LIBERTY UNIVERSITY

Strategic Informer: Student Publication of the Strategic Intelligence Society

Volume 1 | Issue 1 Article 7

March 2012

Innovation and National Security: The Loss of Economic and Military Strength through the Theft of Ideas

Matthew D. Pedersen
mpedersen@liberty.edu

Innovation and National Security

The Loss of Economic and Military Strength Through the Theft of Ideas

Matthew D. Pedersen

From the earliest days of nation-states, measures of power have been displayed by emphasizing the size and superiority of military force. The 16th through the early 20th century saw the increasing size of armed forces as the rest of the world began to appreciate the might and strength of the Spanish Armada, the British Royal Navy, the Imperial Japanese Navy, and the American Carrier Battle Group. The expansion of naval forces allowed countries to colonize lands, gather raw materials, and assist in their global hegemony. Following the end of World War II and the development of nuclear weapons, a transformational shift grew out of the dependency to have cutting edge military technology and the materials to develop them. The strength of nations thus became tied proportionately to the development of the military force's innovation as well as its size.

MILITARY INNOVATION

Military planners were concerned to a lesser extent with having the largest fighting force rather the most adept at fighting the battles throughout the 20th and 21st centuries. For the military force of the latter 20th century, "the degree of national security rapidly declines when reliance is placed on the quantity of existing equipment instead of its quality."[123] While the U.S. Air Force was the branch most concerned with this during the nuclear era of development, that quote is universal to all branches of the military in that "[t]he first essential of air power [or any other power] necessary for peace and security is pre-eminence in research."[124] The advanced research & development (R&D) that had grown out of the Manhattan Project and the shared mutual-interdependence of uniting civilian and military personnel had historically been overseen by military command. By 1950, military R&D contracts numbered nearly 20,000.[125] Although the numbers will have grown since the 1950s, estimates placed military R&D costs in the neighborhood of $600 million. That amounts to nearly one cent of every dollar paid in federal taxes being spent for research towards more effective weapons, equipment, medicines, and utilization of human resources in war.[126]

CIVILIAN INNOVATION

Yet now, more than in any previous period, research and innovation is fostered under private control. Historically, military officers held an advantage over their civilian counterparts when it came to thinking through the dilemmas of warfare; however, the development of nuclear weapons leveled the playing field.[127] The technical superiority that is pursued in research universities, private research labs, and by individual entrepreneurs has most recently coexisted alongside R&D currently undertaken in Federal agencies such as the United States' Defense Advanced Research Projects Agency (DARPA) and its northern neighbor, Defense Research and Development Canada (DRDC). While government agencies' progress is delayed due to the red tape of governmental bureaucracies, their civilian counterparts are able to efficiently bring new products to market because of the demand to gain a market advantage. Many programs receiving federal funds have numerous officials and politicians with a say in the matter that may have their own agenda or wish to impose specific requirements relevant to their department or their county.

This is best described by analogy: while something like a horse may have been originally conceptualized, specialized in purpose and required only to run quickly, the end product after oversight and bureaucracy may turn out to be something that resembles a camel; an odd creature fairly adequate at doing multiple generic tasks or responsibilities. The independence then of the military from the civilian sphere was defunct and the cohesion of the government, military, and private

123 Mahnken, Thomas G. Technology and the American Way of War Since 1945. (Columbia University Press, 04 July 2008), 31.

124 Ibid, 31.

125 Gellhorn, Walter. Security, Loyalty, and Science. (Ithaca, New York: Cornell University Press, 1950), 1-2.

126 Mahnken, 31.

127 Ibid, 26.

sector would then become essential to promoting national security. Nations leading up to the early 20th century were all too eager to flex their military muscles, yet the period following World War II to the present showed the necessity of emphasis and reliance on economic superiority as much as military strength.

GROWTH + R&D

A nation's ability to grow its economy soon became strategic to military planning. This was established predominantly through innovation, as well as the ease of which factors of production were accumulated, specifically raw materials. The Organization for Economic Co-operation and Development (OECD) determined that "innovation has long been recognized as a main driver of economic growth, through the development and exploitation of ideas for new products and processes."[128]

For growth to truly be fueled by R&D, protected intellectual property ("IP") rights are an essential element to allow individuals, companies, and countries to utilize the worthwhile investment to formulate and apply a new idea. Without adequate protection of these intellectual property rights, the incentive to develop new ideas and products would be reduced, thereby weakening the innovation process.[129] The risks of doing R&D become unfeasible when the costs to develop exceed the benefit of the new product, or when the security measure designed to protect IP slows development or comes to a standstill. Gelhorn, the university professor Emeritus at Columbia, wrote that the United States was purchasing security during the Cold War, but only at the expense of progress. He maintains that a secret program's nature of apprehensiveness and compartmentalization hinders the forward progress of scientific energies into the unexplored areas.[130] He details an example at Los Alamos in the 1950s where Security Services personnel far outnumbered the scientists at the location.[131] Yet according to the National Counter-Intelligence Executive, Robert "Bear" Bryant, the R&D of both public and private sectors is estimated at $400 billion annually.[14]

INFORMATION TECHNOLOGY

The contest to develop and bring to market the newest innovation or idea requires a centralized hub for engineers, consultants, and designers to amalgamate their separate work. The race begun in the 1940s to collect radioactive material for nuclear weapons and civil electricity also brought about changes to electronics and computational theory; their byproducts, the microprocessor and computer, would revolutionize the way wars are fought and how money is made.

Information technology (IT), and the way in which information is stored and distributed, emerged as a way to allow more involvement from more individuals in different locations. A theory developed from computer usage, and argued during the early 1990s, was the idea of the interrelatedness between the military and the economy. The main tenets of the concept known as network-centric warfare was that information technology had revolutionized and had fundamentally changed both war and business through its interconnected nature.[132] As Admiral Arthur Cebrowski stated, "nations make war the same way they make wealth." Just as success in business depends on the ability to circulate information, the same is true of militaries; the victorious army is the one which obtains and properly applies the most accurate information.[133]

ESPIONAGE

With the digitization of theories and ease of developing complex ideas, innovation and economic growth have exponentially increased. The development of the computers and the networks to connect them

128 "The Economic Impact of Counterfeiting and Piracy." Organisation for Economic Co-operation and Development (OECD). OECD Directorate for Science, Technology and Industry. June 2008. http://www.oecd.org/document/4/0,3746,en_2649_34173_40876868_1_1_1_1,00.html, (accessed 10 March 2012).

129 "The Economic Impact of Counterfeiting and Piracy."

130 Gellhorn, 4.

131 Ibid, 3.

132 Herspring, Dale. Rumsfeld's Wars: The Arrogance of Power. (Lawrence: University Press of Kansas, 30 April 2008), 26.

133 Ibid.

has eased the flow of information. Unfortunately, as exponential as the growth in ideas and innovation has been, likewise has the relative ease for those ideas and innovations to be acquired and exploited by forces external to the R&D, and implementation of such ideas. The responsibility for the theft of innovation falls equally on the transfer of R&D from military institutions to civilian and private agencies, as well as the ease with which information is transferred in modern times.

Typically, a company's main core competency is tied to an innovative product, process, or service that is protected by patents; yet, unscrupulous agents find little moral quandary in the theft of an idea. In a speech to the Office of the Director of National Intelligence, Bryant stated:

> Today I would say the primary assets of corporate idea are intangible assets – certainly research and development, certainly plans and business plans, and really positions on contracts. The threat to the U.S. private sector is more exposed and vulnerable than ever.[134]

The threat to national security and the diffusion of technologies through theft by hostile actors becomes dangerous partially through the ever-increasing influence that globalization has on the West, in addition to the sheer quantity of occurring theft. While traditional human intelligence (HUMINT) sources have historically been the most utilized form of intelligence acquisition, the 21st century has witnessed the explosion of electronic intelligence (ELINT), cyber-espionage, and cyber-warfare. The reality and scale of cyber threats both to U.S. national security and the economy has now been realized, prompting the Pentagon to build complex defenses around military networks and create the new U.S. Cyber Command to integrate cyber defense with operations across the military.[135] However, there are still vast unprotected arenas available to players interested in subverting national security. According to The Economist, "the threat is complex, multifaceted and potentially very dangerous. Modern societies are ever more reliant on computer systems linked to the Internet, giving enemies more avenues of attack."[136] Unfortunately, the threats are real and growing at an immeasurable rate. The information being stolen requires vigilance to defend as a critical national asset, and that in itself makes it worthwhile to protect. According to Bryant, "What I see as an economic espionage, to a large extent, is really kind of a death by a thousand cuts. And these are being perpetrated by different actors – sometimes foreign intelligence services, sometimes by corporations, sometimes by individuals."

THEFT OF IDEAS

The threat to the United States and its way of life, prosperity, and security is based in attacks by foreign entities on a regular basis as they attempt to steal not just America's products or ideas, but its livelihood. The theft occurs in nearly every sphere as military and civilian targets are not distinguishable as foreign entities seek to draw out every last shred of information that is crucial to America. According to the Office of National Counter-Intelligence Executive report on stolen U.S. economic secrets, the categories of significant interest to foreign entities are:[137]

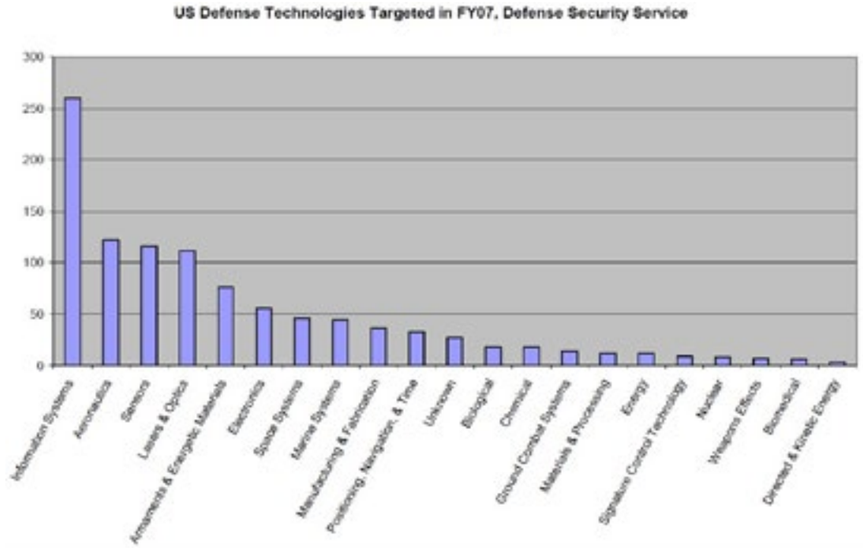
- information and communications technology
  - forms the backbone of nearly every other technology
- business information
  - could pertain to supplies of scarce natural resources or provide foreign actors an edge in negotiations with U.S. businesses or the U.S. government
- military technologies
  - marine systems, UAVs, and other aerospace/aeronautic technologies in particular
- civilian and dual-use technologies
  - especially in sectors likely to experience fast growth, such as clean energy and healthcare/pharmaceuticals

Furthermore, a 2007 report to Congress notes:

> Foreign collectors attempted to obtain information and technologies from each of the 20 categories on the Developing Sciences and Technologies List (DSTL). The DSTL is a compendium of scientific and technological capabilities being developed worldwide that have the potential to significantly enhance or degrade US military capabilities in the future.[138]

The theft of American IP that has escalated in the 21st century occurs through illegal use of HUMINT gathering as well as the marginally less ominous open-source Competitive Intelligence Solution (CIS), an extension of Business Market Analysis. By using legal loopholes, foreign entities are able to utilize CIS and acquisitions of American enterprises to retain the company's IP and optimize it for their own domestic purposes.

China, through its sheer number of possible recruits, exploits the population base by employing its trademark human-wave/mosaic intelligence gathering sources to gather IP and foreign technologies. The gathering of intelligence through open source channels and the collection of many small pieces of intelligence that have significance only when put together with the rest of the pieces is a daunting chore. While not exclusive to China, it is capable only by a country with a large network of analysts available. Although it is a tedious task, it indicates their patience in applying the notion implemented under Chairman Mao known as "Guanxi;" the development of personal networks used to gain favors.[139] These networks utilize Chinese migrants in the West to obtain technological and economic intelligence that is crucial to its national development.[140] The reliance on Chinese nationals for intelligence gathering and implementation of Guanxi networks shows the distrust toward foreigners; the Chinese Ministry for State Security (MSS) traditionally gathers intelligence through ethnic Chinese only.[141]



134 Robert Bear Bryant to Office of the Director of National Intelligence. The Report to Congress on Foreign Economic Collection, ODNI Public Affairs. 03 November 2011. http://www.ncix.gov/publications/reports/fecie_all/EconEsp_PressConf.pdf, (accessed 10 March 2012).

135 Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyber-strategy". Foreign Affairs. 01 September 2010. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain, (accessed 03 April, 2012).

136 "The Threat from the Internet: Cyber War." The Economist. 01 July 2010. http://www.economist.com/node/16481504?story_id=16481504&source=features_box1, (accessed 03 April 2012).

137 Foreign Spies Stealing US Economic Secrets in Cyberspace. Report to Congress. Office of the National Counterintelligence Executive. October 2011. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf, (accessed 03 April 2012).

138 Ibid.

139 "Special Report: Espionage with Chinese Characteristics". Stratfor. 24 March 2010. http://www.stratfor.com/analysis/20100314_intelligence_services_espionage_chinese_characteristics?page=15&width=480&inline=true, (accessed 03 April 2012).

140 Ibid.

141 Ibid.

Agents gather technical intelligence in three primary ways: [142]

1) Chinese nationals are asked to acquire targeted technologies while traveling

2) Foreign companies with the desired technologies are purchased by Chinese firms

3) Equipment with the desired technologies is purchased by Chinese front companies, usually in Hong Kong

The first method utilizing travelers, students, and student exchange programs, such as the Chinese Association of Scientists and Engineers in Japan (CASAJ) and the Association of Chinese Scientists and Engineers in Japan (ACSEJ), gains access to legally acquire knowledge on foreign technologies. The ACSEJ's stated purpose is "to promote and strengthen cooperation and exchanges between Chinese scientists and engineers in Japan and between relevant organizations, institutions, and scholars in China and other countries, especially Japan."[143] Its bylaws note the manner in which these goals are to be met, including "helping form PRC Science &Technology (S&T) policy and supporting China's development of new high technology."[144]

In 2011, James Dyson, inventor of the bagless vacuum cleaner, warned that Chinese students were stealing technological and scientific secrets from UK universities.[145] He also noted that Chinese students were planting malware that would relay information to China even after their departure from the university.[146]

The mimicry of espionage methods should come as no surprise, as China's manner of espionage has been emulated by South Korea's Ministry of Science and Technology (MOST) which is said to have quadrupled its support for "informal" acquisition of foreign technology; read espionage.[147] According to ROK news reports, part of the spending will be directed towards a consolidated brainpool administered by Seoul to recruit foreign scientists.[148] MOST planned on using the program to solve domestic technological bottlenecks and to absorb advances and technological knowledge. As part of the spending increase, Seoul hosts a triennial event that attracts domestic and overseas Korean scientists for the purpose of sharing new scientific and technological information. Ethnic Koreans numbering 291 and hailing from 12 countries were said to have been in attendance. The event's theme was described as contributing to South Korea's competitiveness through the globalization of science and technology.[149]

The second method of foreign technology procurement is through the acquisition of foreign companies. China National Aero-Technology Import & Export Corporation (CATIC) purchased the American defense firm Mamco Manufacturing in the 1990s, despite a direct connection between CATIC and the People's Liberation Army (PLA).[150] An inside source noted that Chinese companies such as Huawei Technologies withdrew a bid to purchase 3Com, a U.S. Internet and networking company, after an investigation found links to China's intelligence services.[151] In 2008, Huawei established a joint venture with the U.S. anti-virus software company Symantec, headquartered in Chengdu, China. Currently, it only offers software in China, but Stratfor sources suggest that if Huawei were to be used for Chinese intelligence, it could easily insert spyware into computer systems which subscribe to its service.[152] As a backdrop to this

142 Ibid.

143 "Chinese Science and Technology Supported in Japan". Office of the National Counterintelligence Executive. March 2003. http://www.ncix.gov/docs/CHINESE_SUPPORT_GROUPS_JAPAN.pdf, (accessed 03 April 2012).

144 Ibid.

145 "Foreign Economic Collection and Industrial Espionage Reports". Office of the National Counterintelligence Executive. October 2011. http://www.ncix.gov/publications/reports/fecie_all/index.php, (accessed 03 April 2012).

146 Ibid.

147 "South Korea: Large Boost in Funds For Technology Transfer." Office of the National Counterintelligence Executive. March 2003. http://www.ncix.gov/docs/SKoreaBoostsFundsForTechTransfer.pdf, (accessed 03 April 2012).

148 Ibid.

149 Ibid.

150 "Special Report: Espionage with Chinese Characteristics." Stratfor. 24 March 2010.

151 Ibid.

152 Ibid.

consideration, it is relevant to note that Huawei was founded in 1988 by Ren Zhengfei, a mere four years after retirement from the Chinese military where he finished his career as deputy director of the Science Research Institute of the Engineering Army Corps.[153]

The third method of acquiring foreign technologies, although technically legal in most instances, occurs when Chinese companies and state-owned enterprises (SOE) purchase products with technologies requested to further grow Chinese S&T policies. One of the largest targeted industries is aviation, publicized by a case that involved a Chinese individual who was arrested for attempting to purchase aerospace-related microchips from BAE Systems; this is one of the companies involved in the development of the Lockheed-Martin F-35 Joint Strike Fighter.[154] Similar espionage may have played a role in China's development of the new J-20 fifth-generation fighter, yet that remains mere conjecture.[155] Other speculation abounds in China's aviation industry, where it was alleged that they purchased the remains of Israel's IAI Lavi and reverse-engineered it into the Chengdu J-10 Fighter.[156] Although there is still debate as to the legitimacy of these claims, Russian engineers claimed to have knowledge of China's possession of the Lavi, although the authenticity of those claims remains contested.[157]

Concerns about the theft of aviation technology are also shared by Russia.[158] An arrangement was in place for China to acquire 200 Sukhoi SU-27 Fighters, but China canceled the order early after reverse-engineering Russian avionics and electronics. China has recently revealed a version of Russia's Al-31F engine that they have produced domestically, comparable in both technology and performance.

The Third Bureau of the MSS is responsible for purchasing targeted technologies through shell and front companies.[159] Most of these businesses are run independently of overt Chinese intelligence management, though their leadership frequently includes individuals who maintain connections with intelligence officers, as previously noted in Guanxi personal networks. One recent case involved the 88 Queensway Group, named for the address of an office building in central Hong Kong that houses many state-owned Chinese companies, along with the China Investment Corporation, the country's sovereign wealth fund, and various private firms.[160] A U.S. Congressional report shows a possible link between the building and "China's intelligence apparatus."[161]

One of the most recent and brazen espionage cases conducted by China involves American Superconductor Corp (AMSC), a computer systems developer that serves as the electronic brains of wind turbines, being sold to a Chinese turbine manufacturer called Sinovel Wind Group Company. AMSC's technicians were unable to get turbines to follow system commands and it was not until they consulted with their software department that they realized the Sinovel turbine was running a stolen version of AMSC's software. The Beijing-based manufacturer was utilizing AMSC's proprietary source code, and thus with no further need for AMSC, they terminated their agreement.[162]

Even worse for American national security is that amongst Sinovel's investors is a private equity group founded by Wen Yunsong, son of China's Premier, Wen Jiabao.[163] Shortly after the termination of the agreement, Sinoval's Chairman and President Han Junliang helped create Dalian Guotong Electric,

153 Engleman, Eric, "Huawei, ZTE Face Scrutiny From U.S. House Intelligence Panel." Bloomberg. 18 November 2011. http://www.bloomberg.com/news/2011-11-17/house-intelligence-panel-probing-chinese-phone-companies-in-u-s-.html, (accessed 03 April 2012).

154 Noonan, Sean. "Chinese Espionage and French Trade Secrets." Stratfor. 20 January 2011. http://www.stratfor.com/weekly/20110119-chinese-espionage-and-french-trade-secrets, (accessed 03 April 2012).

155 Ibid.

156 Hewson, Robert. "Chinese J-10 'Benefited from the Lavi Project'". IHS.19 May 2008. http://www.janes.com/products/janes/defence-security-report.aspx?id=1065926403, (accessed 03 April 2012).

157 Ibid.

158 Johnson, Reuben F. "Russian Industry Wary of Su-35 Sale to China." IHS. 16 March 2012. http://www.janes.com/products/janes/defence-security-report.aspx?ID=1065966179&channel=defence&subChannel=air, (accessed 03 April 2012).

159 "Special Report: Espionage with Chinese Characteristics." Stratfor. 24 March 2010.

160 Levkowitz, Lee, Marta McLellan Ross, and J.R. Warner. "The 88 Queensway Group: A Case Study in Chinese Investors' Operations in Angola and Beyond," U.S.-China Economic & Security Review Commission. 10 July 2009. http://www.uscc.gov/The_88_Queensway_Group.pdf, (accessed 03 April 2012), 33-35.

161 Ibid.

162 Riley, Michael A. and Ashlee Vance. "China Corporate Espionage Boom Knocks Wind Out of U.S. Companies." Bloomberg. 15 March 2012. http://www.bloomberg.com/news/2012-03-15/china-corporate-espionage-boom-knocks-wind-out-of-u-s-companies.html, (accessed 03 April 2012).

163 Ibid.

making himself chairman and granting Sinovel a 20 percent stake.[164] After opening up a second Sinovel turbine, AMSC investigators noted that an AMSC power converter had been swapped for a Guotong-manufactured duplicate.[165]

Although most countries that seek American IP and technology have dedicated HUMINT organizations, China is the exception. Nearly 70 percent of Chinese intelligence operations are not directly conducted by Chinese intelligence services such as the MSS, MPS, or MID.[166] Most open source intelligence is gathered by a wide array of civil Chinese institutions that are only marginally distanced from the PLA. An example of a civilian agency performing espionage for China's S&T is the State Administration for Science, Technology and Industry for National Defense (SASTIND). Although administrated separately from the PLA, it indirectly makes recommendations to the Central Military Commission (CMC) for research and planning in technological military development, functionally akin to DARPA in the United States.[167]

TRANSITION TO ELINT

The necessity of gathering intelligence from multiple sources and implement the acquired knowledge is a race amongst nations. Mikhail Fradkov, a former Deputy Minister for Foreign Economic Relations and the current director of Russian foreign intelligence, explains that intelligence "aims at supporting the process of modernization of our country and creating the optimal conditions for the development of its science and technology."[168]

MALWARE

The multitude of channels used by foreign nations to conduct espionage on the United States, legal or otherwise, shows the dedication and priority placed on acquiring American ideas. Though HUMINT sources and shell corporations have historically been prominent tools, the emergence of computer networking and the vast globalization of business have made the U.S. even more susceptible to threats from multiple sources. The vast wasteland of the Internet, devoid of market forces or global policing to control it, has proven to be a complicated border to seal, and the extent of damage done to America's progress is difficult to calculate. Some cases exist where HUMINT sources leak technology intentionally and electronically such as the theft of B-1B technology at Rockwell which was sold to the Chinese aviation industry by a Chinese engineer.[169]

Yet, most of the espionage of the 21st century will be through electronic and cyber means. Cyber-attacks can come through multiple avenues, as many of the most recent and blatant incursions have revealed. These penetrations are miniscule in perspective to the quantity of successful incursions. Recently reported events in the media, such as the keylogging of Unmanned Aerial Vehicles (UAVs) and Unmanned Combat Aerial Vehicles (UCAVs) flown from Creech Air Force Base in Nevada, may not directly be the theft of technology or ideas, yet they show the modus operandi (MO) and operational procedures of U.S. proprietary technology.[170] Vulnerabilities are noted as in the case of Iraqi insurgents gaining multiple days of footage of UAVs and UCAVs operating in Iraq. Foreign entities can take advantage of the unencrypted streaming video and design systems to operate in the same manner as the United States unmanned vehicle program.[171]

USB PERIPHERALS

The keylogging program embedded and running in the background of Creech AFB's private and secure network was perpetrated with one of the cheapest and most commonly used computer peripheral.[172]

164 Ibid.

165 Ibid.

166 "Special Report: Espionage with Chinese Characteristics." Stratfor. 24 March 2010.

167 Ibid.

168 "Foreign Spies Stealing US Economic Secrets in Cyberspace." October 2011.

169 Ibid.

170 Shachtman, Noah. "Exclusive: Computer Virus Hits U.S. Drone Fleet." Wired. 07 October 2011. http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/, (accessed 03 April 2012).

171 Ibid.

172 Ibid.

External USB drives are available for less than $10, yet their potential as a vehicle to deliver malware is increasing as the seemingly innocuous device can have malware code embedded. Left in the open or mailed to a recipient as a gift, as soon as they are plugged into a port they can then infect the entire network, which up until that point may have been private and secure.

The Creech AFB case is just one of many documented accounts. A 2008 DOD report of a U.S. military installation in the Middle East details the breaching of the base due to a USB drive and the transfer of data to a server under foreign control.[173] One of the greatest issues with the use of devices manufactured overseas such as USB drives, or any such peripheral, is that the manufacture of computer chips and hardware for Western companies and governments could come from the factory loaded with malware, and that most USB drives are already infected before they leave the factory.[174] The Pentagon has recently banned the use of USB drives due to the unknown nature of foreign factories and the countries in which they are located.[175]

NETWORK INTRUSIONS AND ANTI-VIRUS

The extent to which foreign nations use the interconnected nature of computers to steal technology has forced companies and governments to maintain stringent operational standards in order to sustain the privacy and security of their networks. Examples of this include the Stuxnet and Shadyrat viruses; two documented cases of intrusions into networks too complex to have been perpetrated by criminal organizations and appear to have links to intelligence organizations.[176] Incidents such as Operation Shady Rat and the use of remote access tools to commandeer computers of particular Asian countries were said to have lasted longer than two years.[177]

For data protection managers, the most chilling element in malware and cyber attacks is the complicity of some anti-virus manufacturers. A conflict of interest arises where there have been links forged between anti-virus companies and foreign intelligence services. Huawei, the aforementioned telecommunications company which attempted to purchase the U.S.-based 3Com, has established a joint venture with the U.S. anti-virus manufacturer Symantec. The partnership has obvious conflicts of interest as much of the malware and bots in distribution have some connection with advancing China's needs in technology and intelligence gathering.[178]

TELECOMMUNICATIONS BREACH

Another espionage method has been the subversion of telecommunications networks, both domestically and in foreign countries. Most reported cases of incursions are through IP rerouting, fraudulent secure socket layers (SSLs), and physical phone tampering. Reuters reported that in 2010, Internet traffic was rerouted through a foreign server controlled by a state-owned enterprise (SOE).[179] The hijacked IP belonged to the U.S. government and military sites including the DOD, the armed forces, and a few select commercial websites.[180] Intelligence services also note that digital certificates (falsely) confirming the legitimacy of websites and fraudulently-issued SSLs have been issued in order to allow foreign countries to send and receive transmissions to lure unsuspecting individuals to compromise passwords or disclose confidential trade secrets.[181]

Foreign countries are also utilizing travel and business to compromise international trade secrets.

173 Lynn, William J. III, "Defending A New Domain." 01 September 2010.

174 "Pushing Ahead of the Cyberwarfare Pack." Stratfor. 02 March 2009. http://www.uspoliticsonline.net/science-technology/51078-chinas-cyber-war-against-world.html, (accessed 03 April 2012).

175 Ibid.

176 "Building A Cyber Secure Plant." Siemens Totally Integrated Automation. 30 September 2010. http://www.totallyintegratedautomation.com/2010/09/building-a-cyber-secure-plant/, (accessed 03 April 2012).

177 Finkle, Jim. "Q+A-Massive cyber attack dubbed 'Operation Shady RAT." Reuters. 03 August 2011. http://www.reuters.com/article/2011/08/03/cyberattacks-idUSN1E76R22Q20110803, (accessed 03 April 2012).

178 "Pushing Ahead of the Cyberwarfare Pack." Stratfor. 02 March 2009.

179 Wolf, Jim. "Pentagon Says "Aware" of China Internet Rerouting." Reuters. 19 November 2010. http://www.reuters.com/article/2010/11/19/us-cyber-china-pentagon-idUSTRE6AI4HJ20101119, (accessed 03 April 2012).

180 Ibid.

181 Keizer, Gregg. "Hackers Steal SSL Certificates for CIA, MI6, Mossad." Computer World. 4 September 2011. http://www.computerworld.com/s/article/9219727/Hackers_steal_SSL_certificates_for_CIA_MI6_Mossad, (accessed 03 April 2012).

There are reported cases of China's Public Security Bureau (PSB, the Chinese equivalent of the FBI) going to Western hotel chains in China during the 2008 Olympics, with assertions that they had to install "special internet monitoring devices" that would give the PSB unprecedented access to foreign communications, and potentially even foreign trade secrets.[182]

The threat to American innovation is a direct challenge to American prosperity according to Jeffrey Goldberg of Bloomberg News; advanced American technological innovations are "the physical manifestation of American ingenuity and confidence."[183] The perpetrators of the theft that affects American prosperity are wide ranging, but most actors fall into three categories: state actors, non-state actors, and quasi-state actors.

STATE ACTORS

State actors such as state intelligence agencies have historically been the largest parties concerned with the theft of military technology, yet the dependence on economic strength and the hoarding of raw materials have become a larger priority of national security. Countries have employed Competitive Intelligence Solution (CIS) to obtain open source information in addition to utilizing spy agencies to gather intelligence. Yet, the foreign policy nightmare of getting caught operating in a foreign area has forced some intelligence services to utilize the other two actors to maintain plausible deniability.

NON-STATE ACTORS

Due to the globalization of markets and the spread of corporatism, corporations have more commonly been utilizing spy agency and espionage tactics to gain a market advantage or as part of a broader national security initiative. Companies such as the infamous 88 Queensway Group have holdings vital to strategic Chinese interests in a variety of countries, including:[184]

- Angola
- Bermuda
- Cote d'Ivoire
- Israel
- Nigeria
- Portugal
- Singapore
- United States
- Argentina
- Congo
- Indonesia
- Mozambique
- North Korea
- Russia
- Tanzania
- Venezuela

88 Queensway Group appears to have connections with Chinese State Security; however, many corporations acquire foreign technology through illegitimate means with no national security initiative and are focused solely on industrial espionage.[185] Preferred companies to be targeted are often well-regarded global producers such as: Ford, Valspar, Rockwell, GM, Boeing, BAE Systems, DuPont, Dow Chemical, Google, Apple, Lockheed Martin, Microsoft, and most recently, Renault.

QUASI-STATE ACTORS

The final actors involved in intellectual property theft are the individuals and small organizations which exploit industrial espionage for personal gain and concealed motives. While nations and companies often have similar end goals, they usually have different methods of attaining said objectives; quasi-state actors have veiled intentions and their purposes appear concealed. Incidents such as the malware embedded at Creech AFB's private servers may be viewed as part of a nationalist agenda, yet when footage of operational procedures of UAVs and UCAVs appear on insurgents' computers in Iraq, they seem to have less of a strategic and more of a tactical purpose.[186]

The "quasi-state actor" branding tends to encompass a broad, overreaching category such as terrorists, hackers, militias, and websites like WikiLeaks. Yet they all share a broad advantage over the rest of their counterparts: the United States has publicly declared that cyber attacks and espionage from foreign nations may be considered a declaration of war; yet, the quasi-state actor is difficult to declare war upon due to the difficulty of tracing origins in addition to their use of proxy servers. Furthermore, the deterrence strategy of "mutually assured destruction" prevalent during the Cold War appears to be ineffective against quasi-state actors who have no concrete, physical location or allegiance to any particular nationality. For quasi-state actors with legitimate ties to a nationality or corporation, the advantage would appear to be the plausible deniability of their actions.

182 "Pushing Ahead of the Cyberwarfare Pack." Stratfor. 02 March 2009.

183 Goldberg, Jeffrey. "Let Space Shuttle Demise Awaken Gingrich Dream: Goldberg." Bloomberg. 23 April 2012. http://www.bloomberg.com/news/2012-04-23/let-the-shuttle-s-demise-awaken-gingrich-s-space-dreams.html, (accessed 23 April 2012).

184 Levkowitz, Lee, Marta McLellan Ross and J.R. Warner. "The 88 Queensway Group: A Case Study in Chinese Investors' Operations in Angola and Beyond."

185 Ibid.

186 Shactman, Noah. "Exclusive: Computer Virus Hits U.S. Drone Fleet." Wired. 07 October 2011. http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/, (accessed 23 April 2012).

ESPIONAGE ECONOMICS AND DEMOCRACY

The globalization of markets and cultures has provided the corporate world with unparalleled access to customers and sources of manufacture. Yet, the diffusion of intellectual property in both civilian and military spheres has given rise to foreign nations acquiring technology that is crucial to American culture and values. The development of these ideas is to be accessible only in free and democratic societies wherein people are challenged to think outside the box and are rewarded for their creativity in doing so. The steps to grow democracy and the free markets to exploit the ingenuity are being skipped ahead of by nation-states that lack the means to develop their own creative potential. Rather than allowing the shifting of power to citizens or giving them the ability to operate in a heterogeneous society, nations are gaining the after-effects without putting in the necessary time to see those developments happen locally and naturally.

For those nations stealing ideas, the long-term issue becomes that the emphasis is placed on reverse-engineering and deconstruction of foreign ideas, be it a physical product or a process, while it would be better to invest their efforts in developing their own ideas. Otherwise, host nations of technologies will unveil newer technology before the reverse engineer is complete. According to Willy Shih, a professor at Harvard Business School, countries employing espionage will need to develop their own research and development process and mindset to succeed their skills of copying others.[187] He continued, noting that "many countries go through an imitation phase, but the real challenge is moving to an innovation phase."[188] China and other countries are introducing programs aimed at developing key deficiencies in market or military competitiveness. Programs such as the National High Technology Program (P863) target key deficiencies in sectors crucial to China's long-term competitiveness and national security. Those goals sometimes include the clandestine acquisition of American technologies.[189]

CONCLUSION

The concept of military size as the principle means of power has been drastically altered in the 21st century. American assets for espionage are ever increasing, as are the adversaries attempting to steal them. Drastic reforms to electronic data transmission will become battlegrounds for contentious debate in the House and Senate. For America to continue to assert its global power militarily and economically, the corporate, civil, and military worlds will have to cooperatively protect America's largest assets: its human capital and ingenuity. By securing these, the United States can remain a stronghold for valuable ideas and innovation of new ways to improve the world as a whole, and the lives of those who live on it.

187 Riley, Michael A. and Ashlee Vance, "China Corporate Espionage Boom Knocks Wind Out of U.S. Companies."

188 Ibid.

189 "Annual Report to Congress on Foreign Spies Stealing US Economic Secrets in Cyberspace." ONCIX. 2011.

Acknowledgments

Caroline V. Perricaudet ..... Director of Research
Mary A. Doyle ..... Assistant Director of Research
Jon B. Mitchell ..... Assistant Editor
Dr. Charles Murphy ..... Faculty Advisor

LIBERTY
UNIVERSITY.

The Strategic Intelligence Society is a campus club at Liberty University in Lynchburg, Virginia. The purpose of the Strategic Intelligence Society is to prepare undergraduate students for employment within the Intelligence Community by encouraging critical thinking that leads to the analysis of current events: specifically, the ability to discern intelligence from information within the fields of politics, technology, transnational issues, economics, and military policy. This is accomplished by providing the students with a multitude of opportunities, which include interactive sessions with guest speakers from various fields within government, the intelligence community, and law enforcement, a variety of intelligence-related extra-curricular opportunities, and various analytical publications. The *Strategic Informer* is the publication of the Strategic Intelligence Society, featuring articles from distinguished faculty members within the Helms School of Government at Liberty University as well as selected articles from top student contributors concentrating on current affairs pertaining to intelligence, law enforcement, and national security.

LIBERTY
UNIVERSITY.