2009-01-00

Competing with Intelligence: New Directions in China's Quest for Intangible Property and Implications for Homeland Security

Slate, Robert

Monterey, California. Naval Postgraduate School

Homeland Security Affairs (January 2009), v.5 no.1
http://hdl.handle.net/10945/25026

Competing with Intelligence: New Directions in China's Quest for Intangible Property and Implications for Homeland Security[†]

Robert Slate

INTRODUCTION

Some enterprises do not hesitate to use illegal means to collect intelligence from their competitors, making trade secret protection increasingly challenging and urgent.

—China Business Training Course on Competitive Intelligence Practices
Shanghai, Oct. 17-18, 2008[1]

Chinese executives' intense desire to succeed globally, combined with the Chinese government's encouragement and support,[2] has driven some companies to develop corporate competitive intelligence (CI) programs that increasingly rely on illegal human and technical intelligence collection methods[3,4] to acquire intangible property from U.S. companies and government agencies. The plethora of industrial espionage cases involving Chinese companies in recent years reveals extensive Chinese government involvement in such activity[5] and the role of CI in facilitating the transfer of U.S. proprietary technology from civilian to military uses.[6] Against this backdrop, the United States faces a rising national security threat from Chinese corporations that employ robust CI programs to enhance illegal company- or government-directed espionage and intellectual property (IP) theft and infringement. The complicated and global character of this phenomenon[7] requires that the U.S. government rethink the traditional intelligence community (IC) approach to collection and analysis of intelligence on China and the implications for homeland security.

This article draws upon a body of Chinese literature on CI to explore the role of CI in helping China to conduct industrial espionage and acquire U.S. IP and illustrate how the study of Chinese CI can help the U.S. government and business make sense of future trends in Chinese industrial espionage. Chinese CI theory and practice is pushing Chinese intelligence in new directions;[8] however, this trend has gone relatively unnoticed in the U.S. intelligence and academic communities, probably because CI is largely viewed as the domain of private sector and professional organizations in the United States.[9] Despite Chinese corporations' growing reliance on CI, and the significant role it has played in corporate successes, many U.S. companies remain relatively unfamiliar with the state of Chinese corporate intelligence and the evolving risks for U.S. corporations.

INTANGIBLE THREAT

The 17th Century French missionary Louis Le Comte wrote in his memoirs that trade and commerce "is the soul of the (Chinese) people" and "the *primum mobile* of all their actions."[10] China's trade and commercial genius has certainly played a major role in the

spectacular rise of China's economy and its integration with the U.S. economy over the last several decades. Some observers view China's growing stake in America's economic system as an extremely positive development for the United States, while others see Beijing as a military, economic, and technological threat. Most would probably agree, however, that China's growing economic power[11] and massive annual trade surplus with the United States – $250 billion and growing – puts China in a position to affect the United States economy in ways considered improbable in the past.[12]

Chinese firms' increasing involvement in corporate spying and IP theft in America raises the stakes of the trade deficit problem with China and is the source of a great deal of concern for U.S. homeland security. Chinese corporations that use IP theft and infringement as components of their overall business model, and effectively employ corporate intelligence programs to that end, are damaging the foundations of the American corporate world: intangible property.

Most of the value in corporations, particularly in America, remains in intangible property. The term "intangible property" is generally used to refer to the following non-physical assets, such as intellectual property (e.g., patents, copyrights, trademarks, and trade secrets), legal rights (e.g., leases, contracts, and licenses), relationships (e.g., supply and custom distribution chains) and brands. According to a 2006 Brand Finance report in 2006, 62 percent of the value of corporations around the globe is based on intangibles ($19.5 trillion of global market value).[13] U.S. corporations have 75 percent of their value tied up in intangibles.[14] Not surprisingly, intangible property accounts for 98 percent of the U.S. technology sector.[15]

Intellectual property receives a lot of attention because its misappropriation can devastate companies, especially those in IP industries, and can have a disproportionate impact on countries like the United States, where IP factors so prominently in the overall economy. U.S. IP industries, for example, have been responsible for approximately 40 percent of the total growth of the U.S. economy.[16] The International Intellectual Property Alliance (IIPA) released an economic study in 2007 that assessed U.S. copyright industries (e.g., entertainment software, motion picture, business software, and recording) as contributing more job growth, gross domestic product (GDP), and foreign exports and sales to the U.S. economy than any other industry; they contributed about $1.38 trillion to U.S. GDP, employed 11.3 million workers, and accounted for approximately $110.8 billion in foreign sales and exports in 2005.[17]

OVER 300 HUNDRED YEARS OF COUNTERFEITING EXCELLENCE

Le Comte extolled Chinese merchants for their commercial genius, but suggested they focus much of their "labor and natural industry" on dishonest business practices and counterfeit "almost everything they vend."[18] He writes: "(Chinese merchants) counterfeit Gammons of Bacon so artificially, that many times a Man is mistaken in them; … It is certain a Stranger will be always cheated, if he buy alone, let him take what care he will."[19]

Remarkably, Le Comte's observations from over 300 years ago remain valid today, and manifest themselves in the intractable problem U.S. companies encounter doing business with China: how to take advantage of China's vast trade and commercial

potential without losing much of the intangible value of their corporations to counterfeiting and other forms of infringement.

Chinese counterfeiting and piracy levels are extremely high. According to the IIPA's 2008 Special 301 Report, Chinese copyright piracy cost U.S. copyright industries almost $3 billion in 2007; piracy levels reached 90 percent of published records and music, 80 percent of business software and 95 percent of entertainment software. According to the U.S. trade representative's report to Congress on China's World Trade Organization compliance in 2004, the value of Chinese counterfeit products brought into the U.S. market reached $134 million. Chinese counterfeiting also limits demand for legitimate U.S. IP products globally, which damages company revenues and, by extension, the U.S. economy. The U.S. Department of Commerce, for example, reported that Chinese counterfeiting cost the U.S. economy about $20-24 billion in 2004.

Counterfeiting is not limited to Chinese street merchants. Chinese multinational corporations (MNC) are significant contributors to the overall counterfeiting of high-tech products. Cisco Systems filed an IP infringement claim in 2003 against Huawei Technologies (a powerful Chinese MNC that produces telecommunications and networking equipment) for copying patented Cisco technologies, user manuals, and the source code used for Huawei's counterfeit routers. In a 2005 interview with PriceWaterhouseCoopers, Warren Heit, a partner at White & Case, states that display cases at some of Huawei's offices contained 'perfect' knock-offs of Cisco telecom and Polycom equipment.[20]

Some Chinese MNCs view both legal IP development and illegal IP theft and infringement as extremely important components of their business models and key to their long-term profitability and survival. Huawei's business model, for example, is partly based on selling counterfeit products in developing countries with poor IP protection. As Heit suggests: "Huawei is saying to itself… 'I am going to knock (Cisco) products off and to the extent the IP law allows me to practice in these areas, I'm going to go there…Cisco, maybe you can have the U.S., but I'll take you everywhere you haven't gone.'"[21]

Chinese corporations' counterfeiting of high-tech equipment and IP theft raises concerns beyond economic loss. Counterfeit computer components from China, for example, could be used to compromise U.S. corporate and government computer networks and cause military systems to fail.[22] The U.S. government in early 2008 seized $76 million worth of counterfeit Cisco routers, switches, WAN interface cards, and gigabit interface converters, which were purchased by the U.S. Naval Academy, U.S. Naval Air Warfare Center, General Services Administration, U.S. Naval Undersea Warfare Center, and defense contractor Raytheon, among others.[23] Melissa Hathaway, director of the Director of National Intelligence's (DNI) cyber security office, commented on the government's seizure of over 400 counterfeit routers: "Counterfeit products have been linked to the crash of mission-critical networks, and may also contain hidden 'back doors' enabling network security to [be] bypassed and sensitive data accessed [by hackers, thieves, and spies]."[24]

COUNTERFEITER, HACKER, SOLDIER, SPY

Chinese espionage directed against U.S. government and corporate targets is well-documented in the recent literature. U.S. Immigration and Customs Enforcement officials have investigated over 540 instances of illegal technology exports to China, which often involve Chinese corporations. The *Washington Post* published an article in April 2008 describing twelve cases of Chinese espionage that have occurred since March 2007. The charges range from illegal export of warship technology and source codes for simulation software for the precision training of fighter pilots, to theft of trade secrets from two companies on behalf of a Chinese military program. Joel Brenner, the head of the counterintelligence office of the DNI, states: "Espionage used to be a problem for the FBI, CIA and military, but now it's a problem for corporations…It's no longer a cloak-and-dagger thing. It's about computer architecture and the soundness of electronic systems."[25]

The U.S. Defense Department and IC claim that China is America's most serious cyber security threat.[26] The Office of the DNI, in response to a *Business Week* inquiry, stated that computer intrusions have been successful against a wide range of government and corporate networks across the critical infrastructure and defense industrial base.[27] A recent *Business Week* special report revealed Chinese hackers may have recently sent an e-mail attachment containing the malicious computer code to an executive at Booz Allen Hamilton, a $4 billion U.S. corporation, in an attempt to infect the company's computer network and acquire sensitive information. According to the report, hackers have launched numerous similar attacks on U.S. companies and government agencies for the last several years; the Departments of Defense, State, Energy, Commerce, Health and Human Services and Treasury, and corporations Boeing, Lockheed Martin, General Electric, Raytheon and General Dynamics, are some of the known victims. The U.S. government reported the occurrence of 12,986 cyber intrusions and other cyber security events on government and defense contractor networks; U.S. military networks experienced a 55 percent increase in attacks.[28] O. Sami Saydjari, a former National Security Agency (NSA) official, suggests the scale of organized Chinese hacking activities – much of which involves the Chinese military[29]– is having a devastating impact on U.S. government and corporate computer networks.[30]

A number of Chinese companies aggressively employ intelligence collection methods that cross the line of propriety and legality, and some of them are also IP infringers. According to the U.S. Department of Justice, U.S. auto-parts manufacturer Metaldyne, one of only two corporations in the world capable of transforming powdered metal into high-performance engine components, was seriously damaged when one of its former engineers gave proprietary information to potential Chinese competitors. A Huawei employee illegally took photos of Fujitsu circuit boards at Supercomm in 2003; *Business Week* speculated that the employee may have also collected proprietary information from AT&T, Cisco, Lucent, Nortel, and Tellabs.[31] The U.S. software maker 3DGeo Development Inc. caught several trainees of the Chinese state-owned oil company Petro China Co. trying to access 3DGeo's secure computer systems; one was sentenced to two years in prison in 2004.[32] As a result of the increased incidents, the FBI decided in 2007 to identify the ten highest-value U.S. corporations (including General Electric,

DuPont and Corning) in the respective areas of the FBI's fifty-six field offices throughout America and brief those corporations on the threat.[33]

Chinese government research institutes are also actively involved in trade secret theft. The FBI and other U.S. government agencies recently identified about 150 individuals and businesses involved in illegally transferring aerospace and weapons technology to China and Iran; the espionage may have benefited Chinese government's space program.[34] Most notably, the FBI arrested physicist Shu Quan-sheng, the president of a National Air and Space Agency (NASA) subcontractor, for allegedly exporting restricted U.S. technology to China to assist the development of China's Long March V heavy booster. According to the federal claim, Shu allegedly transferred sensitive data on the components of a specialized cryogenic hydrogen tank to the People's Liberation Army's General Armaments Department and its 101st Research Institute. In a separate case, the U.S. Department of Justice (DOJ) reported in June 2008 that China's Naval Research Center acquired Quantum3D Inc.'s Mantis 1.5.5 and viXsen trade secrets – software programs used to simulate real world motion and train military fighter pilots – from Xiaodeng Sheldon Meng, a Chinese software engineer and former employee of Quantum3D Inc.[35]

STRATEGIC ROAD AHEAD: CHINESE CORPORATIONS MUST LEAD THE WAY

The late Professor Zheng Chengsi, father of IP in China and former director of the Intellectual Property Office of the Chinese Academy of Sciences (CAS), declared China's economic growth in the 21st Century will largely depend on its ability to manage intangible property and produce enterprises capable of successfully engaging in global IP competition.[36] Zheng's work at CAS persuaded the State Council to develop China's first *National Intellectual Property Strategy* – promulgated in June 2008 – and his intellectual imprint is reflected in the *Strategy's* emphasis on transforming the way companies create and acquire IP overseas.[37] Section 2 (12) of the *Strategy* emphasizes the importance of making the corporation "the principal entity in the creation and utilization of intellectual property." The *Strategy* also bears the mark of China's national security experts in that it calls upon government agencies and enterprises to make more effective use of IP for national defense and encourages the development and use of civilian IP for military purposes.[38]

The *Strategy* highlights the importance of improving China's capacity to create IP and Chinese-developed standards,[39] in which increased research and development (R&D) plays an integral role.[40] On this front, Beijing has been very successful in inducing most large U.S. high technology firms to invest heavily in R&D in China – largely in the form of high-technology R&D programs and centers in exchange for market access and financial incentives – which is gradually helping China close the gap between basic research and bringing inventions to market. In addition, U.S. R&D activities in China not only help Chinese subsidiaries improve their own R&D programs,[41] but could also indirectly help China's defense-modernization efforts.[42]

> [L]ocal Chinese employees working at foreign R&D centers may gain an in-depth understanding of how foreign technologies are developed and function. In some instances, R&D activity has included integrating foreign technology with local

> systems or making foreign technology compatible with Chinese technical standards. This latter form of knowledge transfer (systems and standards integration capabilities), in particular, could be of potential use to China's defense modernization goals, especially in developing asymmetric capabilities. For this and other reasons…extensive knowledge transfers through R&D in China could pose risks for long-term US security as well as economic interests. [43]

China spends heavily on R&D to improve China's capacity to rapidly absorb and adopt foreign technologies that can advance civilian and defense technology and IP development. According to the 2007 OECD report, China has become one of the most R&D intensive countries in the world, second only to the United States; China's R&D spending in 2007 surpassed Japan's for the first time. China's R&D spending could increase 24 percent in 2008 to $216.8 billion, which is roughly 18 percent of R&D spending worldwide.[44] China's total R&D spending in 2007 reached approximately $175 billion (an increase of nearly $155 billion in R&D spending since 2003). U.S. and Japanese spending during that same period totaled about $353 billion and $143.5 billion, respectively.[45] The European Commission recently assessed that, if China continues to increase its R&D spending at the current pace, China could match the EU in R&D expenditure as a percentage of GDP by 2009.[46] It is important to note, however, that government-sponsored R&D focuses primarily on applied research and technology development (the government used less than 6 percent of total R&D funding for basic research in 2002 and 2003).[47]

Chinese corporations are becoming the most important contributors to the R&D spending in China. According to the Research Institute of Industrial Economics and Orebro University in Sweden, Chinese companies conducted about 68 percent of China's total R&D in terms of spending in 2005, which highlights the dramatic shift from a government-centered to a corporate-dominated innovation system.[48]

Comparisons of China's R&D expenditures with developed countries do not account for the large disparities between China and the West in the quality and cost of research staff. As Dr. Xu Zhijun, chief marketing officer of the Chinese multinational telecommunications giant Huawei argues, because of China's low labor costs and access to high-quality researchers, Huawei may have spent only $1.1 billion in R&D last fiscal year, but that is equivalent to about $4 to $5 billion spent by western rivals such as Cisco.[49]

As suggested later in this article, the global economic downturn has important implications for Chinese corporate R&D programs. Chinese companies will have to make hard choices about R&D funding, and many of them will probably choose to focus exclusively on combining in-house R&D with imported technology to avoid the high costs and risks associated with basic and more innovative research. (This R&D strategy has been heavily used by legitimate companies and counterfeiters in the past for reverse engineering purposes).[50]

THE STRATEGIC VALUE OF COMPETITIVE INTELLIGENCE

Beijing's push to make IP the strategic imperative of government agencies and corporations, as manifested in the *Strategy*,[51] has had a significant impact on Chinese companies. Many Chinese executives, seeking to fulfill the government's desire that

their enterprises become the driving force behind China's technological innovation and IP creation, have established new competitive intelligence (CI) units or expanded their existing programs.[52] Chinese companies have reportedly intensified efforts to hire qualified Chinese CI personnel to fill a growing number of CI collection and analysis positions.[53]

Zhong Tianwei, the Guangzhou branch manager of Beijing TRS Information Technology Company,[54] notes that many domestic enterprises can attribute their successes to CI.[55] Competitive intelligence can help companies determine competitors' R&D capabilities, keep informed of competitors' product developments, assess competitors' product performance, design new technologies and products, assess a competitor's management strategies and decision-making capabilities, plan and manage R&D activities, create advanced S&T-based strategies, identify competitors interested in strategic alliances, and improve a company's capability to protect its intellectual property from illegal human and technical collection.[56]

The Mandarins' Perspective on Competitive Intelligence

Chinese government officials, scholars, and business strategists have written extensively about CI and recognize how it can help China (as it did Japan) achieve its IP goals and eventually become an economic superpower.[57] China's vigorous promotion of CI, and its subset competitive technical intelligence (CTI), have helped make these important topics of concern in China.[58] The Chinese Ministry of Ordnance Industry's Intelligence Research Institute, National Defense Science and Industry Scientific and Technical Intelligence Bureau, and the State Science and Technology Commission initiated a study comparing domestic and foreign intelligence research and held a series of seminars on strategic intelligence research and development from 1991 to 1994, resulting in a change in the direction of Chinese intelligence research work: competitive intelligence became its new focal point.[59]

Since the mid-1990s, a growing number of Chinese PhD dissertations have focused on CI and the use of intelligence to advance China's national interests.[60] Many of these students have gone on to become influential in business, government, and academia, and have helped push the theoretical development of corporate intelligence in China. Dr. Chen Feng, for example, who received his PhD from Beijing University and wrote his dissertation on CI in China with the assistance of his advisor Liang Zhanping, director of China's Institute of Information Science and Technology, is now a CAS associate researcher and senior consultant to Ding Lu Management Consultants, Ltd. and has advised Chinese high-technology firms how to set up CI programs.[61]

U.S. and Chinese scholars have provided a myriad of definitions of CI and CTI. Corporate CI can generally be defined as activity related to the collection, processing, exploitation, analysis, and dissemination of information and finished intelligence on corporate competitors and pertinent industries that could impact a firm's competitive situation. How narrowly or broadly a corporation defines the term depends on the company's mission and the goals of its intelligence programs; generally, more resources and funding are required to meet intelligence goals that are broader in scope. W. Bradford Ashton of Pacific Northwest National Laboratory and Richard Klavans of the Center for Research Planning define CTI as "business sensitive information on external

scientific or technological threats, opportunities, or developments that have the potential to affect a company's competitive situation."[62]

Chinese scholars have generally accepted the above definitions, but have added caveats of their own. Chinese and U.S. scholars also agree that corporate intelligence does not and should not include unethical or illegal forms of intelligence collection, such as unauthorized monitoring of phone and internet communications, trade secret theft, etc. However, some Chinese scholars concede that a gray area exists in CI, where reverse engineering and IP transfer may take place without necessarily breaking the law and the benefit to public interest may override the ethical considerations.[63]

Chinese academics point out that company intelligence efforts are necessarily proprietary and need to be protected. The company's sources and methods of collecting, processing, and analyzing information, and the intelligence derived from such activities, is confidential and usually well-guarded because unauthorized disclosure could negatively impact the company's competitive position. This is primarily why Chinese companies are so interested in "anti-competitive intelligence" (also referred to as counterintelligence) programs: to help protect against IP loss in the "gray area." This is discussed with some frequency in the Chinese literature.[64] (As will be suggested later in this article, U.S. companies could also benefit from increased emphasis on counterintelligence programs.)

Chinese Competitive Intelligence in Practice

Chinese corporate intelligence in practice can differ substantially from how it is described in scholarly works. Although Chinese scholars stress that corporate intelligence programs must employ ethical and legal intelligence techniques and methods to produce intelligence, mounting evidence suggests Chinese firms are increasingly using their intelligence units to enhance the effectiveness of their illegal activities. Chinese espionage cases involving IP theft from U.S. companies since 2007 indicate the emphasis China places on illegal corporate intelligence, the great risks China is willing to take to acquire U.S. IP, and the disregard it has for the global IP system (note that the Chinese government denies any illegal conduct).

As discussed, Chinese executives and managers hope to transform their companies into global competitors (86 percent of Chinese executives interviewed for a McKinsey survey in 2008 indicated they had global ambitions). They view the development of corporate intelligence programs as a means to improve strategic management and help identify struggling U.S. firms to purchase. This ambition can drive them to turn otherwise ethical CI programs into illegal collection platforms. 'The Chinese are out to develop a modern economy and society in one generation,' notes Joel Brenner. 'There is much about their determination that is admirable. But they're also willing to steal a lot of proprietary information to do it, and that's not admirable.[65]

The most robust Chinese corporate intelligence units are likely located in R&D centers overseas (often called "listening posts"), where the company can most effectively collect intelligence from its competitors and leverage the deep expertise of its many high-quality and relatively low-cost scientists and engineers to analyze and evaluate the technology and IP the company purchases or steals.[66] The Chinese literature suggests the intelligence units' internal processes are generally similar to those described in some of the most prominent works on corporate intelligence in the west.[67] The organization of

some of the units may differ somewhat from those in the West, but they likely combine personnel with formal intelligence training and those who are experts in their given technical or scientific fields to conduct intelligence collection, processing and exploitation, analysis, production, and dissemination.[68] Personnel assigned to listening posts can use their legal collection and analysis of patents, standards, business and market data, and information to inform illegal collection activities and vice-versa. They can also rely on scientific and technical assistance from their company headquarters, some of which are located in high-technology science parks in China and so have direct access to world-class government research institutes and universities (many of which employ scientists, engineers and academicians who have undoubtedly developed a corpus of useful knowledge and techniques related to obtaining proprietary and classified information from U.S. corporate and government laboratories).[69, 70]

These listening posts – some of which may receive Chinese government intelligence and military financial support and collection guidance[71] – may also employ illegal technical collection techniques (such as hacking) in the United States to obtain proprietary information from key U.S. competitors. Brenner claims Chinese hackers, on behalf of a Chinese corporation, hacked into "a large American company" to obtain sensitive company information prior to an impending business negotiation between the U.S. and Chinese companies. In a *National Journal* article, Brenner recounted the following incident: "The [U.S. business] delegation gets to China and realizes, 'These guys on the other side of the table know every bottom line on every significant negotiating point.' They had to have got this by hacking into [the company's] systems."[72]

Chinese illegal technical collection threatens U.S. corporate facilities worldwide and puts U.S. R&D centers operating in China at risk. In late 2007, Jonathan Evans, the director general of Britain's domestic intelligence agency MI5, warned 300 firms operating in the UK of growing evidence that state-sponsored Chinese hackers were attacking corporate networks and stealing proprietary information.[73] Although U.S. technology firms likely have physical and operational security procedures in place in their facilities inside China, they are probably no match for China's corporate and government intelligence services – among the most effective in human and technical intelligence collection in the world.[74] Microsoft Corporation, which intends to invest one billion dollars in China R&D over the next three years, will undoubtedly be a target for domestic Chinese competitors.

RETHINKING THE INTELLIGENCE PARADIGM

Roger George, senior analyst at the CIA's Global Futures Partnership, argues the traditional intelligence paradigm, which was relatively successful in dealing with state-centric problems, is less effective at collecting and analyzing global and transnational phenomena. These emerging challenges are 'blind spots' that are difficult for analysts operating under traditional organizational and functional constraints to identify and understand.[75] The global character of Chinese corporate espionage challenges the effectiveness of traditional U.S. intelligence and law enforcement efforts.[76] An analysis of recent studies and press reports also suggests the U.S. IC and law enforcement communities still lack sufficient resources and expertise to effectively collect and

analyze data and information on Chinese espionage activities directed against U.S. companies worldwide.

Although the *Cox Report* was written a decade ago, many of its findings are relevant today. The report acknowledges the U.S. government cannot "completely monitor PRC activities in the United States" because of the scope of China's "decentralized collection efforts."[77] According to the report, the CIA, Department of Commerce, FBI, and DoD never considered Chinese technology acquisition an intelligence priority. They failed to establish collection requirements to obtain information on Chinese government or commercial efforts to acquire U.S. technology companies, identify and obtain advances in U.S. technology, or establish business relationships with U.S. high-technology companies. Nor did U.S. agencies establish requirements to examine commercial affiliations between Chinese foreign nationals and U.S. companies.[78] The Select Committee of the U.S. House of Representatives determined U.S. government agencies only conducted "narrow" or "reactive" monitoring of Chinese business activities rather than taking more proactive measures.[79] "[T]here is little or no coordination," states the report, "within the U.S. Government of counterintelligence that is conducted against the PRC-directed efforts to acquire sensitive U.S. technology."[80]

The IC's scientific and technical (S&T) intelligence framework – an outgrowth of the Cold War which largely collects and analyzes key S&T data and information within a classified system[81] to understand foreign weapons platforms and identify emerging S&T threats,[82] remains ill-suited to adequately handle evolving Chinese corporate espionage focused on IP theft and infringement. Under this S&T paradigm, Chinese CI would not likely be considered relevant for S&T collection and analysis (the IC would probably view it as a business or management issue) and IP would be treated primarily as an economic, legal, and trade-related matter. Chinese academics, government, and industry, however, encourage greater collaboration between government and industry intelligence programs[83] and largely view S&T and IP as inseparable, whether from an intelligence or economic perspective.

Dr. Rob Johnston, in his 2005 study on analytic culture in the IC, suggests there is a separation of the domains of S&T and economic intelligence and expertise within the analytic community.[84] To the extent that situation now exists and is not mitigated through collaboration, some S&T and economic analysts, who are looking at data and information from the perspective of their areas of focus and expertise, may overlook critical IP and R&D data and information that directly impacts analytic judgments on S&T developments in China.[85] An economic analyst who has spent a career learning the tenets of economic analysis may not understand how unique IP and R&D data and information could inform S&T intelligence analysis,[86] or consider how Chinese corporate intelligence impacts trade and innovation. If such issues are not overlooked, they would probably fall under the purview of analysts working on transnational matters; those analysts may or may not have extensive scientific, technical, or economic expertise, or even speak Chinese (RAND suggests the IC's expertise and focus on S&T analysis and the assessment of foreign R&D programs has decreased).[87] [88]

The lines between Chinese intelligence, military, and commercial activities are not truly 'blurred.' The blurring of the lines cited in the *Cox Report*[89] demonstrates how the IC has tried to apply a Western construct to understanding Chinese business and intelligence practices. As suggested from the evidence in previous sections of this article,

there are no strict legal lines separating Chinese intelligence activities from the corporate world as exist in the United States. Chinese corporations are always subject to extensive government influence and control, and many companies prefer having close links to the government for protection and access to resources and information that can give them a competitive advantage.

The barrier the IC has created between S&T and IP could create an imbalance in the allocation of resources and funding for collection and analysis of the issues. This could influence which U.S. agencies handle certain requirements and how IC offices are organized and staffed to deal with particular analytic problem sets; it could hinder collaboration and increase analytic error.[90]

The IC lists its intelligence collection priorities in the National Intelligence Priorities Requirements Framework (NIPF), which emphasizes about twelve priority intelligence targets, countries, or issues out of 150, according to a 2008 study by the RAND Corporation.[91] The NIPF ranking of the relative importance of these priorities affects government resource allocations and those of the most critical importance to the country receive more funding for collection and analysis.[92] The RAND study characterizes priorities such as terrorism, WMD proliferation (an S&T intelligence issue) and China as NIPF "crosscutting problems or theme-areas."[93] The study points out the "NIPF has great value for many uses, but it also provides an incentive to reduce spending resources on all but the hottest current priorities, often at the expense of deeper assessments of longer-term challenges."[94]

Many U.S. policymakers tend to look to organizations such as the Department of State, DOJ, and the U.S. Patent and Trademark office for expertise on IP and other IP-related issues. Trade secret theft – one area of IP most often discussed in the intelligence context – is largely seen as the purview of agencies dealing with domestic counterintelligence matters, such as the FBI.[95] Because of this, some other IC agencies, which are in the position to assist the FBI, might not be doing so because of cultural or institutional barriers.

It is also difficult for the U.S. government to impress upon companies the seriousness of the threat and persuade them to respond appropriately. Some U.S. corporations might be unwilling to assist the FBI or Department of Homeland Security (DHS) – for example, by revealing the fact a Chinese corporation has stolen proprietary information through human or technical intelligence collection methods – to avoid potentially negative repercussions for their business interests in China or damage to shareholder confidence.[96]

There are also indications that U.S. companies are still not taking the Chinese seriously. A recent McKinsey survey suggests that while U.S. executives view Chinese corporations as a significant threat, few (28% of respondents) have taken sufficient steps to counter the threat because of a perception that Chinese firms are relatively weak in product quality, marketing, and brand development. The report observes: "This lackluster reaction to the global ambitions of Chinese companies raises the question of whether business executives elsewhere are setting themselves up for some unhappy competitive surprises."[97]

THE COMING STORM

Chinese leaders have made it clear that they want to reinvent China's role in the world economy and move from dependence on foreign technology and direct investment to a country that rivals the United States in terms of industrial and technological power. They recognize that this requires promoting and rewarding scientific discovery and true innovation, increasing IP ownership, developing new technology standards, and making it possible for Chinese corporations to play an even greater role in foreign technology acquisition and IP transfer. China has made considerable advances in developing favorable national and local S&T, IP, and business policies, and has increased its emphasis on education and R&D.

Chinese companies have shown they can effectively absorb and adopt U.S. technology and IP to push innovation. According to Curtis Carlson and William Wilmot of SRI International, the company that pioneered innovations such as the computer mouse and robotic surgery, China is working with preeminent partners around the globe to create the future technologies, attaining parity with the United States in some areas such as nanotechnology.[98] Along these lines, Frans van Houten, CEO of the European semiconductor company NXP, states China is now home to about 400 semiconductor firms that design chips and some of these companies will rapidly become top-notch innovators.[99] Motorcycle suppliers, designers, and manufacturers, in Chongqing, China, have collaborated to develop a unique entrepreneurial network and business model called 'localized modularization', which allows manufacturers to request parts from suppliers without specifying details; i.e., makers note the size and weight of the parts in their orders and suppliers decide what parts to provide. This push to innovate is contributing to the rapid expansion of China's patent system: Chinese domestic patent applications grew from 165,773 in 2001 to 470,342 in 2006.[100]

Some observers are very optimistic about China's largely untapped capacity to innovate. The National Science Foundation estimates China could graduate about four-times more engineering PhDs than America in the next several years. Based on their observations of the work of Chinese scientists, engineers, and researchers, Carlson and Wilmot believe the Chinese are just as creative as their Western counterparts; there is ample evidence of creativity and entrepreneurial ambition in Chinese firms.[101] Many Chinese engineers and scientists who received their PhDs in the United States, some of whom played important roles in successful innovations in U.S. high-tech firms, are now returning to China.[102]

At the same time, Chinese industrial espionage and IP misappropriation, often done with the support or knowledge of the government, shows China is also willing to disregard the traditional rules of the game when convenient and take great risks to acquire U.S. government secrets and corporate proprietary information to the detriment of U.S. national security. As demonstrated earlier, a number of the most well-known and powerful Chinese corporations actively engage in IP misappropriation, theft, and reverse engineering and solicit IP transfer from their foreign competitors' former employees. To date, intense U.S. corporate and government pressure on the Chinese government to improve the enforcement of IP rights has had limited results. Clearly, the blowback for Chinese espionage has not been severe enough for some Chinese companies to stop their illegal activities.

Against this backdrop, one wonders how long U.S. technology firms – despite their current comparative advantage in S&T and IP – will be able to withstand Chinese competition. Many U.S. scholars and business leaders might argue that most U.S. firms will not succumb to Chinese competitive pressure until China improves its capability to innovate and strengthen its IP base vis-à-vis the United States. This could take several decades at a minimum. However, some of these same U.S. observers (perhaps due to bias, mirror imaging, apathy or hubris) fail to take seriously a question that weighs heavily on the minds of many Chinese executives with global aspirations and government leaders who want to turn China into a superpower: "How can we further improve the effectiveness of our CI programs, whether it be through legal or illegal means, to continue to close the IP gap with U.S. companies?"

ECONOMIC DOWNTURN CREATES OPPORTUNITIES

The global economic crisis is having a major impact on Chinese companies and trade. Chinese President Hu Jintao recently told members of the Communist Party that the global economic downturn is hurting China's competitive advantage in trade and threatens Party legitimacy and ability to rule.[103] Chinese leaders are growing increasingly concerned that the economic crisis, which has significantly reduced demand for Chinese exports and played a major role in the collapse of over 68,000 small Chinese companies, will leave millions of workers unemployed and lead to widespread domestic unrest.[104]

As the situation worsens, the pressure for Huawei and other MNCs to gain a competitive edge over U.S. and European competitors grows. Huawei's CEO called on his employees in July to prepare "psychologically" for the impending downturn; employees must work in "crisis mode" to ensure growth and innovation.[105] The pressure of working for Huawei is well-known in China, and employee depression and suicides have been on the rise this year, according to Chinese press reports. A Huawei employee, speaking on condition of anonymity, said that overtime is part of employee evaluations and the corporate culture encourages overtime to shorten product cycles and remain competitive vis-à-vis international giants.[106]

Huawei and some other large Chinese companies view the crisis as an opportunity to invest in the United States and acquire Western IP at an excellent value.[107] Recent press reports, for example, suggest Huawei will continue to expand in the U.S. market in 2009.[108] China Mobile Ltd. also intends to set up its first R&D center outside of China (in California's Silicon Valley in 2009) to assist its work on Internet and telecommunications integration. Donald Straszheim, an economist and vice chair of Roth Capital Partners, which has handled the financing of Chinese companies, states: "In the global recession, Chinese companies are looking around the world to acquire knowledge."[109] Chinese employees of Frog Design, a consulting firm that develops innovative products for Fortune 500 companies, take the following view of the crisis:

> In China, the rule of the game is always "Stay One Step Ahead of Your Competitors"…[W]hen Chinese businesses run out of initiatives in which to invest their capital or when their investments stop…they make a concerted effort to…invest in research and development. In fact, senior executives in some companies have said publicly that in the near future they would either invest in

> their own health and personal happiness, or they would increase R&D budgets in their businesses to invest in better products to prepare for a new run when the downturn ends…This puts a premium on vision and strategic planning instead of short-term financial risk taking.[110]

Some companies, which lack funds for R&D because of the credit crunch, may simply decide to engage in IP theft to maintain an edge over competitors. Michael Kump, a lawyer specializing in IP law, contends:

> As economic conditions tighten and people start looking for ways to cut corners and gain an advantage, some will cross the line…in an illegal manner. One of the classic shortcuts is to steal competitors' intellectual property. It can be quicker to target key employees at a successful competitor and try to get those employees to come over to your side than to invest in process and grow your business the right way.[111]

PriceWaterhouseCoopers notes that established Chinese companies can greatly benefit from employee IP transfer; former U.S. technical specialists can receive financial support to establish start-up companies that rely on the proprietary knowledge obtained from their U.S. employers.[112]

As the global economy continues to weaken, Chinese corporations will likely seek to expand their CI and R&D activities in the United States to increase productivity and improve their competitive positions. This growth will include acquiring struggling U.S. technology firms or their R&D centers, which could result in windfall IP transfers to Chinese firms. Jin Chen, a professor at Zhejiang University, asserts that Holly, a Chinese conglomerate, used its wholly-owned subsidiary in the U.S. to identify and acquire the Code-Division Multiple Access R&D unit from Phillips Electronics, which gave Holly rights to all IP at the facilities and many experienced engineers. The acquisition allowed Holly to improve its mobile telephone chip designs and position in the Chinese telecommunications market.[113] Other notable examples include Lenovo's purchase of IBM's personal-computer business, the Shanghai Automotive Industry Corporation acquisition of Rover technology to create the Roewe brand,[114] and Huawei's purchase of Marconi to tap European markets and relationships with local carriers.[115]

The list of high technology companies that are reducing their technical staff is growing. Sun Microsystems Inc. announced in early November 2008 that it would lay off about 6,000 employees. Teradyne Inc., the leading maker of microchip test equipment, stated it would release about 185 workers worldwide. National Semiconductor Corp., which makes chips, decided to lay off 330 employees and Applied Materials Inc., a manufacturer of chip equipment, announced it would cut 1,800 positions.[116] Some Chinese companies may increase efforts to hire recently laid-off employees of U.S. high technology firms, which could be a growing source of IP transfer.[117]

RECOMMENDATIONS

The following recommendations are provided for the consideration of the U.S. government:

Take Steps to Encourage the Chinese Government and Industry to Stop Illegal Industrial Espionage and Large-Scale Intellectual Property Theft

Thus far, complaints from the U.S. government and industry to stop this illegal behavior have either been met with Chinese government denials, abject disregard, or half-hearted enforcement efforts. Although U.S.-China trade agreements have had some success in curbing IP infringement, U.S. IP industries claim Chinese IP infringement is still occurring at unacceptable levels. It would be neither fair nor accurate to attribute all industrial espionage and IP misappropriation to the Chinese government, or state that all Chinese firms are engaged in this sort of behavior. However, the mounting evidence of Chinese illegal activities is creating a dark cloud of mistrust regarding Chinese business practices that fuels the more pessimistic views of Beijing's plans and intentions.

U.S. government representatives should impress upon their Chinese counterparts that this behavior could have a long-term negative impact on U.S. public perception of China. In addition, given the level of Chinese industrial espionage, the U.S. government should consider enacting laws that would impose more severe sanctions on Chinese companies whose employees are caught stealing U.S. technology and IP.

Closely Review Proposals of Chinese Companies to Purchase R&D Centers of U.S. High-Technology Companies

Huawei proposed to purchase its U.S. competitor 3Com last year, which would have given it access to technology supplied to the Pentagon.[118] Although this was clearly a case in which national security interests were at stake, a closer examination of future high-technology purchase proposals may reveal security implications that are not quite so obvious.

Make CI a New Strategic Theme in the IC

The IC should consider designating CI as a new 'strategic research theme' to help identify and monitor new trends in foreign intelligence that could impact homeland security.[119] China has made CI the center of its intelligence studies and, as mentioned, this is having an impact on Chinese government intelligence research. CI exerts an important influence on the evolution of intelligence programs in other countries as well. In France, for example, CI "involves all levels of government, numerous support organizations from the private and public sectors as well as public private partnerships and quasi-governmental organizations, like the Chamber of Commerce and Industry…or the Agency for the Diffusion of Information and Technology."[120]

Develop Programs on IP and CI at U.S. Government Civilian and Military Colleges and Universities

The extensive Chinese literature on CI has provided a window into a side of China that one is otherwise hard-pressed to find: a detailed discussion of Chinese government intelligence and counterintelligence operations. CI gave the Chinese a vehicle through which they could once again openly discuss intelligence and operations within the politically safe context of international business. At the same time, U.S. literature and understanding on the subject is relatively inadequate, with few books having been written on the subject of Chinese intelligence operations. Against this backdrop, the U.S. government should develop courses and sub-discipline programs at government civilian

and military colleges and universities to train and educate students and professionals in IP and CI matters.

Devote More Funding to Collection and Analysis

As part of this effort, the IC should devote more resources and funding to collection and analysis of the Chinese S&T and IP collection issues. As S&T intelligence requirements are part of the NIPF (National Intelligence Priorities Requirements Framework), according to the RAND report IP requirements should be combined with S&T requirements and ranked among the 'hottest priorities.' The IC should also require Chinese S&T analysts to obtain a deeper understanding IP issues and the development of Chinese language skills. S&T analysts who do not have S&T backgrounds should be required to obtain formal training and education in critical S&T areas.

The IC also needs more intelligence officers to devote to the problem. Despite the rapid increase in cyber security incidents and illegal technology transfer activities in America, the number of officers available to handle these cases remains limited. For example, the number of FBI agents assigned to handle Chinese spying activities in the United States has only risen from 150 in 2001 to 350 in 2007.[121]

Develop a Cadre of Analysts, Scientists, and Technical Personnel with Chinese Language Proficiency

The IC also requires more S&T analysts fluent in Chinese. As suggested in some of the declassified National Intelligence Estimates (NIE) on China (from 1949 to 1976), the IC had difficulty assessing the strategic objectives, military, and scientific and technical capabilities of China because the IC lacked collection in some areas and was forced to rely on Chinese press reporting.[122] Given China's intense secrecy today, IC China analysts are perhaps forced to rely on Chinese open source material more than analysts focusing on other foreign countries.[123]

Unfortunately, only a limited number of IC analysts can read Chinese; translating scientific and technical Chinese documents requires specialized skill. More China analysts must develop the capability to read and understand scientific and technical Chinese. Developing this skill is especially crucial for today's S&T analysts because of the great strides China is making in S&T and R&D (many key Chinese S&T documents and books have only been published in Chinese).

The following recommendations are provided for the consideration of U.S. corporations:

Establish or Strengthen Competitive Intelligence Programs

U.S. corporate executives and managers also need to develop or strengthen intelligence and counterintelligence programs in their companies. Some Chinese companies are outperforming their U.S. competitors in this area, and their successes can provide useful lessons for U.S. companies doing business with China. The consensus in the Chinese literature on CI is that training and education is essential for a successful CI program.[124] Although U.S. companies also understand this is important, they lag far behind some Chinese companies in CI training and education. For example, while DuPont employees are required to complete online training regarding insider risks,[125] employees in some Chinese companies are obtaining their doctorates in CI.[126]

Consider Sending Employees to Outside Competitive Intelligence Training Courses

Company employees could learn a great deal about CI matters by attending outside CI training courses in China and the United States. Chinese companies send employees to CI courses held in various cities in China. The Chinese Business Training Network (CBTN) offers CI courses in China almost monthly. The course syllabus covers the following selected topics: goals of intelligence and competitive intelligence collection; using intelligence analysis and production methods; preventing disclosure of proprietary information during company visits; developing insiders in competitors' companies; creation of social networks to find and recruit key IT personnel; creating CI units within the company; establishing clear lines of communication and support with other departments; protecting trade secrets; identifying and neutralizing intelligence threats; and case studies on real espionage cases and lessons learned (including case studies based on traditional CIA espionage operations and Chinese corporate counterintelligence investigations).[127]

Increase Collaboration with Government Agencies and Heed Government Warnings

Although the FBI and DHS have set up official groups within which U.S. companies can confidentially reveal their computer network vulnerabilities to the government,[128] some companies remain loath to do so, for reasons mentioned previously. The *National Journal's* recent article on Chinese hacking also suggests that some U.S. companies view government warnings as alarmist hyperbole.[129]

Strengthen Protection of Sensitive Data and Consider the Long-term Risks Associated with Lay-Offs of Employees with Knowledge of Critical Proprietary Information

As high-technology corporations increase employee lay-offs, they must take steps to ensure their sensitive data is well protected. Current information storage technologies, such as USB drives and other devices, have facilitated the ability of employees to take vast amounts of proprietary information to a company's competitors.[130] Cadence Design Systems, a software company, developed standard operating procedures – consisting of strict access and document controls, enterprise rights management and compartmentalization – to control the unauthorized release of such proprietary information. Cadence also employs modular software development procedures to compartmentalize information when conducting R&D in developing countries.[131] However, the potential problem with such a method is that all of the money and effort put into its design can be lost if only one trusted employee with access to the right proprietary data departs the company and works for a competitor. Many U.S. high-technology corporations, with the sole aim of cutting costs, often release employees without even assessing how they could damage compartmentalization efforts and long-term market position.

CONCLUSION

The U.S.-China Economic Security and Review Commission warns in its 2007 annual report that, as U.S. companies continue to develop new technologies in hundreds of high-tech factories and joint R&D facilities in China, Chinese espionage poses the most significant threat to U.S. technology. If the U.S. government and industry cannot adequately control Chinese espionage in America, they certainly cannot expect to stop massive IP infringement and theft from U.S. R&D centers and other facilities located in China. Although U.S. IP industries can continue to push for stronger legislation (in both America and China) that would increase the penalties for Chinese companies and individuals involved in espionage, they must take steps to protect their intangible property to maintain their competitive positions worldwide.

China's large-scale infringement and theft of IP hurts the U.S. economy and, at the same time, helps advance Chinese science and technology, improve new weapons systems, and develop new products and processes. If America cannot do better at curbing these activities, then it becomes imperative for the IC to develop more robust methods of following Chinese S&T developments and informing policymakers of their potential ramifications. As U.S. preeminence in S&T and IP begins to wane, the importance of tracking and understanding emerging trends – such as CI in China – grows. Left unchecked, Chinese illegal forms of intelligence collection will enhance China's corporate intelligence programs and competitive advantage to the detriment of U.S. corporations and the U.S. economy.

China must strengthen efforts to cooperate with the United States on stopping such illegal activities, which greatly damage China's image and could push American public opinion toward protectionism or economic retaliation during an extended economic downturn.[132] As the cases of contaminated Chinese food products and toys demonstrate, the short term economic benefits of unscrupulous and illegal behavior is not worth the long-term damage to the image of Chinese corporations and their business practices in the United States. The majority of ethical Chinese businessmen and laborers have worked too hard over the last several decades to watch their many successes become tarnished by the refusal of the Chinese government and unscrupulous corporations to admit and stop such wrongdoing.

Robert Slate is a lead systems engineer at the MITRE Corporation. He formerly served as a captain in the U.S. Army and faculty member at the National Defense Intelligence College, Post-Graduate Intelligence Program-Reserves. Prior to obtaining his Juris Doctorate, he received his master's degree from the Fletcher School of Law and Diplomacy and bachelor's from Oberlin College. Slate is currently pursuing his PhD in environmental science. He has previously published articles on U.S. intelligence and Chinese military, strategy, and legal issues. Mr. Slate may be contacted at rbslate@gmail.edu.

---

† The views express in this manuscript are the author's and do not reflect the official position of the MITRE Corporation or imply endorsement by the Office of the Director of National Intelligence or any other U.S. government agency. The author's affiliation with MITRE is provided for identification only. It does not convey or imply MITRE's concurrence with, or support for, his positions, opinions, or viewpoints.

[1]China Business Training Network (CBTN), *Competitive Intelligence Gathering and Trade Secret Protection Practices* (Shanghai, China, 2008), http://hk.top.sh/main/detail.net?IDTradeInfo=21554. [Hereafter cited as *Trade Secret Protection*.]

[2] "Competition from China: Two McKinsey Surveys," *The McKinsey Quarterly* (2008): 8. [Hereafter cited as "Two Mckinsey Surveys"]; The National Counterintelligence Executive's 2005 report holds: "Foreign governments and intelligence organizations have created quasi-official organizations to enable them to capitalize on the private-sector technology theft that is underway. Indeed, the CI Community believes that foreign governments are major beneficiaries of the private-sector technology flow…To elicit sensitive information from those attending these quasi-official organizations, government officials may appeal to the professional egos of the private sector contacts, to their patriotism, or to their commercial sensibilities, by offering domestic business deals to accomplish technology transfer. Coercion is also an option in countries like Russia and China, where security services still hold considerable sway over the private sector." National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (2005)*, (Washington, DC: National Counterintelligence Executive, 2006), 6. [Hereafter cited as *Collection and Industrial Espionage*.]

[3] The Office of the Director of National Intelligence (DNI) states human intelligence collection "is performed by overt collectors such as diplomats and military attaches… [and] includes clandestine acquisition of photography, documents, and other material; overt collection by personnel in diplomatic and consular posts; debriefing of foreign nationals and U.S. citizens who travel abroad; and official contacts with foreign governments." See Official Website, Office of the Director of National Intelligence, http://www.dni.gov/what_collection.htm.

[4] Wesley Wark suggests some methods of technical collection, such as "line-tapping, bugging, outputs from remote sensors, computer hacking (and) perhaps 'deep mining' of the Internet" can be difficult to neatly place in any single-intelligence agency category. Wesley Wark, *Twenty-First Century Intelligence* (Oxford, UK: Routledge, 2005), 53. Technical collection generally refers to signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT) and geospatial intelligence (GEOINT). According to the DNI, SIGINT "is derived from signal intercepts comprising – however transmitted – either individually or in combination: all communications intelligence (COMINT); electronic intelligence (ELINT); (and) foreign instrumentation (FISINT). Ibid. For the purposes of this paper, "illegal" technical collection primarily refers to illegal SIGINT and computer hacking.

[5] Joby Warrick and Carrie Johnson, "Chinese Spy 'Slept' in U.S. for 2 Decades," *The Washington Post,* April 3, 2008. [Hereafter cited as *Decades*.]

[6] See, for example, Wang Qi, "Business Competition and Competitive Intelligence," [*Qiye Jingzheng yu Jingzheng Qingbao*] *Military Dual-Use Technology and Products* (2002); "A Chinese Website advertising a technology exhibit in April 2006 in Chongqing, China, highlights the emphasis Beijing places on facilitating the transfer of technology from civil to military uses. According to the Website, the exhibit has three objectives: breaking down the barriers to sharing technology among industries, bureaucratic entities, and state and private sectors; facilitating coordinated development between the civilian hi-tech sector and the military; serving as a technology-exchange platform for civilian and military technologies." *Collection and Industrial Espionage, supra* note 2, 5.

[7] Christopher Bellavita, in his article "Changing Homeland Security: Shape Patterns, Not Programs," *Homeland Security Affairs* II, No.3 (October 2006), notes the majority of homeland security policy matters are overly "undefined…broad…(and) complex." [Hereafter cited as *Shape Patterns*.]

[8] Li Yingzhou et al., *A Summary of Nearly a Decade of Competitive Intelligence Research in China* [*Jin Shi Nian Wo Guo Jingzheng Qingbao Yanjiu Zengshu*] (Jan. 1, 2007) http://www.zoomchina.cn/content/view/45/97/1_0.html. [Hereafter cited as *Decade of CI*.]

[9] Jamie Smith and Leila Kossou, "The Emergence and Uniqueness of Competitive Intelligence in France," *Journal of Competitive Intelligence and Management*, No. 4.3 (2008): 65. [Hereafter cited as *CI in France*.]

[10] Loius Le Comte, *Memoirs and Observations Typographical, Physical, Mathematical, Mechanical, Natural, Civil, and Ecclesiastical, Made in a Late Journey through the Empire of China, and Published in Several Letters*, Printed for Benj. Tooke at the Middle Temple Gate, and Sam. Buckley at the Dolphin over against St. Dunstans Church in Fleetstreet (London, 1697), 238-239. [Hereafter cited as *Memoirs*.]

[11] Over the past sixteen years, foreign direct investment in China has reached almost a half-trillion dollars; China's annual economic growth rate has routinely topped upwards of 8 percent, and some years it has approached 10 percent. David Lei, "Outsourcing and China's Rising Economic Power," *Orbis: A Journal of World Affairs* 51, No. 1 (2007).

[12] See, for example, David D. Hale and Lyric Hughes Hale, "Reconsidering Revaluation: The Wrong Approach to the U.S.-Chinese Trade Imbalance," *Foreign Affairs* (Jan/Feb 2008): 57; Felix K. Chang and Jonathan Goldman, "Deterring the Debt Weapon," *The American Interest* 3, No. 5 (May/June 2008): 86-87.

[13] *Global Intangible Tracker 2006: An Annual Review of the World's Intangible Value* (December 2006), http://www.brandfinance.com/Uploads/pdfs/Global%20Intangible%20Tracker%202006.pdf.

[14] *Global Intangible Tracker 2007: An Annual Review of the World's Intangible Value* (December 2007), http://www.brandfinance.com/Uploads/pdfs/BF_GIT_07_REPORT_Final%20Version%20Low%20Res.pdf.

[15] *The Invisible Business,* http://www.brandfinance.com/Uploads/pdfs/Invisible%20business.pdf.

[16] Robert Slate, "China's National Intellectual Property Strategy: Implications for U.S. National Security," *Defense Intelligence Journal* 16, No. 2 (2007): 31. [Hereafter cited as *Implications*.]

[17]"IIPA's New Economic Study Reveals the Copyright Industries Remain a Driving Force in the U.S. Economy," January 30, 2007, http://www.iipa.com/pdf/IIPA2006CopyrightIndustriesReportPressReleaseFINAL01292007.pdf.

[18] See *Memoirs*, supra note 10, 238-239.

[19] Ibid., 238.

[20] *Redefining Intellectual Property Value: The Case of China* (PriceWaterhouseCoopers, 2005), 31. [Hereafter cited as *Case of China.*]

[21] Ibid.

[22] "FBI: China May Use Counterfeit Cisco Routers to Penetrate U.S. Networks," *WorldTribune.com,* May 15, 2008, http://www.worldtribune.com/worldtribune/WTAR/2008/ea_china0141_05_15.asp. See also, Brian Grow, et al., "Dangerous Fakes: How Counterfeit, Defective Computer Components from China are Getting into U.S. Warplanes and Ships," *Business Week,* October 13, 2008, 036. [Hereafter cited as *Dangerous Fakes*.]

[23] Ibid.

[24] *Dangerous Fakes*, *supra* note 22, p. 035.

[25]*Decades*, *supra* note 5.

[26] Brian Grow, Keith Epstein, and Chi-Chu Tschang, "The New E-Spionage Threat: A BusinessWeek Probe of Rising Attacks on America's Most Sensitive Computer Networks Uncovers Startling Security Gaps," *Business Week,* April 21, 2008, p. 034. [Hereafter cited as *E-Spionage*.]

[27] Ibid., 035.

[28] Ibid., p. 033.

[29] According to the *National Journal*, the Chinese government and military employs computer hackers to steal government secrets and corporate proprietary information. Shane Harris, "China's Cyber-Militia:

Chinese Hackers Pose a Clear and Present Danger to U.S. Government and Private-Sector Computer Networks and May Be Responsible for Two Major U.S. Power Blackouts," *National Journal Magazine* 31 (May 2008), http://www.nationaljournal.com/njmagazine/print_friendly.php?ID=cs_20080531_6948. [Hereafter cited as *Cyber-Militia*.]

[30] *E-spionage*, *supra* note 26, 040.

[31] *Case of China, supra* note 20.

[32] *Implications*, *supra* note 16, 43-48.

[33] David J. Lynch, "FBI Goes on Offensive Against China's Tech Spies," *USA Today,* July 7, 2007, http://www.usatoday.com/money/world/2007-07-23-china-spy-2_N.htm. [Hereafter cited as *FBI Offensive*.]

[34] Craig Covault and James Ott, "Caught in the Net: Justice Dept. Implicates Iran, China Contacts in Tech-Transfer Violations," *Aviation Week & Space Technology,* November 3, 2008, 34.

[35] Ibid. See also, Department of Justice, *Chinese National Sentenced for Economic* Espionage (2008), http://hongkong.usconsulate.gov/uscn_others_2008061802.html.

[36]Zheng Chengsi, *Shortcomings of the Information, Intellectual Property and the Intellectual Property Strategy of China* [*Xinxi, Zhishi Chanquan yu Zhongguo Zhishi Chanquan Zhanlue Ruogan Wenti*] (January 20007), http://www.sipo.gov.cn/sipo/xwdt/mtjj/2007/200701/t20070129_131223.htm; Lin Yuhong, *Zheng Chengsi: Guobao Ji* [Zheng Chengsi: National Treasure] *Guangming Daily,* September 17, 2006, http://www.gmw.cn/01gmrb/2006-09/17/content_480949.htm; See also, *Implications*, *supra* note 16, 42

[37] *Implications*, *supra* note 16, 42; State Council of the People's Republic of China, *Outline of the National Intellectual Property Strategy*, §V (1)(40) (June 5, 2008), available at http://www.law-now.com/law-now/sys/getpdf.htm?pdf=outlineof thenationalintellectualpropertystrategy1.pdf. [Hereafter cited as *Strategy*.] The impetus for the IP strategy largely originated from the tireless efforts of the late Professor Zheng Chengsi, the "father of IP in China" and former director of the IP Office of the Chinese Academy of Sciences (CAS). Zheng visited Japan's Patent Office in 2002 to learn more about Japan's newly-launched National IP Strategy. Japan's IP Strategy impressed Zheng because Japan had used it to help revitalize its lagging economy. Subsequently, Zheng held a large-scale seminar on Japan's IP Strategy at CAS, which became of the substance of a CAS report delivered to the State Council. The report had a significant impact on the Council, and in January 2005, the Council established the Leading Group (LG) for National Intellectual Property Strategy Formulation.

[38] "The administration of intellectual property needs to cover all links in national defense, including research, production, operation, equipment procurement and guarantee, and project management, and control of major intellectual property related to national defense should be strengthened. A guideline to key technologies needs to be published. Create a number of the self-relied intellectual property in areas such as key technologies for weapons and military equipment and high technologies for both military and civilian purposes. An early warning mechanism for intellectual property related to national defense needs to be established, and special examinations of IPRs related to national defense should be carried out in military technology cooperation and arms trade…Make more effective use of intellectual property related to national defense. The rules for keeping secrecy and declassification of intellectual property related to national defense need to be further improved. Promote the use of intellectual property related to the national defense for civilian purposes with the condition that national security and the interests of national defense are not compromised. Encourage the use intellectual property for civilian purposes in the area of national defense." Ibid., §IV (7) (38, 39).

[39] China's push to create standards for third-generation (3G) mobile telephony, based on the TD-SCDMA (Time Division-Synchronous Code Division Multiple Access) standard, and the Internet (IPV6), is motivated by a desire to avoid licensing fees and ground the standards for these technologies in Chinese IP. James Popkin and Partha Iyengar suggest China is generally developing standards to protect domestic firms from foreign competition and, in the case of security standards for wireless communications, to

decrypt and monitor foreign communications inside China. James M. Popkin and Partha Iyengar, *IT and the East*: *How China and India are Altering the Future of Technology and Innovation* (Boston, MA: Harvard Business School Press, 2007), 24.

[40] Ibid., §VI (1) (30); See also Richard P. Suttmeier et al., *Standards of Power? Technology, Institutions, and Politics in the Development of China's National Standards Strategy* (Seattle, WA: The National Bureau of Asian Research, 2006), 1.

[41] Chien-Hsun Chen et al., *High-tech Industries in China* (Cheltenham, UK: Edward Elgar Publishing, 2005), xv. "In the vast majority of cases, multinationals are willing to provide their China subsidiaries with advanced technology; this was true of 86.6 percent of the multinationals included in the sample. 65.3 percent of the multinationals in the survey were providing technology that had not previously been available in China. Technology obtained from foreign-invested enterprises accounts for over 50 percent of all foreign technology introduced into China; in more than 60 percent of cases multinationals' Chinese subsidiaries are using technology that is less than three years old." Ibid.

[42] Kathleen Walsh, *Foreign High-tech R&D in China: Risks, Rewards, and Implications for US-China Relations* (Washington, D.C.: The Henry L. Stimson Center, 2003), 105.

[43] Ibid.

[44] "2008 Global R&D Report: Changes in the R&D Community," *R&D Magazine,* September 7, 2007, G3, http://www.rdmag.com/pdf/RD79GlobalReport.pdf.

[45] Ibid. See also Maximilian von Zedtwitz, "Managing Foreign R&D Laboratories in China," *R&D Management* 34, No. 4 (2004): 439.

[46] Nannan Lundin and Sylvia Schwaag Serger, *Globalization of R&D and China: Empirical Observations and Policy Implications*, (Stockholm, Sweden: Research Institute of Industrial Economics, 2007), 1.

[47] See *Case of China*, *supra* note 20, 3-4.

[48] Ibid., 2.

[49] Julian Goldsmith, "Huawei Touts R&D Prowess," *Silicon.com,* September 6, 2007 [hereafter cited as *Prowess*]; Huawei spends approximately 10 percent of its yearly revenue on R&D. See Huaichuan Rui and George S. Yip, "Foreign Acquisitions by Chinese Firms: A Strategic Intent Perspective," *Journal of World Business* (2008), 9. [Hereafter cited as *Strategic Intent*.]

[50] Some Chinese counterfeiting operations are so advanced that they include well-funded and elaborate underground R&D programs. Xu Chao, "Black Phone Innovations [Hei Shouji Chuangxin]," *World Communications Weekly* (June 10, 2008) http://www.cww.net.cn/mobile/html/2008/6/10/20086101826494773.htm; See also *Case of China*, *supra* note 20, 3-4.

[51] China's IP Strategy is intended to transform China's IP activities from being primarily a legal and trade-related issue, to becoming a strategic imperative that is the domain of Chinese corporations and government agencies. Numerous policymakers and officials from the State Council, SIPO, COSTIND (State Commission on Science, Technology and Industry for National Defense), the Ministry of Science & Technology (MOST), CAS, Supreme People's Court (SPC), Ministry of Public Security (MPS) and representatives from top universities in China, such as Beijing and Qinghua Universities, have been involved in developing, collaborating and coordinating on various aspects of the Strategy. Coinciding with the development of the IP Strategy, statements on the importance of IP and the IP Strategy for improving the development of the national economy, innovation and military weaponry began to appear in national S&T development plans, China's National Defense White Papers (NDWP) (2006), and COSTIND publications—a relatively recent phenomenon in China. The NDWP, for example, emphasizes that the military should improve innovation to build better weapons and equipment and that increased R&D in the military has resulted in the development of new S&T inventions and IP. *Implications*, *supra* note 16, 29.

[52] Li Yan et al., "Analysis of the State of Competitive Technical Intelligence" ["Jishu Jingzheng Qingbaode Xiankuang Fenxi"], *Competitive Intelligence Journal* [*Jingzheng Xuebao*] (2006).

[53] Xue Yafang, *The Growing Demand for Intelligence Personnel Is Becoming More Conspicuous* [*Qingbao Rencai Xuqiu Riyi Xian Xinghua*], April 16, 2005, http://www.chinahrd.net/zhi_sk/jt_page.asp?articleid=76116; Justin L. Bloom, "Japan as a Model for a National Approach to Business Intelligence," W. Bradford Ashton and Richard A. Klavans, eds., *Keeping Abreast of Science and Technology: Technical Intelligence for Business* (Columbus, OH: Batelle Press, 1997), 49.

[54] TRS conducts R&D on information retrieval and content management systems for the Chinese government and industry and provides information technology support to corporate and government CI systems. TRS Website [[in Chinese], *Company Profile,* http://www.trs.com.cn/company/compintro/lhz.

[55] Zhong Tianwei, "The Practice of Competitive Intelligence and Development," 13th Annual Session on China's Competitive Intelligence, Nanning, Guangxi, November 8, 2007, http:www.trs.com.cn/news/ztbd/2007CIS/.

[56] W. Bradford Ashton and Richard A. Klavans, "An Introduction to Technical Intelligence in Business," *Keeping Abreast of Science and Technology: Technical Intelligence for Business* (Columbus, OH: Battelle Press, 1997), 113-114. [Hereafter cited *Technical Intelligence*.]

[57] Justin L. Bloom, "Japan as a Model for a National Approach to Business Intelligence," 49.

[58] See Chinese SCIP Official Website, http://www.scic.org.cn/NOTICE/08lj.doc.

[59] *Decade of CI*, *supra* note 8.

[60] Chen Feng, *Mian Xiang Qiye Zhanlue Guanli de Jingzheng Qingbao* Yanjiu [Research on Competitive Intelligence and Strategic Management], Ph.D. Dissertation, Beijing University (2002) [hereafter cited as *CI & Strategic Management*]; Liu Ting, *Guojia Anquan de Qingbao Baozhang Tixi Yanjiu* [Research on Intelligence Support to National Security], Ph.D. Dissertation, Nanjing University (2002).

[61] See for example, http://www.dinglv.com.cn/zjtd.html.

[62] CTI techniques could include technology prospecting, Web mining, data mining, patent analysis or scientometrics, etc.; W. Bradford Ashton and Richard A. Klavans, "An Introduction to Technical Intelligence in Business," *Keeping Abreast of Science and Technology: Technical Intelligence for Business* (Columbus, OH: Battelle Press, 1997), 11. [Hereafter cited *Technical Intelligence*.]

[63] *Decade of CI*, *supra* note 8.

[64] Ibid.

[65] *Cyber-Militia*, *supra* note 29.

[66]Chinese R&D and CI labor costs are significantly lower than in America. According to Huawei, at one-fifth of that in the West, Chinese multinational giants can compete in the R&D arena with less than a quarter of the R&D budget of large Western firms. *Prowess*, *supra* note 49.

[67] *Technical Intelligence*, *supra* note 56.

[68] See *Decade of CI*, *supra* note 8.

[69] Chinese companies that are located in high-tech science parks in China not only benefit from preferential tax, financial and foreign exchange treatment, but are also able to collaborate with first-class research institutes and universities. Beijing's Zhongguancun Science Park, for example, contains over 12,000 firms and is located in the Haidian district, which contains 232 scientific research institutes, 73 universities (including the Harvard and MIT of China, Beijing University and Qinghua University, respectively). Company R&D and innovation costs are tax deductible, and imported technology and IP receive tariff exemptions. According to official Chinese data, the park's gross industrial output reached about $25 billion in 2003. Quanlin Gu et al., "Firm Dynamics in Economic Transition: Evidence from a

Chinese Science Park," in Haiying Li, ed., *Growth of New Technology Ventures in China's Market* (Cheltenham, UK: 2006), 35.

[70] Notra Trulock, the former director of intelligence at the U.S. Department of Energy, writes: "[T]he Chinese approached spying differently from the Russians… Chinese techniques were "nontraditional" in that they concentrated more on eliciting information from visiting scientists and other officials and less on Soviet-style spycraft…[T]he Chinese would employ scientists, academicians and students to collect information of interest…Intelligence taskings would come from scientists or academic institutions engaged in research for the People's Liberation Army or from other government customers…The Chinese painstakingly collected lab and Energy Department unclassified technical reports, and visitors to Chinese facilities were struck by the thoroughness of their collections. In their own writings, the Chinese assessed these reports as 'provid[ing] intelligence of great value.' The Chinese knew all about the labs' penchant for sloppy handling and "inadvertent" releases of classified documents…" Notra Trulock, *Code Name Kindred Spirit: Inside the Chinese Nuclear Espionage Scandal* (San Francisco, CA: Encounter Books, 2003), 106-07; Chinese companies located in the park also have access to government-supported research in scientific and technical areas. *Strategic Intent*, *supra* note 49, 5.

[71] Some large Chinese companies receive financial support from the Chinese government for some of their illegal activities, and in turn, assist the military or civilian intelligence services with identifying and acquiring foreign technology. *The Cox Report: U.S. National Security and Military/Commercial Concerns with the People's Republic of China*, Report of the Select Committee, United States House of Representatives (Washington, DC: Regnery Publishing, Inc., 1999), 68-70. [Hereafter cited as *Cox Report*.]

[72] *Cyber-Militia*, *supra* note 29.

[73] *E-spionage, supra* note 26, 040.

[74] *Cox Report*, *supra* note 72.

[75] Roger Z. George, "Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm," *Studies in Intelligence* 51, No. 3 (Extracts-September 2007): 1, citing Director of National Intelligence, *Report on the Progress of the Director of National Intelligence in Implementing the "Intelligence Reform and Terrorism Prevention Act of 2004*," May 2006, 5-11. Available online at http://www.dni.gov/reports/CDA_14-25-2004_report.pdf.

[76] Ibid.

[77] *Cox Report*, *supra* note 72, p. 87.

[78] Ibid., 87-88.

[79] Ibid., 88.

[80] Ibid.

[81] Ibid..

[82] Robert M. Clark, "Scientific and Technical Intelligence Analysis," *Studies in Intelligence*, 19, No. 1 (Spring 1975), in H. Bradford Westerfield, ed., *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal*, 1955-1992 (New Haven, CT: Yale University Press, 1995), 294. [Hereafter cited as *Intelligence Analysis*.]

[83] *CI & Strategic Management*, *supra* note 60.

[84] Rob Johnston, *Analytic Culture in the US Intelligence Community: An Ethnographic Study* (Washington, DC: Center for the Study of Intelligence, 2005), 66-70. [Hereafter cited as *Analytic Culture*.]

[85] Ibid.

[86] Ibid., 67.

[87] Gregory F. Treverton and C. Bryan Gabbard, *Assessing the Tradecraft of Intelligence Analysis* (Santa Monica, CA: RAND Corporation, 2008), 4. [Hereafter cited as *RAND report*.]

[88] *Intelligence Analysis*, *supra* note 82, 294.

[89] *Cox Report*, *supra* note 72, 50.

[90] *Analytic Culture*, *supra* note 84, 66-70.

[91] *RAND report*, *supra* note 87, 1.

[92] Ibid.

[93] Ibid., 48.

[94] Ibid., 7.

[95] *Decades*, *supra* note 5, A1.

[96] *Cyber-Militia*, *supra* note 29.

[97] *Two McKinsey Surveys*, *supra* note 2, 6.

[98] Curtis R. Carlson and William W. Wilmot, *Innovation: The Five Disciplines for Creating What Customers Want* (New York, NY: Crown Publishing Group, 2006), 268-269. [Hereafter cited as *Innovation.]*

[99]" Revving Up: How Globalization and Information Technology are Spurring Faster Innovations, in Special Report on Innovation," *Economist,* October 13, 2007, 6.

[100] *Implications*, *supra* note 16, 46.

[101] *Innovation*, *supra* note 98, 268-269.

[102] Geoffrey Colvin, "America Isn't Ready: Here's What to Do About It," *Fortune,* August 4, 2005, 77.

[103] *Chinese Leader Says China Losing Competitive Edge* (November 30, 2008), http://news.yahoo.com/s/ap/20081130/ap_on_bi_ge/as_china_economy.

[104] Ariana Eunjung Cha, "As China's Losses Mount, Confidence Turns to Fear Officials Use Bailouts to Forestall Unrest," *Washington Post Foreign Service,* November 4, 2008, A01.

[105] Robert Clark, *Huawei Posts Record Result, Frets About Downturn* (July 14, 2008) http://www.telecomasia.net/article.php?id_article=9446.

[106] According to various reports, Huawei encourages a "mattress culture" where every software developer keeps a mattress in the office to sleep after hours. "Huawei CEO Writes a Letter to Employees Addressing the Issue of Depression" [Huawei CEO Gei Yuangong Xie Yantan Yindu Zao Bao Guang] *Daily Economic News* [*Meiri Jingji Xinwen*], April 18, 2008, http://news.xinhuanet.com/employment/2008-04/18/content_8002142_1.htm.

[107] Tim Lebrecht, "For China, the Financial Crisis is An Opportunity," *CNET Blog Network*, October 18, 2008, http://news.cnet.com/8301-13641_3-10069536-44.html.

[108] "Huawei's Ever-Expansion Strategy May Hit a Wall, or Not," October 31, 2008, http://www.chinastakes.com/story.aspx?id=781.

[109] James Flanigan, "An Eye on Growth, Deals Stretch Across the Pacific," *New York Times*, November 20, 2008, http://www.nytimes.com/2008/11/20/business/smallbusiness/20edge.html.

[110] Ibid.

[111] Meridith Levinson, "How to Avoid Getting Sued by a Former Employer," November 13, 2008, http://www.cio.com/article/462663/How_to_Avoid_Getting_Sued_by_a_Former_Employerhttp://www.cio.com/article/462663/How_to_Avoid_Getting_Sued_by_a_Former_Employer.

[112] The company's 2005 study on Chinese IP points out: "In China, a large number of technical specialists who have retired after enjoying a full career in the United States or Europe discover a very supportive

environment for a second career in China…funds are available for such start-ups from domestic and foreign sources, and venture capital money increasingly is attracted to ones with major potential and apparent political support." *Case of China*, *supra* note 20, 5.

[113] Jin Chen and R. Michael Holmes Jr., "Theory and Empirical Evidence on R&D Globalization in Chinese Firms," in Haiying Li, ed., *Growth of New Technology Ventures in China's Market* (Cheltenham, UK: 2006), 273-74.

[114] Thomas Luedi, "China's Track Record in M&A," *The McKinsey Quarterly*, No. 3 (2008), 77.

[115] *Strategic Intent*, *supra* note 49, 9.

[116] Hiawatha Bray, "Downturn Lashes into High Tech: Industry Cutting Thousands of Positions as Businesses and Consumers Trim Purchases," *The Boston Globe,* November 15, 2008, http://www.boston.com/business/technology/articles/2008/11/15/downturn_lashes_into_high_tech/.

[117] *Case of China*, *supra* note 20, 5.

[118] *Implications*, *supra* note 16, 43.

[119] Christopher Bellavita suggests using a "pattern-based approach" to help make sense of such evolving homeland security issues "to sift through the elements of strategic disorder…and determine whether an issue can be ordered—and thus subject to a rich set of knowledge and methodologies…" See *Shape Patterns*, *supra* note 7.

[120] *CI in France*, *supra* note 9, 64.

[121] *FBI Offensive*, *supra* note 33.

[122] See, for example, National Intelligence Council, *Tracking the Dragon: National Intelligence Estimates on China During the Era of Mao, 1948-1976* (Washington, DC: National Intelligence Council, 2004), 405-412.

[123] Ibid.

[124] *Decade of CI*, *supra* note 8.

[125] *FBI Offensive*, *supra* note 33.

[126] *Decade of CI*, *supra* note 8.

[127] See *Trade Secret Protection*, *supra* note 1.

[128] *Cyber-Militia*, *supra* note 29.

[129] Ibid.

[130] "Data Theft Experts Discuss Enforceable Data Leakage Prevention Policies During Economic Downturn," *MarketWire,* November 10, 2008, http://www.marketwatch.com/news/story/Data-Theft-Experts-Discuss-Enforceable/story.aspx?guid=%7BF20E3631-A4FA-4A1F-A391-5ACBD07B472D%7D.

[131] 'You just don't give the developers access to the code tree the way we would in an equivalent position here…We're just opening up Russia as an example. We have 100 people there; we'll have 200 people there a year from now. They're superb engineers. They are the best of the best out of the Russian Academy of Sciences and their engineering schools, and they're astonishing mathematicians. So we're giving them big math problems, big algorithm problems to help drive the heart of these software packages that we produce. It doesn't connect to anything for them—it's just a big matrix to solve, and they're doing a marvelous job of it.'" *Case of China*, *supra* note 20, 58-60.

[132] Thomas P.M. Barnett, "Ten Reasons Why China Matters To You," *Good* 10 (2008), 63. Although Professor David Lampton, Director of China Studies at John's Hopkins University's School of Advanced International Studies, does not support a "confrontationalist" policy toward China, he concedes that China must cooperate with the United States on the matter of intellectual property protection: "China

simply is too big to be allowed to violate foreign intellectual property the way earlier, smaller modernizing economies did. Beijing has to assume responsibility for the local officials who have become addicted to the revenues and employment their localities generate through the theft of intellectual property." David M. Lampton, "Paradigm Lost: The Demise of "Weak China," *The National Interest*, No. 81 (2005), 79-80.