARDIAN.

Brown, A., Osborn, T., Chan, J. M., & Jaganathan, V. (2005). Managing intellectual capital. Research Technology Management, 48(6), 34–41.

Chapa, O., & LeMaster, J. (2007). Chinese intellectual property rights? Know before you go. Thunderbird International Business Review, 49, 567–590.

Congressional-Executive Commission on China, Annual Report (2010), at 57 (citing Regulations on the Administration of Publishing [Chuban guanlitiaoli].

David Barboza, (2009). Baidu's Gain from Departure Could Be China's Loss, N.Y. TIMES

David Barboza, (2010). Hacking Inquiry Puts China's Elite in New Light, N.Y. TIMES, Feb. 21,2010, available at http://www.nytimes.com/2010/02/22/technology/22cyber.html.

Dickie, M. (2006). Music magazine hits sour note with China bureaucracy. Financial Times.

Edwards, C. (2007, March). How to shake the fakes. Engineering & Technology, 2(3), 42–45, doi:10.1049/et:20070305

Evengy Morozov, (2010). Battling the Cyber Warmongers, WALL STREET JOURNAL, May 8,

Green, S. (2007). China years: How many are you living? In on the ground—Asia. London: Standard Chartered.

Hulme, V. (2009). Mark Cohen on intellectual property. China Business Review, 36(2), 22–25.

Jack Goldsmith, July 1, (2009). Defend America, One Laptop at a Time, N.Y. TIMES.

James Mulvenon and Rebecca Samm Tyroler-Cooper, (2009). "China's Defense Industry on the Path to Reform"(citing Fortifying China:The Struggle to Build a Modern Defense Economy (Ithaca: Cornell University Press), at 9), U.S.-China Economic and Security Review Commission.

Keith B. Alexander, (2010). Advance Questions for Lieutenant General, USA Nominee for Commander, United States Cyber Command: Hearing Before the Senate Armed Services Committee, 111th Cong.

King, A. (2009) The Chinese Novel Finds New Life, WIRED.

Larry M. Wortzel, Commissioner, US-China Economic and Security Review Commission, House Committee (2010). China's Approach to Cyber Operations: Implications for the United States: Hearing before the on Foreign Affairs, 111th Cong.

Lt Col Graham H. Todd, (2009). Armed Attack in Cyberspace: Deterring Asymmetric Warfare With An Asymmetric Definition, A.F. L. REV 82

Major Arie J. Schaap (2009)., USAF Cyber Warfare Operations: Development and Use Under International Law, A.F L. REV 64

Sullivan. J.H. (2009). Tracking GhostNet. *Munk Centre for International Studies, University of Toronto*,

Sullivan. J.H. (2010). Shadows in the Cloud. *Munk School of Global Affairs, University of Toronto*,

Todd Huntley, (2010). Controlling the Use of Force in Cyberspace: the Application of the Law of Armed Conflict during a Time of fundamental Change in the Nature of Warfare, 60 NAV. L. REV. 1

US-China Economic and Security Review Commission, (2008). "China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities.

Us-China economic and security review commission. (2009). Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Oct. 9, 67-74.

Weinstein, J. (2009). Department of Justice, Statement before the United States House of Representatives.

Xinhua Net (2009). China detains two hackers for stealing deposits at R0Kbanks.