Protecting Against Economic Espionage: Trade Secrets, Standards, and Criminal Liability

Mark A. Frazzetto
Loyola University of Chicago School of Law
Part Time Student -4L
20409 Ithaca Road
Olympia Fields, IL 60461
708-283-9824

Introduction

On February 11, 2008 Dongfan "Greg" Chung was arrested for stealing trade secrets concerning military and space vehicles, including the Space Shuttle.[1] A year and a half later Najibullah Zazi was indicted for plotting to launch a terrorist attack on U.S. soil.[2] Chung committed acts of espionage. He acquired critical U.S. technological secrets for China. Zazi is an alleged terrorist; the plot described in his indictment could have cost the lives of many U.S. citizens.[3]

The indictment against Zazi alleged he traveled to Pakistan in 2008 to receive explosives training from operatives with ties to Al-Qaeda.[4] He is also alleged to have been in "urgent" contact with Al-Qaeda operatives in Pakistan and to have tested a "volatile brew" of chemicals obtained from beauty supply stores before traveling to Queens, New York around the anniversary of the September 11, 2001 attacks.[5] From 1973 to 1996 Chung worked for Rockwell International.[6] In 1996 Boeing bought Rockwell's defense and space unit, the unit Chung worked for.[7] Chung retired from Boeing in 2002. He returned to Boeing as an independent contractor in 2003 and left Boeing again in 2006.[8] The indictment against Chung alleges that Gu Weihao of China's Ministry of Aviation wrote Chung a letter dated May 2, 1987, asking Chung for "assistance on technical issues" for various aviation programs.[9] Chung had a

[1] Rachanee Srisavasdi and Andrew Galvin, *Ex-Boeing Engineer Arrested on Spy Charges*, The Orange County Register, February, 11 2008.
[2] Carrie Johnson and Spencer S. Hsu, Terrorism Suspect Planned Peroxide Bombs, Officials Say, The Washington Post, September 25, 2009.
[3] Srisavasdi and Galvin, *supra*.
[4] Johnson and Hsu, *supra.*
[5] *Id*.
[6] Srisavasdi and Galvin, *supra*.
[7] *Id*.
[8] *Id*.
[9] Jonathan Eric Lewis, *The Economic Espionage Act And The Threat Of Chinese Espionage In The United States*, 8 J. Intell. Prop. 189, 216 2008-2009

security clearance that allowed him entrée to Boeing's trade secrets.[10] In addition to the Space Shuttle program, Chung took secrets relating the C-17 military transport aircraft and the Delta IV rocket.[11]

As the United States enters the 21st century these two cases represent disparate threats to the nation's security. At first glance it seems the threat posed by Zazi and other terrorist cases poses the greater peril. Certainly Zazi posed the more imminent threat. If Zazi had succeeded the deaths of hundreds of Americans would have been the result. But even if Zazi had succeeded the United States as a nation would have continued. While some have posited that a terrorist WMD event involving nuclear or biological weapons could cause paradigmatic changes in the political system of the United States, this is still not an existential outcome. The United States would continue to exist in some form.

Chung's activities did not present an imminent threat of loss of life. However Chung was working for the People's Republic of China ("PRC"). The PRC is the latest government of a civilization that has existed for thousands of years. For all the economic and military might of the United States, its 70 some years as a superpower is the proverbial mote in God's eye to the Chinese. China thinks strategically not in years or decades but generations. It is this paper's position that the Chung type case poses the greater danger. Economic espionage, in both its human and cyber variants, is costing the United States monetarily and also its military and technological advantages. Economic espionage, in other words, is threatening this Nation's very position in the world. What makes this trend even more worrisome is that one of the worst offenders is China.

[10] Srisavasdi and Galvin, *supra*.
[11] *Id*.

There are many aspects to the danger posed by economic espionage: diplomatic, economic, and military. This paper focuses on the legal aspect. This paper argues that in the area of economic espionage, both the existing and proposed statutes addressed to this peril are woefully inadequate.

The paper begins by examining the nature of the threat posed by economic espionage and China in particular, including both the traditional economic espionage conducted by human actors as well as the increasing use of cyber attacks. The paper examines the statutory tools currently provided to law enforcement, and also examines proposed legislature. This paper focuses on the economic espionage statutes whose purpose is to defend trade secrets. Export controls, as such, are beyond the scope of this paper. Given the nature of the threat, these economic espionage statutory tools are found wanting. The paper than argues that standards for cyber and traditional trade secret security be promulgated by Congress or Congress' designee (as opposed to only cyber security standards under proposed legislation). This paper further argues that companies, management, and employees who violate these standards are criminally reckless. Finally, under federal criminal law as interpreted by the United States Supreme Court these violators are culpable and should be held criminally liable.

Nature of the Threat

In his classic treatise on military strategy "The Art of War" the Chinese general Sun-Tzu wrote "to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting."[12] In his 1997 book, "War by Other Means", author John J. Fialka writes "War to the Chinese is a matter of guile, feints, endless patience, and above all spies, whose intelligence reveals the enemy's weak point, that when

[12] Sun Tzu, *The Art of War* (Project Guttenburg ebook, Lionel Giles trans., http://www.gutenberg.org, 1994, ebook #132)

struck, makes the battle short lived and unnecessary."[13] This strategy of feint, deception, and patience seems especially well suited to take advantage of American corporate management's fealty to its stockholders, and consequently the daily fluctuation of stock prices. One American CEO was once quoted as saying: "We're in the business of making money for our stockholders. If we have to put jobs and technology in other countries, than we go ahead and do it." [14] In addition to the losses in jobs, if the intellectual property this displaced technology represents is not adequately protected (it isn't, *infra*) the loss of these trade secrets severely damages the United States' geopolitical position and more importantly creates profound vulnerabilities the Nation has not faced before.

In the 1990s American aerospace companies, including the company led by the aforementioned CEO, contracted with Chinese factories to make fuselages and nose cones for commercial airliners.[15] As the Chinese learned to make these components "emerging versions of Chinese fighter planes were suddenly improving; their fuselages were better made and their aluminum skins were better."[16] Further, as American aerospace and other companies invested money and manufacturing capacity in China, China in turn would direct its economic espionage efforts in the United States at these same companies.[17] In effect, these companies were funding the economic espionage efforts being directed against them.[18]

Little has changed since the last decade of the 20th century. Generally, "The threat to the United States from foreign economic intelligence collection and industrial espionage has

[13] John J. Fialka, *War by Other Means*, 19 (1997).
[14] *Id*. at 32.
[15] *Id*. at 32.
[16] *Id*. at 32.
[17] *Id.* at 22.
[18] *Id*. at 22.

continued unabated."[19] The FBI has stated that a third of all economic espionage cases can be linked to China.[20] "For many years China has used its military intelligence capabilities for economic purposes."[21] One author has stated that the "workforce available to the Chinese government and its corporations [for] gathering information in the United States is nearly limitless."[22] Accordingly, the FBI has increased the number of agents assigned to economic espionage from 150 agents in 2001 to more than 350 agents as of the summer of 2007.[23]

Additionally, China in 1986 launched the "863" program. This program's mission is to "acquire and develop technology acquire and develop biotechnology, space technology, information technology, laser technology, automation technology, energy technology, and advanced materials."[24] The 863 program is run by China's central government and linked to the Chinese military.[25] The FBI believes the 863 program is implicated in many economic espionage cases.[26]

In addition to the threat posed by human actors, economic espionage is increasingly becoming the objective of cyber attacks. "Cyber threats are increasingly pervasive and are rapidly becoming a priority means of obtaining economic and technical information. Reports of new cyber attacks against US Government and business entities proliferated in FY 2008."[27] A proposed federal statute finds that "industrial espionage that exploits weak cybersecurity dilutes our investment in innovation while subsidizing the research and development efforts of foreign

[19] National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* FY 2008 1 (2009).
[20] Lewis, *supra*, at 192.
[21] *Id*. at 205.
[22] Larry M. Wortzel, *Sources and Methods of Foreign Nationals Engaged in Economic and Military Espionage*, Heritage Lectures, September 15, 2005 at 1.
[23] Lewis, *supra*, at 192.
[24] Wortzel, *supra* at 2.
[25] Lewis, *supra*, at 208.
[26] *Id*.
[27] National Counterintelligence Executive, *supra*, at 13.

competitors."[28] The Obama Administration's cybersecurity review states that "a growing array of state and non-state actors are compromising, stealing, changing, or destroying information and could cause critical disruptions to U.S. systems."[29] Foreign adversaries have been able to "penetrate poorly protected U.S. computer networks and collect immense quantities of valuable information."[30] Consequently,

> Porous information systems have allowed our cyberspace opponents to remotely access and download critical military technologies and valuable intellectual property – designs, blue prints, and business processes - that cost billions of dollars to create. The immediate benefits gained by our opponents are less damaging, however, than is the long term loss of U.S. economic competiveness. We are not arming our competitors in cyberspace; we are providing them with the ideas and designs to arm themselves and achieve parity. America's power, status, and security in the world depend in good measure upon its economic strength; our lack of cybersecurity is steadily eroding this advantage.[31]

China has a finger in this pie. The Chinese military designs viruses to attack its adversaries' computer systems.[32] This has resulted in a new and dangerous military capability which allows China to infiltrate worldwide computer networks.[33]

Against this backdrop China has experienced thirty years of economic growth, growth which has seen China's economy double nearly three times over. This surge has no equal in modern times.[34] Manufacturing increasingly shifts to China from the United States and the rest of the world.[35] This includes consumer goods and big ticket items as well: cars, trucks, planes,

---

[28] Cybersecurity Act of 2009, S. 773, 111th Cong. § 2(2) (2009).
[29] Executive Office of the President, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* 17 (2009), available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
[30] Ctr. for Strategic and Int'l Studies, *Securing Cyberspace for the 44th Presidency* 11 (2008), available at http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.
[31] *Id*. at 13.
[32] Lewis, *supra*, at 229.
[33] *Id*. at 227 – 228.
[34] Ted C. Fishman, *China Inc.*, 12 (2005).
[35] *Id*. at 15.

ships, networks, factories, submarines, satellites, and rockets.[36] Additionally, China's plunder of intellectual property creates a "massive global subsidy worth hundreds of billions of dollars to its businesses and people."[37] The economic result is a sort of neo-colonialism, where China's vast "counterfeiting schemes act on the rest of the world as colonial armies once did, invading deep into the economies of their victims, expropriating their most valued assets, and in doing so, undermining their victims' ability to counter." [38]

The United States' military advantage, as well as the global military balance, is impacted as well. China has increased its GDP from 1.95 trillion in 2000 to a projected 4.19 trillion (USD) in 2008.[39] This enabled China to devote increased resources to its military capacity without hindering its economy.[40] "As a result, China continues a two-decade trend of double digit percentage annual increases in its military budget."[41] One of the sources for Chinese military growth is foreign military technology acquisition; and besides actual purchases China acquires military technology by "spin-offs from foreign direct investment and joint ventures in the civilian sector, technical knowledge and expertise of students returned from abroad, and state-sponsored industrial espionage to increase the level of technologies available to support military research, development, and acquisition."[42]

As the preceding shows, the nature of the threat is quite serious. Chinese military thinking looks at war holistically. Sun-Tzu's admonition that a truly victorious general never fights a battle is echoed in modern Chinese strategic planning. The People's Liberation Army's military science text observes that ""war is not only a military struggle, but also a comprehensive

[36] *Id*.
[37] *Id*. at 252.
[38] *Id*.
[39] United States Department of Defense, *Military Power of the People's Republic of China*, Annual Report to Congress VII (2009).
[40] *Id*.
[41] *Id*. at 31.
[42] *Id*.

contest on fronts of politics, economy, diplomacy, and law." [43] Economic espionage is incorporated into this strategy. While there a variety of responses and programs the United States has or will make to this threat, the focus of this paper now shifts to how intellectual property is protected from foreign human actors and cyber attack domestically. In particular, the emphasis will be placed on how federal criminal law is applied to this new kind of warfare.

Federal Criminal Statutes and Economic Espionage

Congress enacted the Economic Espionage Act ("EEA") in 1996; its purpose is to federally criminalize acts of economic espionage.[44] The act criminalizes both the theft of trade secrets and proprietary information by both private individuals and corporations and by foreign governments.[45] The act defines foreign economic espionage, this paper's concern, when a human actor "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly…"[46] The EEA is a criminal statute and so gives "the federal government authority to prosecute those who engage in trade secret theft against private American corporations."[47] Importantly, no liability is extended to companies and their agents who fail to provide sufficient safeguards for proprietary information and/or fail to report the theft of proprietary information when such theft occurs. Nor does the EEA provide any standards for companies who wish to provide sufficient safeguards for proprietary information.

The primary statute that federally criminalizes hacking is 18 U.S.C. 1030, which concerns fraud and related activity in connection with computers. In particular, the act makes it a federal crime for anyone who illegally accesses proprietary information for the benefit of a

[43] Department of Defense, *supra*, at 14.
[44] *See* 18 U.S.C. §§ 1831 - 1839 (1996).
[45] Lewis, *supra*, at 190.
[46] 18 U.S.C. § 1831(a) (1996).
[47] Lewis, *supra*, at 202.

foreign government.[48] Again, however, this statute provides no guidance as to computer security standards. Of course, the statute therefore can't extend any liability to companies or their agents who violate such standards, or who fail to report theft of valuable intellectual property.

One piece of proposed legislature is interesting in that does call for the formation of standards and even a compliance mechanism. The bill, introduced in the Senate, is called the "Cybersecurity Act of 2009"[49] and currently sits in the Senate Committee on Commerce, Science, and Transportation. The bills provisions call for among other things, the establishment of standards and a compliance requirement. The bill mandates that, within one year of the statute's enactment, "the National Institute of Standards and Technology shall establish measurable and auditable cybersecurity standards for all Federal Government, government contractor, or grantee critical infrastructure information systems and networks".[50] As to compliance, the bill, if enacted, would require

> "compliance with the standards developed by the Institute under this section by software manufacturers, distributors, and vendors; and shall require each Federal agency, and each operator of an information system or network designated by the President as a critical infrastructure information system or network, periodically to demonstrate compliance with the standards established under this section."[51]

However, the standards relate to software primarily and there is indication what failure to comply results in for entities or individuals who don't meet bill's standards. There are no prescriptions for the preservation of trade secrets nor is there an extension of liability to those organizations or their agents who violate the standards.

[48] *See* 18 U.S.C. 1030(a).
[49] S. 773, 111th Cong. (2009).
[50] *Id.* at §6(a).
[51] *Id.* at §7(d)(2).

Finally, there is the ‘‘Cybersecurity Enhancement Act of 2010’’.[52] This proposed statute has passed the House and currently sits in the Senate Committee on Commerce, Science, and Transportation. The bill would develop a cybersecurity workforce, coordinate and prioritize federal research and development, and promote cybersecurity education and awareness for the general public.[53] The bill does nothing to address the issues of standards and liability.

It is this paper's position that all these statutes fail because they do nothing to assign responsibility to the United States' primary source of vulnerability to economic espionage: its corporations, especially those corporations that do business with inimical foreign nations who, like China, seek to compete with the United States itself. Further, this lack of responsibility on the part of corporate America is most damaging when a nation like China regards economic competition as a form of warfare.

American corporations are on the front line of this struggle. "Individual firms decide whether and how to protect trade secrets."[54] Further, "The private sector . . . designs, builds, owns, and operates most of the network infrastructures that support government and private users alike."[55] At the same time, "The damage a clever spy can wreak in a supposedly peaceful economic setting is 'often invisible and decisive.' And the victim – especially if he must answer to angry stockholders - is not often inclined to want a history."[56]

As noted above, the statutes enacted or proposed by Congress do not really address these issues. The EEA was not "not formulated with the aim of encouraging trade secret holders to invest in additional information security measures; proponents of the statute argued that the

[52] H. R. 4601, 111th Cong. (2010).
[53] *Id.*
[54] Aaron J. Burstein, *Trade Secrecy As An Instrument Of National Security? Rethinking The Foundations Of Economic Espionage*, 41 Ariz. St. L.J. 933, 962 (2009).
[55] Executive Office of the President, *supra*, at 17.
[56] Fialka, *supra*, at XIII.

government should pay the costs of reducing economic espionage through law enforcement."[57] The other statutes mentioned, with the possible exception of the Cybersecurity Act of 2009, suffer from the same malady. Given the nature of the threat described above, they are inadequate because they don't apply sufficient pressure on the private sector to protect themselves – and, by extension, the United States.

Further, there is nothing in the current economic espionage statutory regime that addresses the fact that companies often keep thefts of their proprietary information secret. "The only thing a company will protect more than its information is the fact that they've lost it." [58] Evidence about Internet based attacks are difficult to obtain; even if it is obtained the perpetrators are often in another country.[59] Even with private sector cooperation traditional economic espionage cases are difficult to assemble.[60] The failure of American companies to report trade secret theft only exacerbates the situation.

American CEOs seem more concerned with the bottom line than with the threats to national security posed by economic espionage. Recall the statement made by an American CEO earlier: "We're in the business of making money for our stockholders." "If we have to put jobs and technology in other countries, than we go ahead and do it." Meanwhile, Chinese engineers were "crawling all over" manufacturing facilities the CEO's company had moved to China.[61] American companies simply do not seem to consider the larger question - "[I]f you're losing American jobs and American technology while simultaneously building an industrial base in China that will compete with you, there is in fact great damage going on."[62]

---

[57] Burstein, *supra*, at 949.
[58] Fialka, *supra*, at 15.
[59] Burstein, *supra*, at 972 - 973.
[60] *Id*.
[61] Fialka, *supra*, at 31 – 34.
[62] *Id*. at 39.

A Proposal: Standards for Trade Secret Protection and Criminal Liability for Failing to Meet Them

Whether we like it or not we have been engaged by China in a struggle that could cost the United States its position in the world. The United States, "the last superpower", would see itself replaced by a totalitarian regime that shows no sign of moving any closer to democracy.[63] What happens after such a geopolitical shift of this magnitude occurs simply can't be good for the long term future of the United States.

Given these stakes, it is nothing short of reckless for American companies to allow their trade secrets to be stolen by foreign governments, especially when there is a solid probability that the foreign government is the PRC. However, the current statutory regime looks at these companies as "victims" who have no responsibility to protect their proprietary intellectual information beyond the minimum statutory requirements required to classify such property as "trade secrets".

As a first step, Congress needs to promulgate stringent standards that require American businesses to protect trade secrets above and beyond what it is currently required. Because trade secrets can be stolen both by human actors and by cyber attack, the standards need to incorporate provisions for both eventualities. Also, since successful cyber attacks can be accomplished by individuals thousands of miles away from their targets, the standards must apply to all U.S. businesses that have a presence in cyberspace. The standards can be calibrated to the size of the business and the economic and security impact the loss of a particular trade secret may cost the nation as a whole – looser standards for a hardware store as opposed to more stringent standards

[63] *See* David Shambaugh, *The Year China Showed its Claws*, Brookings Institution 1 (2010), available at http://www.brookings.edu/opinions/2010/0216_china_shambaugh.aspx.

for a multinational corporation. These details can be worked out and are beyond the scope of this paper.

The greater question is how to enforce a set of standards promulgated by Congress to protect trade secrets. This paper has described the nature of the threat foreign economic espionage poses to the United States. Foreign economic espionage is not simply "a cost of doing business"; rather, it poses a long term strategic threat to the United States' position in the world. As such, the harm done by foreign economic espionage is not just to the companies involved but to the well being of the nation as a whole. Accordingly, it is well within Congress' purview to establish sanctions for those who fail to protect trade secrets according to Congress' specifications. Further, such sanctions should be criminal in nature.

But how can corporations and their agents be held criminally culpable? Are they not simply businesses doing business? The most important pillar in the foundation of criminal law is the concept of moral blameworthiness. That is, no one will convicted (or punished) of a crime unless the act or omission was morally blameworthy.[64] The United States Supreme Court will demand that the "that the government prove moral culpability when statutory language might reach conduct that is 'not inevitably nefarious'; that is, conduct that is not inevitably blameworthy."[65] Are companies who don't adhere to standards to protect trade secrets promulgated by Congress morally blameless?[66]

In deeming whether conduct is criminally culpable, the Court has increasingly "construed federal statutes to impose broader mens rea requirements in cases in which the federal interest in

[64] Stephen F. Smith, *Proportionality And Federalization*, 91 Va. L. Rev. 879, 882 (2005).
[65] John Shepard Wiley Jr., *Not Guilty By Reason Of Blamelessness: Culpability In Federal Criminal Interpretation*, 85 Va. L. Rev. 1021, 1035 (1999) quoting Ratzlaf v. United States, 510 U.S. 135, 144 (1994).
[66] The issue of fair notice is also germane to the question of culpability. Fair notice is largely a question of statutory drafting and beyond the scope of this paper.

regulating the subject matter at issue is comparatively high."[67] In the case of companies who fail to adequately protect their trade secrets, and thereby allow foreign nations who are competing with the United States to gain economic advantage, the federal interest is high indeed.

The specific level of moral culpability that fits into what the Supreme Court calls "broader mens rea requirements" is criminal recklessness. The Model Penal Code defines recklessness as the "material element of an offense when [the actor] consciously disregards a substantial and unjustifiable risk that the material element exists or will result from his conduct."[68] Under the Model Penal Code recklessness is part of a descending order of culpability: purpose, knowledge, recklessness, and negligence.[69] Federal criminal law, which is not based on the Model Penal Code, generally recognizes two levels of culpability: purpose and knowledge.[70] However in its 1994 decision *Posters 'N' Things v. United States* the Supreme Court defined "knowledge" type culpability to mean:

> Further, we do not think that the knowledge standard in this context requires knowledge on the defendant's part that a particular customer actually will use an item of drug paraphernalia with illegal drugs. It is sufficient that the defendant be aware that customers in general are likely to use the merchandise with drugs. Therefore, the Government must establish that the defendant knew that the items at issue are likely to be used with illegal drugs. *Posters 'N' Things v. United States*, 511 U.S. 513, 524 (1994).

Under this standard, therefore, a company that does not subscribe to standards promulgated by Congress to protect trade secrets would have to know only that its trade secrets are *likely* to be stolen by foreign interests – given the current global environment not a huge leap. In subsequent decisions, the Court has adhered to the rule of *Posters 'N' Things. See Dixon v. United States* ("the term 'knowingly' merely requires proof of knowledge of the facts that

[67] Note, *Mens Rea In Federal Criminal Law*, 111 Harv. L. Rev. 2402, 2402 (1998).
[68] Model Penal Code § 2.02(2)(c).
[69] *Id*. at § 2.02(2).
[70] Wiley, *supra*, at 1030.

constitute the offense.");[71] *see also Babbit v. Sweet Home* ("Secretary's conclusion that activities not intended to harm an endangered species, such as habitat modification, may constitute unlawful takings under the ESA").[72]

After being put on fair notice by Congress' promulgation of trade secrets protection standards, a company, under federal criminal culpability standards as interpreted by the Supreme Court, is guilty of criminal negligence if it does not meet those standards whether it intended for its trade secrets to be stolen or not.

Conclusion

China does not defeat its rivals, it absorbs or rejects them. The Mongol horde of Genghis Khan conquered China; by the time of his grandson Kublai's reign the Mongols were speaking Chinese. The same happened to the Manchus. The 19th century European imperial powers receded. Even the Japanese armies of World War II were slowly being swallowed by the Chinese.

Terrorists are capable of truly horrific acts and deserve the attention they receive from the U.S. national security apparatus. However, the United States continues to ship manufacturing capacity to China. The Chinese intelligence services continue to prod and pilfer U.S. technological and other trade secrets both here and in China. The absorption of the United States has begun.

We need tougher actions against those who would put profit before country. The long range costs to this country and its position in the world have far greater import than a particular company's stock price.

[71] *Dixon v. United States*, 548 U.S. 1, 5 (2006) quoting *Bryan v. United States*, 524 U.S. 184, 193 (1998).
[72] *Babbit v. Sweet Home*, 515 U.S. 687, 701 (1995)