THE ECONOMIC ESPIONAGE ACT AND THE THREAT OF CHINESE ESPIONAGE IN THE UNITED STATES

Jonathan Eric Lewis*

Abstract

With the advent of computers and the Internet, American national security became inexorably linked with the safeguarding of the nation's trade secrets and critical technological infrastructure. In light of the threat posed by corporate and economic espionage, Congress passed the Economic Espionage Act in 1996. The Economic Espionage Act was the first federal statute to criminalize the theft of trade secrets.

The Economic Espionage Act had two primary provisions, one criminalizing domestic economic espionage, and another criminalizing trade secret theft intended to benefit a foreign power. Since the passage of the Act over a decade ago, the vast majority of law review articles and commentaries have focused on the Economic Espionage Act's domestic provision. This article seeks to fill a gap in the existing scholarship by focusing mainly on the provision that criminalizes trade secret theft intended to benefit a foreign power. As the overwhelming number of cases under this provision involved a connection with the Chinese government, this article seeks to analyze the efficacy of the Economic Espionage Act by studying recent cases of Chinese economic espionage in the United States. As such, this article takes a comprehensive look at Chinese economic and military rivalry and focuses on several recent high-profile economic espionage cases in California. Finally, I draw parallels between the problem of economic

* Jonathan Eric Lewis, University of Connecticut School of Law, J.D. expected, May 2010. The author would like to thank Professor Lewis Kurlantzick for his comments.

espionage that Congress responded to in 1996 and the problem of hacking and cyber espionage that the Obama Administration considers a vital national security concern.

Introduction

During the Cold War, Soviet espionage posed a danger to American national security. The targets of Soviet espionage were primarily military and political.[1] The best-known Cold War espionage case was *United States v. Rosenberg*, in which Ethel and Julius Rosenberg were convicted of violating the Espionage Act, 50 U.S.C. § 32.[2] The Rosenbergs were eventually executed for having passed atomic secrets to the Soviet Union.[3]

With the end of the Cold War, the American industrial base became the new target of foreign espionage.[4] Foreign intelligence agencies began devoting substantial efforts to spying upon American corporations seeking to steal American trade secrets.[5] For instance, in 1990, China's Ministry of State Security, ("MSS") formed as a joint intelligence and espionage service, sent Bin Wu, a university professor, to the United States to acquire American high-tech items.[6] Wu was subsequently caught by the Federal Bureau of Investigation ("FBI") in a complex scheme in which he sought to acquire night-vision technology for the Chinese military.[7] The America of the 1990s had "become the chief target of the world's economic spies."[8] Because of the dire threat of a foreign intelligence service pilfering American technology, Congress finally

---

[1] *See* Darren Tucker, Comment, *The Federal Government's War on Economic Espionage*, 18 U. PA. L. REV. 1109 n.3 (1997).
[2] *United States v. Rosenberg*, 195 F.2d 583 (2nd Cir., 1952); 50 U.S.C. § 32 is now codified at 18 U.S.C. § 794.
[3] *See* Sam Roberts, *Figure in Rosenberg Case Admits to Soviet Spying*, N.Y. TIMES, Sept.11, 2008, *available at* http://www.nytimes.com/2008/09/12/nyregion/12spy.html.
[4] 104 CONG. REC. S12201-14 (daily ed. Oct. 2, 1996), *available at* http://www.usdoj.gov/criminal/cybercrime/EEAleghist.htm (discussing the Economic Espionage Act of 1996).
[5] *Id.*; *see also*, IRA WINKLER, SPIES AMONG US 81 (2005) (contending that "[a]lmost all foreign governments put economics as the main focus of their intelligence efforts").
[6] JOHN J. FIALKA, WAR BY OTHER MEANS: ECONOMIC ESPIONAGE IN AMERICA 21-22 (1997).
[7] *Id.* at 25, 28.
[8] *Id.* at 4.

took action and passed the Economic Espionage Act of 1996 ("EEA" or "the Act"), which made the theft of trade secrets a federal crime.[9] The Act was a "single vehicle [that prohibited] the theft of trade secrets and proprietary information by both private individuals and corporations and by foreign governments acting on their behalf . . ."[10] The Act was the first federal statute that provided criminal penalties for the misappropriation of trade secrets.[11]

Testifying on the passage of the Economic Espionage Act of 1996, Senator Kohl of Wisconsin stated that, "[s]ince the end of the cold war, our old enemies and our traditional friends have been shifting the focus of their spy apparatus. Alarmingly, the new target of foreign espionage is our industrial base. But for too many years, we were complacent and did not heed these warnings."[12] FBI Director Louis Freeh testified that in 1996 the FBI was investigating allegations of economic espionage against the United States by over twenty different countries.[13] The CIA noted that France, Israel, Russia, China, and Cuba were engaged in economic espionage against the United States.[14]

Over a decade has elapsed since the passage of the Economic Espionage Act of 1996; however, the threat of foreign-sponsored economic espionage has by no means subsided.[15]

---

[9] *See* 18 U.S.C. §§ 1831-39 (1996).
[10] http://www.usdoj.gov/criminal/cybercrime/EEAleghist.htm.
[11] Ronald Abramson *Theft of Trade Secrets Addressed*, N.Y. L.J. Apr. 28, 1997.
[12] 142 CONG. REC. S10,882-02 (daily ed. Sept. 18, 2006) (statement of Sen. Kohl).
[13] *See* Terry Philip Segal, *The Economic Espionage Act of 1996: A New Federal Prosecution Tool in the Fight Against Espionage and Trade Secret Theft*, 42-OCT B. B.J. 10, September/October 1998. For a cynical take on the FBI's role in combating economic espionage, *see* Pamela B. Stuart, *The Criminalization of Trade Secret Theft: The Economic Espionage Act of 1996*, 4 ILSA J. INT'L & COMP. L. 373, 374 (1998) ("While its full implications are not yet apparent, the passage of the Economic Espionage Act of 1996 might be viewed as the FBI agent full employment act . . . . It is yet one more step in the progress of the effort to criminalize conduct that was formerly of interest only to commercial lawyers.").
[14] Chris Carr, Jack Morton, & Jerry Furniss, *The Economic Espionage Act: Bear Trap or Mousetrap?*, 8 TEX. INTELL. PROP. L.J. 159, 162 (2000).
[15] According to the FBI, billions of dollars are lost every year to foreign competitors who deliberately target economic intelligence and trade secrets. *Investigative Programs Counterintelligence Division: Focus on Economic Espionage*, http://www.fbi.gov/hq/ci/economic.htm (retrieved on September 19, 2008); for a reference to French

According to the FBI, China is currently linked to about a third of all economic espionage cases.[16] Due to the severity of the threat, the FBI increased the number of agents working on countering alleged Chinese espionage from 150 agents in 2001 to more than 350 agents as of summer 2007.[17] According to one author writing nearly a decade ago, "[b]y far the largest, most problematic player is the People's Republic of China, ("PRC"), a nuclear power which is using U.S. technology and some of the profits from a ballooning trade surplus with the United States to modernize its army, navy, and air force."[18] U.S. allies also engage in economic espionage against the United States; however, due to the particular economic and military challenges posed by China, I shall focus on Chinese espionage in this paper.[19]

Chinese economic espionage is likely to increase in the years ahead and to appear in different forms. This paper is the first to synthesize the numerous recent Economic Espionage Act cases involving Chinese espionage. I argue that the Economic Espionage Act is a necessary, but not sufficient, response to the threat of Chinese-government-sponsored economic espionage activities that imperil American national security.[20] Although the drafters of this legislation were prescient, with the exponential growth of the Internet and advanced technology in the decade since, the threat of economic espionage now must be linked with the threat of foreign-

---

economic espionage *see*, *Air France Denies Spying on Travelers*, INT'L HERALD TRIB., Sept. 14, 1991, *available at* http://www.iht.com/articles/1991/09/14/spy_.php.

[16] David J. Lynch, *FBI Goes on Offensive vs. Tech Spies*, USA TODAY, July 24. 2007, 1B, *available at* http://usatoday.com/printedition/money/20070724/china_spy2.art.htm; *see also* David J. Lynch, *Law Enforcement Struggles to Combat Chinese Spying*, USA TODAY, July 23, 2007, *available at* http://www.usatoday.com/printedition/news/20070723/1a_cover23.art.htm ("About one-third of all economic espionage investigations are linked to Chinese government agencies, research institutes or businesses, according to Bruce Carlson of the FBI's counterintelligence division, who leads the bureau's efforts to combat Chinese spying."). France and Israel also engage in significant economic espionage against the United States. *See,* WINKLER, *supra* note 5, at 93.

[17] http://usatoday.com/printedition/money/20070724/china_spy2.art.htm.

[18] FIALKA, *supra* note 6, at 12.

[19] *Economic Espionage: Hearing Before the S. Select Intelligence and Terrorism Comm.*, S. Hrg. 104-499 (1996) (statement of U.S. Gen Accounting Office).

[20] FIALKA, *supra* note 6, at 206 (Fialka, writing in the late 1990s, called the EEA a "good start").

government supported computer hacking designed not only to steal trade secrets, but also to disrupt our critical technological infrastructure.[21]

The question is whether federal criminal law is the best mechanism for dealing with a complex economic, political, and potential military threat from a 21st-century superpower. On the one hand, the EEA has given federal prosecutors a framework to prosecute persons who, with the aim of benefiting the Chinese governmental-industrial complex, seek to steal American trade secrets. The EEA, however, cannot alone counter the threat posed by Chinese espionage. The federal government should employ the EEA along with political and diplomatic initiatives aimed at mitigating the threat of Chinese economic espionage. That said, Congress should revise the Economic Espionage Act to include stricter penalties for the theft of trade secrets intended to benefit a foreign government or entity. Furthermore, Congress should enact new federal legislation that makes it a federal crime to aid knowingly, conspire to aid, or to engage in computer hacking designed to steal trade secrets or to disrupt American corporate or governmental computer systems with the intent of benefiting a foreign government or entity. While there is already federal legislation criminalizing the unlawful use of a computer, Congress should enact new, comprehensive anti-hacking legislation that would give federal prosecutors further investigative authority and prosecutorial power to counteract foreign-government-sponsored hacking.

This paper is divided into four parts. First, I shall discuss the myriad ways in which legislators and commentators have defined economic espionage and, for coherence, shall focus on Congress's definition of economic espionage in the Economic Espionage Act of 1996.

[21] *See* Ellen Messmer, *Cyber Espionage: A Growing Threat to Business*, PC WORLD, Jan. 21, 2008, *available at* http://www.pcworld.com/printable/article/id,141474/printable.html.

Second, I will analyze several cases in which federal prosecutors have employed the Economic Espionage Act in order to prosecute persons engaged in economic espionage intended to benefit the Chinese government.[22] Third, I shall argue, in light of the serious national security threat posed by Chinese governmental economic espionage in the United States, the EEA should be revised to increase criminal penalties and to redefine what acts constitute economic espionage. I shall also argue that the EEA, while an effective statute, cannot serve as a substitute for a comprehensive political and diplomatic strategy aimed at countering Chinese espionage. Fourth, I shall examine the vast number of computer hacking incidents of the past two years, incidents in which intelligence officials attribute to the Chinese government. I will argue that the EEA provides a good model for a federal criminal anti-hacking law that should be designed as a counterintelligence provision.

I. The Economic Espionage Act of 1996 (EEA)

A. Defining Economic Espionage

What exactly is economic espionage? According to the Office of the National Counterintelligence Executive, "[t]here is no consensus within the US government on the definition of economic espionage."[23] The Counterintelligence Report, however, decided to use the definition employed by the Attorney General, namely "the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information; proprietary economic information, or critical technologies."[24] Economic espionage, or high-technology espionage, has been colorfully defined as "a high-stakes cloak-and-dagger spy game – the theft of critical

[22] As of September 2006, the FBI's office in Palo Alto, California, was investigating "approximately a dozen economic espionage cases with suspected ties to China." K. Oanh Ha, *Silicon Valley a Hotbed of Economic Espionage?*, THE ARGUS (Fremont-Newark, CA), Sept. 29, 2006, *available at* WL 16889362.
[23] NATIONAL COUNTERINTELLIGENCE EXECUTIVE, ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE 2001 (2001), *reprinted in* DAVID J. LOUNDY, COMPUTER CRIME, INFORMATION WARFARE, AND ECONOMIC ESPIONAGE 584, 585.
[24] *Id*.

American technology and trade secrets by foreign companies and governments."[25] *Political-military* espionage occurs when a foreign intelligence agency seeks to infiltrate another country's *political* system to influence clandestinely the political process or to gain access to government-held industrial and military secrets. *Economic* espionage occurs when a foreign intelligence agency spies on foreign *corporations and industry* in order to gain a competitive advantage or to utilize foreign technology as a means of bolstering its military capabilities.[26]

One writer has succinctly defined economic espionage as "business spying against an American company. More specifically, it's theft, copying, or destruction of a trade secret, meant to harm the trade secret's owner and to benefit a foreign government or its interests."[27] Canadian intelligence has defined economic espionage as "illegal, clandestine, coercive, or deceptive activity engaged in or facilitated by a foreign government designed to gain unauthorized access to economic intelligence, such as proprietary information or technology, for economic advantage."[28] Yet another author has defined economic espionage as "a foreign government's sponsoring, coordinating, or assisting intelligence efforts directed at a domestic government, corporation, establishment, or person that involves the unlawful or clandestine targeting or acquisition of (1) trade secrets or (2) sensitive financial, trade, or economic policy information."[29]

---

[25] Robert Cohen, *Business Replaces Military for Spies*, NEWARK STAR-LEDGER, May 4, 2001, *available at* WL 1097274.
[26] *See* Karen Sepura, *Economic Espionage: The Front Line of a New World Economic War*, 26 SYRACUSE J. INT'L L. & COM. 127, 129 (1998) (defining traditional espionage as "the way in which spies acquire an enemy's military secrets").
[27] John Mangel, *Economic Espionage Losses in the Billions, Experts Say*, CLEVELAND PLAIN DEALER, July 20, 2001, *available at* WL 251403.
[28] Sepura, *supra* note 26, at n.5.
[29] Tucker, *supra* note 1, at 1112.

Notable in the latter definition is that the focus of the foreign government's intelligence efforts could be on a "domestic government," or a "[domestic] corporation."[30] Thus, according to this author's definition, economic espionage would occur when the foreign intelligence service of Country X spies on either American Agency Y or American Corporation Z. The problem with this definition is that it is too broad. Foreign intelligence service X's spying on American Agency Y is traditional political-military espionage because the target is the American government. When foreign intelligence service X devotes its energies to spying on private American Corporation Z, X is conducting economic espionage.

For the purposes of this paper, the working definition of economic espionage comes from § 1831 of the Economic Espionage Act of 1996, which deals with foreign-sponsored espionage.[31] Section 1831(a) defines economic espionage as the acts of a person who "knowingly performs targeting or acquisition of trade secrets to . . . knowingly benefit any foreign government, foreign instrumentality, or foreign agent."[32] Unlike the broader definition of economic espionage as including the targeting of "sensitive financial, trade, or economic policy

---

[30] *Id.*

[31] 18 U.S.C. § 1831(a)-(b) (1996). Statute reads in full:
1831. Economic espionage
(a) In general.--Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly--
(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
(4) attempts to commit any offense described in any of paragraphs (1) through (3); or
(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.
(b) Organizations.--Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

[32] 18 U.S.C. § 1831(a) (1996); *see also Investigative Programs Counterintelligence Division: Focus on Economic Espionage*, http://www.fbi.gov/hq/ci/economic.htm (retrieved on Sept. 19, 2008).

information," the EEA defines economic espionage solely in terms of "trade secrets."[33] Although the statutory text of the EEA does not preclude the holder of the misappropriated trade secret from being an American governmental agency[34], the legislative history of the EEA makes it reasonably clear that Congress intended to protect *corporate* trade secrets.[35]

Notwithstanding the statutory definition of economic espionage, a consideration of how Congress might have defined it differently bolsters the notion that Congress defined economic espionage correctly.. Indeed, Congress might have adopted the Canadian intelligence service's definition and created a statute that singularly criminalized foreign-government-sponsored espionage of a purely economic nature.[36] Such a statute would have had a broader reach than the EEA.[37] Congress, however, decided to criminalize the theft of trade secrets by both foreign intelligence services and corporate competitors in separate provisions, §§ 1831 and 1832.[38] While the statutory definition of economic espionage in the EEA is the one that federal prosecutors must rely on in prosecuting cases involving the theft of trade secrets, Congress, as in all cases, retains the option to revise the statutory definition in the future.

---

[33] 18 U.S.C. § 1831(a)(1).

[34] *See* 18 U.S.C. § 1831(a)(1) ("obtains a trade secret"). The statutory text of Section 1831 does not explicitly mention who the holder of the trade secret would have to be in order for the EEA to come into play. For a definition of "trade secret" under the EEA and subsequent case law, *see* Part I.C, *infra*.

[35] *See* H.R. REP. No. 104-788 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 1996 WL 532685 ("[T]here is considerable evidence that foreign governments are using their espionage capabilities against American companies.").

[36] The traditional statutory espionage provision is found at 18 U.S.C. § 794 ("Gathering or delivering defense information to aid a foreign government") (effective Oct. 11, 1996). 18 U.S.C. § 794(a) criminalizes the conduct of "[w]hoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits . . . either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense . . . ."

[37] The Chinese government-sponsored espionage in the United States which seeks to steal corporate trade secrets often has a traditional military espionage component. For instance, there are several cases when the Chinese government or its agents have encouraged or sponsored economic espionage against American defense contractors. *See infra*, Part II.B.

[38] *See infra,* Part I.B.

B. Congress Responds to the Problem of Economic Espionage

Prior to the passage of the EEA, federal prosecutors relied on three statutes to prosecute the theft of trade secrets: 18 U.S.C. § 1341 (mail fraud); 18 U.S.C. § 1343 (wire fraud); and 18 U.S.C. § 2314 (National Stolen Property Act).[39] According to one Assistant U.S. Attorney working on computer crime, "[f]ederal prosecutors often had difficulty fitting trade secret cases within the existing statutes."[40] According to Thierry Desmet, this was "because corporate spying does not involve the use of the mail or wire."[41] This is overstated, because, although not the case in many of the § 1831 cases[42], corporate spying might well involve the use of the mail or telecommunications However, technological advances often outpaced the federal government's resources to counter new forms of crime.

Dowling v United States is instructive.[43] In *Dowling*, prosecutors had used the National Stolen Property Act to prosecute the distributor of bootlegged Elvis Presley records. The National Stolen Property Act, for instance, criminalizes the interstate shipment of stolen "goods, wares, merchandise, securities or money, of the value of $5,000 or more."[44] However, the statute's definition of stolen property did not appear to reach intangible, intellectual property.[45]

---

[39] *Id.* at n.258; *see also*, Thierry Olivier Desmet, *The Economic Espionage Act of 1996: Are We Finally Taking Corporate Spies Seriously?*, 22 HOUS. J. INT'L L. 93, 103-04 (1999).
[40] George "Toby" Dilworth, *The Economic Espionage Act of 1996: An Overview*, U.S. ATT'YS BULL., http://www.usdoj.gov/criminal/cybercrime/usamay2001_6htm, (accessed Sept. 19, 2008); *see also*, James M. Fischer, *An Analysis of the Economic Espionage Act of 1996*, 25 SETON HALL LEGIS. J. 239, 248-49 (2001).
[41] Desmet, *supra* note 40, at 104; *see also*, Fischer, *supra* note 41, at 250, n.62 (noting that, in his testimony to the House Subcommittee on Crime of the Committee of the Judiciary in 1996, FBI Director Freeh asserted that the non-tangible nature of proprietary information caused some prosecutors to decline prosecuting economic espionage cases).
[42] *See infra*, Part II.B.
[43] *Dowling v. United States*, 473 U.S. 207 (1985).
[44] 18 U.S.C. § 2314 reads, in pertinent part, "[w]hoever transports, transmits, or transfers in interstate or foreign commerce *any goods, wares, merchandise, securities or money*, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud . . ." (emphasis added).
[45] Desmet, *supra* note 39, at 104 n.27 ("The NSPA was designed, however, to prevent traditional property crimes and it does not function adequately to intangible property.").

The Supreme Court held that "interference with copyright does not easily equate with theft, conversion, or fraud."[46] The Court suggested that the aforementioned terms are associated with "physical removal" rather than with copyright infringement. "There is no dispute in this case that Dowling's unauthorized inclusion in his bootleg albums or performances of copyrighted compositions constituted infringement of those copyrights. It is less clear, however, that the taking that occurs when an infringer abrogates the use of another's protected work comfortably fits the terms associated with physical removal . . ."[47] Thus, in resolving a circuit split as to whether the National Stolen Property Act applied to interstate shipment of bootlegged musical recordings, the Court held that, under the rule of lenity, the statute did not apply to Dowling's conduct.[48]

Prosecutors also met a major stumbling block in the prosecution of trade secret theft in *United States v. Brown*.[49] In *Brown*, the Tenth Circuit held that the National Stolen Property Act did not apply to a defendant who had stolen "a computer program in source code form."[50] In 1994, Peter Toren, a trial attorney with the Computer Crime Unit of the Department of Justice's Criminal Division, observed with some degree of concern that "after the Brown decision, there are certain situations that a United States Attorney's Office might very well decline to prosecute under 18 U.S.C. § 2314, even if someone misappropriates an extremely valuable trade secret."[51] Toren recommended that Congress amend the National Stolen Property Act "to specifically

[46] *Dowling*, 473 U.S. at 217.
[47] *Id.*
[48] *Id.* at 213, 228.
[49] *United States v. Brown*, 925 F.2d 1301 (10th Cir. 1991).
[50] *Id.* at 1302 ("The United States appeals from a dismissal by the district court of an indictment charging the defendant . . . with three counts of violations of the National Stolen Property Act . . . . The indictment was dismissed on the ground that the allegedly stolen property, a computer program in source code form, did not come within the ambit of 18 U.S.C. §§ 2314 and 2315 as goods, wares or merchandise. We affirm.")
[51] Toren, *supra* note 39, at 96.

include the interstate transportation of stolen intangible property."[52] He further cited the possible need for Congress to enact "new comprehensive legislation that criminalizes the theft of trade secrets."[53]

Toren would see his recommendations acted on in October 1996, when the Economic Espionage Act became effective.[54] No longer would prosecutors be faced by the limitations of the National Stolen Property Act. As the first federal statute to criminalize trade secret theft, the EEA would become a useful tool for federal prosecutors in the decade ahead. The statutory text of the EEA has nine provisions, two of which define the criminalizing of conduct resulting in the theft of trade secrets.[55] First, § 1831 criminalizes the theft of trade secrets by foreign governments or foreign-sponsored entities. Second, § 1832 criminalizes the "theft of trade secrets carried out for economic or commercial advantage, whether the perpetrator is foreign or domestic."[56] Thus, § 1832 applies to cases when an agent of one domestic corporation steals the trade secrets of his own corporation or of a competitor.

In his signing statement of the EEA, President Clinton reiterated the national security implications of the statute: "[t]rade secrets are an integral part of virtually every sector of our economy and are essential to maintaining the health and competitiveness of critical industries operating in the United States. Economic espionage and trade secret theft threaten our Nation's *national security* and economic well-being." (emphasis added).[57] President Clinton's statement

---

[52] *Id.*
[53] *Id.* at 97 (arguing that a specific federal statute criminalizing the theft of trade secrets would "a strong message that the theft of trade secrets from American businesses will not be tolerated").
[54] Tucker, *supra* note 1, at 1138.
[55] The entire statute is found at 18 U.S.C. §§ 1831-1839 (1996).
[56] Dilworth, *supra* note 41; *see also*, Tucker, *supra* note 1, at 1140-48.
[57] PUB. PAPERS 1814-15 (Oct. 11, 1996); s*ee also*, Gerald J. Mossinghoff, J. Derek Mason, & David A. Oblon, *The Economic Espionage Act: A New Federal Regime of Trade Secret Protection*, 79 J. PAT. & TRADEMARK OFF. SOC'Y, 191 (1997) ("The overriding reasons behind the enactment of the legislation were the fully documented efforts of

that trade secret theft threatens American ‘‘national security and economic well-being” should be read as endorsing the notion that the economic well-being of the United States is a fundamental component of American national security. Corporate trade secrets, although privately held, are integral to the financial well being of the American economy, and hence, to that of the American public.

The EEA is thus a hybrid form of legislation. It serves both as a deterrent to corporate competitors engaging in the theft of trade secrets and as a form of national security legislation. It was designed to give federal law enforcement a framework into which prosecutors can fit cases where a foreign government's intelligence service sought to spy on, and steal trade secrets from, an American corporation. Of course, an issue may arise as to what is a "trade secret." It is to this subject that I shall now turn.

C. The Trade Secret Conundrum

Defining a "trade secret" is perhaps not the easiest of tasks. The Restatement (Third) of Unfair Competition § 39 defines a trade secret as "any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others."[58] The Uniform Trade Secrets Act ("UTSA"), adopted by the majority of states, defines a trade secret as:

information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

> (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

---

foreign governments to gain access to the trade secrets of U.S. companies, in order to advance the economic interests of their private sector.").

[58] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[59]

Prior to the passage of the EEA, the UTSA governed some cases in which competitors or others misappropriated trade secrets. However, the UTSA is not a criminal statute; rather, it creates a "cause of action in tort" for the theft of trade secrets.[60] For American Corporation Z to sue in a state court foreign intelligence service X for the theft of a trade secret likely would be unworkable for several reasons.[61] First, it would likely raise a separation of powers issue, as it could be interpreted as a state court's intrusion into foreign policy. Second, it is highly unlikely that a foreign intelligence service, particularly one hostile to the United States, would recognize the jurisdiction of an American state court. Third, any judgment rendered against a foreign intelligence agency in a state court would almost certainly never be honored. Furthermore, the alleged harm done in a cause of action under the UTSA is to the corporation itself rather than to the public.. Because the EEA is a criminal, rather than a civil, statute, the harm is to society as a whole, thus giving the federal government authority to prosecute those who engage in trade secret theft against private American corporations.

The EEA definition of trade secret is similar to that of the UTSA in that the information "derives independent economic value, actual or potential" from the fact that the general public does not have readily ascertainable access to the information. However, the definition of what sorts of information constitute a trade secret is broader in the EEA. Unlike the UTSA, which lists "a formula, compilation, device, method, technique, or process," the EEA lists "*all forms and types* of financial, business, scientific, technical, economic, or engineering information . . . ."

[59] Unif. Trade Secrets Act § 1-4. Connecticut law defines trade secret identically to that of the UTSA. The statutory definition is at C.G.S.A. § 35-51(d) (West 2008).
[60] Fischer, *supra* note 41, at 253.
[61] *But see infra*, Part III.A. (discussing how derivative suits might be used to counter economic espionage).

(emphasis added). One commentator observed that the EEA "actually expands the traditional view of trade secrets to allocate control and use of other information."[62] Information, broadly construed, falls under the purview of the EEA.

Under the EEA, almost any information that the owner takes reasonable steps to keep secret and which has economic value because of its secret nature is a trade secret. Notable in the EEA definition is the specific reference to engineering information. Should the engineering trade secret pertain to the national defense, it would appear that a prosecutor could choose to invoke either the EEA (engineering factor) or 18 U.S.C. § 794(a), the federal statute criminalizing the gathering or delivering of defense information to aid a foreign government. The theft of business proprietary information, by contrast, would most likely be brought under the provisions of the EEA.

The expansive definition of trade secrets in the EEA has not gone unchallenged. In *United States v. Hsu (Hsu IV)*, the defendant, Kai-Lo Hsu, contended that the EEA was unconstitutionally vague.[63] In an indictment under § 1832 of the EEA, Hsu was charged in a FBI sting operation concerning the theft of technology. Hsu argued "that the definition of 'trade secret' in 18 U.S.C. § 1839(3) offends due process with its vagueness because it does not define either 'reasonable measures' to keep the information secret, or what is meant by information not being 'generally known' or 'readily ascertainable' to the public."[64] The court was troubled by the EEA's definition of trade secret. "With the proliferation of the media of communication on technological subjects, and (still) in so many languages, what is 'generally known' or

---

[62] Leslie G. Berkowitz, *Computer Security and Privacy: The Third Wave of Property Law*, 33 COLO. LAWYER 57 (Feb. 2004).
[63] *United States v. Hsu* (*Hsu IV)*, 40 F.Supp.2d 623 (E.D. Pa. 1999).
[64] *Id.* at 626.

'reasonably ascertainable' to the public at any given time is necessarily never sure."[65] However, as applied to the facts of that particular case, the court held that the "term 'generally known to, and not being readily ascertainable through proper means by, the public,' is not unconstitutionally vague."[66] The *Hsu* court did, however, leave open the door to future challenges under the void-for-vagueness doctrine.

In *United States v. Krumrei*, also a § 1832 case, the defendant filed a motion to dismiss, claiming that the definition of trade secret was unconstitutionally vague.[67] In *Krumrei*, the government had indicted the defendant for transmitting a trade secret to the owner of a corporate competitor. The court noted that the defendant knew that the information was proprietary. Citing *Hsu*, the Sixth Circuit held that the definition of trade secret in the EEA was not unconstitutionally vague as applied to the defendant.[68]

Hsu and *Krumrei* were § 1832 cases rather than § 1831 cases, which deal with economic espionage intended to benefit a foreign government.. However, the constitutionality of the EEA definition of trade secret strengthened prosecutors' abilities to apply the EEA toward a more serious economic espionage crime, foreign-government-sponsored economic espionage against American corporations. It is to a particular country's extensive efforts at engaging in economic espionage in the United States to which I shall now turn.

[65] *Id.* at 630.
[66] *Id.*
[67] *United States v. Krumrei*, 258 F.3d 535 (6th Cir. 2001).
[68] *Id.* at 539.

II. China's Economic War Against the United States

The Chinese Military's Long-Term Strategy

China seeks to be the dominant military power in East Asia.[69] In particular, Beijing seeks to build an offensive naval capability in East Asia and seeks technology that can aid the country in improving its naval capability.[70] Such naval capability would be employed in any potential military confrontation over Taiwan.[71] Furthermore, according to two analysts, "Chinese leaders believe their rule depends on secure sea lanes."[72] To aid them in this quest, the Chinese government and its agents have engaged in economic espionage against American institutions that have critical warship technology.[73]The Chinese People's Liberation Army also "is in the midst of a major transformation in order to prepare for what the top leaders call the new era of information warfare."[74] China seeks to upgrade its military and industrial base. Ira Winkler contends that "[i]ndustrial espionage has always played an important role in Chinese economic development. For many years, China has used its military intelligence capabilities for economic purposes."[75]

---

[69] John J. Tkacik, Jr., Testimony at Committee on Armed Services, U.S. House of Representatives (July 27, 2005), *available at* http://www.heritage.org/research/asiaandthepacific/tst072705.cfm.
[70] Neil A. Lewis, *U.S. Analyst's Case Hints at Breadth of Chinese Espionage*, INT'L HERALD TRIBUNE, July 10, 2008, *available at* http://www.iht.com/bin/printfriendly.php?id=14402344; James Holmes & Toshi Yoshihara, *The Best Defense is a Good Offense for China's Navy*, NAT' INT. (June 2005), *available at* http://inthenationalinterest.com/Articles/June%202005/June2005HolmesPFV.html; *see also*, Thomas Harding, *Jitters Over China's Military Muscle*, SYDNEY MORNING HERALD, September 30, 2008, http://www.smh.com.au/news/world/jitters-over-chinas-military-muscle/2008/09/29/1222650990683.html.
[71] Neil A. Lewis, *Spy Cases Raise Concern on China's Intentions*, N.Y. TIMES, July 10, 2008.
[72] Holmes & Yoshihara, *supra* note 72.
[73] Press Release, The U. S. Atty's Office, Central Dist. of Cal., Chinese Agent Sentenced to Over 24 Years in Prison for Exporting U. S. Def. Articles to China (Mar. 24, 2008), *available at* http://www.usdoj.gov/usao/cac/pressroom/pr2008/032.htm.
[74] Cheng Li & Scott W. Harold, *China's New Military Elite*, CHINA SECURITY VOL.3, NO.4, (2007), *available at* http://www.brookings.edu/articles/2007/fall_china_li.aspx?rssid=china.
[75] WINKLER, *supra* note 5, at 86.

The Chinese government relies heavily upon Chinese scientists and students in the United States, as well as upon the Chinese-American Diaspora, to spy on American corporations.[76] Unlike the efforts of other countries, the Chinese espionage effort is decentralized. Chinese students at American universities may be particularly susceptible to approaches from China's intelligence services.[77]

B. Chinese Economic Espionage in the United States

Economic espionage is one of the primary ways by which the Chinese government seeks to boost its long-term military capability. Due to the seriousness of § 1831 cases, the Attorney General must authorize local prosecutions.[78] Three years after the passage of the EEA, two commentators noted that President Clinton's accolades for the statute vastly overstated the statute's significance and noted that, no prosecutions had been brought under § 1831.[79] However, at the turn of the century, federal prosecutions brought numerous indictments under § 1831. The majority of § 1831 cases have involved Chinese-government-sponsored economic espionage.[80] It is these cases, and the interconnections between them, that I shall now discuss.

---

[76] *See* NICHOLAS EFTIMIADES, CHINESE INTELLIGENCE OPERATIONS 28 (1994). China is not the only country to rely upon ethnic kin in the United States for espionage purposes. *See also*, WINKLER, *supra* note 5, at 94 ("Similarly to the Chinese, the Israelis also utilize ethnic targeting to recruit many of their agents").

[77] WINKLER, *supra* note 5, at 86. None of this, of course, is meant to imply that Chinese-Americans or Chinese students in the United States should be targets of ethnic profiling.

[78] Memorandum from the Office of the Att'y Gen. on Renewal of Approval Requirement Under the Economic Espionage Act of 1996 to all United States Attorneys, all First Assistant United States Attorneys, all Criminal Chiefs, all Criminal Division Section Chiefs and Office Directors (Mar. 1, 2002) (on file with author).

[79] John R. Bauer & Joseph F. Savage, *Criminalization of Trade Secret Theft: On the Second Anniversary of the Economic Espionage Act*, 8 INT'L TRADE L.J. 59, 59 (1999).

[80] Press Release, Dep't of Justice, Chinese Nat'l Sentenced for Econ. Espionage (June 18, 2008), *available at* http://www.usdoj.gov/opa/pr/2008/June/08-nsd-545.htm (last accessed Sept. 14, 2008); the first Section 1831 indictment, however, was against two individuals who conspired to aid an instrumentality of the government of Japan. *See* Press Release, U.S. Dep. of Justice, U.S. Att'y, N. Dist. of Ohio, First Foreign Econ. Espionage Indictment; Defendants Steal Trade Secrets from Cleveland Clinic Found. (May 8, 2001), *available at* http://www.usdoj.gov/criminal/cybercrime/Okamoto_SerizawaIndict.htm; *see also*, John Mangels, *Clinic Case is First Use of New Law: Statute Aims at Economic Espionage that Benefits a Foreign Government*, CLEVELAND PLAIN DEALER, July 30, 2001, 2001 WL 250929.

United States v. Fei Ye and Ming Zhong

Given its centrality to the computer and technology industry, Silicon Valley is a focal point for economic espionage.[81] On November 23, 2001, federal agents arrested Fei Ye and Ming Zhong at the San Francisco International Airport as they attempted to board a flight to the PRC with stolen trade secrets in their possession.[82] Although both men were originally from China, Fei Ye was also an American citizen; Ming Zhong was a permanent resident of the United States.[83] On December 4, 2002, the two men were indicted by a federal grand jury on ten counts, including conspiracy, economic espionage, possession of stolen trade secrets, and foreign transportation of stolen property.[84] With regard to the EEA charges, Fei Ye and Ming Zhong were indicted under both § 1831 and 1832.

Fei Ye and Ming Zhong had engaged in a scheme to steal trade secrets belonging to Sun Microsystems, Inc. and Transmeta Corporation, as well as two other companies, to develop and to sell new microprocessors in China.[85] The government's appellate brief to the Ninth Circuit indicates that the defendants possessed the trade secrets to benefit China by promoting the development of the Chinese integrated circuit industry through an entity known as 'Supervision.'[86] According to the indictment, Ye and Zhong had told others that funding for

[81] Press Release, U.S. Dep't of Justice, N. Dist. of Cal., Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Cos. to Benefit China, (Dec. 14, 2006), *available at* http://www.usdoj.gov/criminal/cybercrime/yePlea.htm.
[82] *See* Brief of Appellant for United States at *5, *United States v. Fei Ye*, 436 F.3d 1117, 1119 (9th. Cir. July 5, 2006) (Docket No. CR-02-20145 JW, 2005 WL 5909164).
[83] Press Release, U. S. Att'y, N. Dist. of Cal., Pair from Cupertino and San Jose, Cal., Indicted for Econ. Espionage and Theft of Trade Secrets from Silicon Valley Cos. (Dec. 4, 2002), *available at* http://www.usdoj.gov/criminal/cybercrime/yeIndict.htm.
[84] *Id.*
[85] *See id.* According to the government, federal agents seized trade secrets from Transmeta in both Ye's and Zhong's luggage and seized trade secrets from Sun in Ye's luggage only. Federal agents seized other trade secrets from Sun, Transmeta, NEC Electronics Corporation, and Trident Microsystems, Inc., in other locations. For the purposes of the Section 1831(a)(3), charges, however, all the seized evidence was from the luggage at the airport. For the Section 1831(a)(5) charge, the location seized included luggage, residences, and Zhong's office.
[86] Brief of Appellant for United States at *7, *Fei Ye*, 436 F.3d 1117 (NO. CR-02-20145 JW), 2005 WL 5909164.

Supervision was being provided by the government of Hangzhou, China; that Supervision was applying for funding from the 863 Program; and that Supervision was working with a Chinese university professor, who was helping them to obtain 863 Program funding.[87] Run by the PRC central government and linked to its military, the 863 Program invests in corporations with new technologies.[88] The FBI suspects, with good reason, that the 863 Program is involved in many economic espionage cases.[89] Testifying before the Senate Judiciary Committee, U.S. Attorney Kevin J. O'Connor referenced the 863 Program as a "funding plan created and operated by the government of the People's Republic of China, also known as the national High Technology Research Development Program."[90] The 863 Program will likewise play a role in the *Le* case. In that case, the government referenced the fact that the General Armaments Division of the People's Liberation Army "had a regular role in, and was a major user, of the 863 Program."[91] According to Larry M. Wortzel, a former military intelligence officer, the 863 Program "is part of the climate in China that rewards stealing secrets" and the program "is related to state-directed and economic espionage, but it is only one of the actors."[92]

In December 2006, Ye and Zhong pled guilty to the charge of economic espionage to benefit a foreign government, the first convictions under § 1831. Significantly, this case, like many federal criminal cases, did not go to trial. However, the question remained as to how

[87] Press Release, N. Dist. of Cal., (Dec. 4, 2002), *supra* note 86.
[88] K. Oanh Ha, *supra* note 22.
[89] *Id.*
[90] *U.S. Government Enforcement of Intellectual Property Rights: Hearing Before the S. Comm. on the Judiciary*, S. Hrg. 110-782 (2007) (statement of Kevin J. O'Connor, United States Attorney for the District of Connecticut, Chairman of the Department of J. Task Force on Intellectual Property).
[91] Press Release, U.S. Dep't of Justice, Two Bay Men Indicted on Charges of Econ. Espionage, (Sept. 26, 2007), *available at* http://www.usdoj.gov/criminal/cybercrime/liIndict.htm.
[92] Ariana Eunjung Cha, *Even Spies Embrace China's Free Market*, WASH. POST, Feb. 18, 2008, at D1.

extensive the Chinese government's involvement in the *Ye* case really was.[93] The EEA does not require that prosecutors prove that a foreign government or entity needed to be involved, directly or indirectly, in the theft of trade secrets. Rather, what is required is for a person or organization to act in such a way that will benefit a foreign government or entity. Congress likely settled upon this language for two practical reasons. First, it would be much more difficult for a prosecutor to prove, beyond a reasonable doubt, that a foreign intelligence service aided or encouraged the acts by a hypothetical principal in an economic espionage case. Second, because of the sensitive nature of counterintelligence operations, the government would be unlikely to want to advertise directly that a foreign government, especially an ally like France or Israel, was caught engaging in economic espionage against American corporations.[94]

In the *Ye* case, however, because of the Chinese connection, prosecutors likely felt that the guilty pleas of both men would serve to deter potential further Chinese-sponsored economic espionage activities. At the very least, the first § 1831 conviction involving a Chinese connection would serve as a validation of the Congressional intent to enact the EEA. The *Ye* case would, however, be only the first in a string of cases all involving a Chinese connection and all occurring in California.

United States v. Xiodong Sheldon Meng

In December 2006, in a 36-count criminal indictment, the government indicted a Chinese-Canadian, Xiodang Sheldon Meng, under § 1831 of the EEA and under the Arms

[93] Jordan Robertson, *A Victory Against Economic Espionage*, HOUSTON CHRON., Dec. 16, 2006, 2006 WL 21887869 ("[T]he settlement leaves unanswered one of the key underlying questions of the case: Did the Chinese government or any of its officials know the trade secrets were stolen?").
[94] *See* WINKLER, *supra* note 5, at 104 ("Although relatively few Israeli espionage cases hit the media, it is extremely likely that Israel is every bit as active in this arena as are the French and the Chinese.").

Control Export Act, as well as other ancillary charges.[95] From June 19, 2000, to March 7, 2003, Meng, of Cupertino, California, was employed at a San Jose, California company, Quantum3D, Inc.[96] He later pled guilty to misappropriating trade secrets, including a product known as nVSensor, a corporate night-vision technology product used exclusively in military applications for training and simulation applications.[97] The government alleged that Meng intended his actions to benefit the PRC Navy Research Center in Beijing.[98] The defense, in court documents, maintained that Meng did not engage in espionage on behalf of a foreign government.[99]

According to Joseph P. Russoniello, the U.S. Attorney for the Northern District of California, "[i]n this case, a Silicon Valley trade secret was used in a demonstration project in Beijing with the intent to Benefit the PRC Naval Research Center."[100] The investigation also indicated that Meng used the military application trade secrets in a demonstration and in a sales proposal to the Malaysian Air Force and the Thai Air Force.[101] However, according to Assistant U.S. Attorney Mark Krotoski, who prosecuted the case, "it was Meng's focus on profits, not a foreign allegiance, that drove him to steal the trade secrets and to try to sell them to the highest

---

[95] Tom Abate & John Coté, *Silicon Valley Espionage Case: Feds Accuse Man of Trying to Sell Software to Asian Military Buyers*, S.F. CHRON., Dec. 15, 2006, at A1, WL 21800509. The Arms Control Export Act is at 22 U.S.C. § 2778 (2004).

[96] Press Release, U.S. Dep't of Justice, U. S. Att'y, N. Dist. of Cal., Former Chinese Nat'l Charged with Stealing Military Application Trade Secrets from Silicon Valley Firm to Benefit Gov'ts of Thail., Malay., and China (Dec. 14, 2006), *available at* http://www.usdoj.gov/criminal/cybercrime/mengCharge.htm.

[97] Press Release, Dep't of Justice, Chinese Nat'l Sentenced for Econ. Espionage, *supra* note 80; *Cupertino Resident Pleads Guilty to Espionage Charges*, SILICON VALLEY – SAN JOSE BUS. J. (Aug. 2, 2007), WL 14842694.

[98] *See* Press Release, U.S. Dep't of Justice, Chinese Nat' Sentenced for Economic Espionage, *supra* note 80 (". . . With the Intent To Benefit China Navy Research Center").

[99] John Coté, *Salesman Sentenced to 2 Years in Prison as Industrial Spy, Thief*, S.F. CHRON., June 18, 2008, at B3, . WL 11527279.

[100] Press Release, U.S. Dep't of Justice, Chinese National Sentenced for Economic Espionage, (June 18, 2008), *available at* http://www.usdoj.gov/opa/pr/2008/June/08-nsd-545.html.

[101] Press Release, U.S. Department of Justice, United States Attorney, Northern District of California, Former Chinese National Charged with Stealing Military Application Trade Secrets from Silicon Valley Firm to Benefit Governments of Thailand, Malaysia, and China (Dec. 14, 2006), *available at* http://www.usdoj.gov/criminal/cybercrime/mengCharge.htm.

bidder."[102] The Justice Department, however, emphasized the national security dimension to the *Meng* case with a specific press release from the National Security Division.[103]

As in the *Ye* case, the question remains as to how extensive was the Chinese government's role. Was the *Meng* case primarily a theft-of-trade-secrets case, a counterintelligence case, or both? If it was primarily a theft-of-trade-secrets case, then § 1831 of the EEA proved to be an adequate statutory provision. However, despite the relative seriousness of the offense, Meng was sentenced to only two years in prison, a comparatively light sentence given that § 1831 allows for up to 15 years imprisonment.[104]

Categorizing *Meng* as primarily a counterintelligence case utilizing the EEA makes more sense because of the connection to the PRC Naval Research Center. Had this case occurred during the Cold War and involved the Soviet Navy, prosecutors would have brought this case under the Espionage Act.[105] Indeed the case, at least theoretically, meets the statutory provision of 18 U.S.C. § 794(a), which makes it a crime to communicate to the "naval force within a foreign country . . . any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense . . ."[106] The statutory language noticeably does not refer to trade secrets; however, it does refer to "information relating to the national defense.' This phrase is probably broad enough to encompass the night-vision technology trade secret. However, the statutory language of the EEA has the advantage of being more precise. The best explanation of why the government chose to prosecute Meng under the EEA rather than under the Espionage

[102] *Engineer Who Tried to Sell Secrets to China Gets 24 Months*, CHICAGO TRIBUNE, June 19, 2008, WL 11538443.
[103] *See* http://www.usdoj.gov/opa/pr/2008/June/08-nsd-545.html.
[104] *See* Coté, *supra* note 99. .
[105] *See supra*, notes 2-3 and accompanying text.
[106] 18 U.S.C. § 794(a).

Act is that the government likely did not want to disclose any information obtained during the investigation of Chinese intelligence operations. Such information might have had to be revealed in court had the prosecutors chosen to bring the case under the Espionage Act and had Meng chosen to go to trial. Nevertheless, with a plea agreement in a § 1831 case, the government was able to send a strong message that Chinese-sponsored theft of trade secrets in Silicon Valley would be discovered and prosecuted. As the following case will show, the interconnections between the Silicon Valley cases should not be underestimated.

United States v. Lan Lee and Yuefei Ge

On September 26, 2007, the Department of Justice announced the indictment of Lan Lee ("Lan Li"), an American citizen, of Palo Alto, California, and Yufei Ge, a Chinese national, of San Jose, on charges of economic espionage.[107] The U.S. Attorney's Office brought the charges under both § 1831 and § 1832.[108] The superseding indictment alleged that Lee and Ge conspired to steal trade secrets from their employer, NetLogics Microsystem, and from Taiwan Semiconductor Manufacturing Corporation. The indictment also alleged that the men created a company, SICO Microsystems, Inc., registered in Delaware, "for the purpose of developing and marketing products derived from and using the stolen trade secrets."[109] The men allegedly stole blueprints that they intended to use to reproduce a super-fast microchip in China.[110]

Similar to the *Ye* case, the 863 Program played a role in the *Lee* case as well.[111] In 2003, SICO signed a deal with a Chinese company run by venture capitalist Liu Baisen, who allegedly

[107] Press Release, U.S. Dep't of Justice, Two Bay Area Men Indicted on Charges of Econ. Espionage, (Sept. 26, 2007), *available at* http://www.usdoj.gov/criminal/cybercrime/liIdict.htm.
[108] *Id.*
[109] *Id.*
[110] Cha, *supra* note 92.
[111] *See supra*, notes 90-95 and accompanying text.

agreed to secure funding from the 863 Program and the General Armaments Department.[112] In the Department of Justice press release, the government explicitly referenced both the Chinese government and the 863 Program. "The defendants sought to obtain venture capital funding for their company from the government of China, in particular the 863 Program and the General Armaments Department."[113] The government also specifically singled out the 863 Program's ties with the Chinese military-industrial complex: "[t]he program was designed by leading PRC scientists to develop and encourage the creation of technology in the PRC and focused on issues such as high technology communications and laser technology, with an emphasis on military applications."[114] According to one press report, Lee and Ge "allegedly reached out to Chinese government agencies for help funding the business, including a branch of the Chinese military responsible for the development of weapons systems, and an agency that funnels money toward technology companies with a military bent."[115] The *Lee* case represents the intersection of trade secret theft and national security. Indeed, *Lee* is exactly the type of case that prompted Congress to enact § 1831. Here, a Chinese national working for a California employer allegedly stole trade secrets intended to benefit the PRC. Making the case even more threatening to national security was the linkage to the 863 Program.

The *Lee* case should not be seen in a vacuum, but rather in the context of a systematic effort by individuals in California to steal trade secrets that would benefit China. Levine has postulated that the Department of Justice has, in economic espionage cases, "an apparent strategy of trading sentencing leniency for one pair of defendants in order to help convict another pair on

[112] Cha, *Even Spies Embrace*, *infra* note 126.
[113] Press Release, U.S. Dep't of Justice, Two Bay Area Men Indicted on Charges of Economic Espionage, *supra* note 107.
[114] *Id.*
[115] *Two Engineers Indicted in Economic Espionage*, L.A. TIMES, Sept. 27, 2007, 2007 WL 18923968.

higher-profile charges . . ."[116] Here, Levine specifically references the apparent ties between the *Ye and Lee* cases. He hints that in Ye and Zhong's plea agreement with the government, the two men provided information to the U.S. Attorney's Office that was then utilized to indict Lee and Ge for economic espionage. "Ye and Zhong's plea deal doesn't specify who they gave up, but they admitted to applying for funding from the same Chinese venture group that Lee and Ge had allegedly solicited."[117] Although there is no mention of venture capitalist Liu in the publicly-available *Ye* documents, such a linkage would suggest that Liu may have been a conduit between the defendants and the 863 Program. According to the *Washington Post*, "[o]ne of the four addresses listed in Liu's former company's official registration papers is a room in the basement of a heavily guarded, unmarked government security complex in Beijing's Zhongguancun neighborhood, which is known as China's Silicon Valley."[118] As of now, the *Lee* case raises more questions about the interconnections between the different California economic espionage cases than answers.

United States v. Dongfan "Greg" Chung

Although the Department of Justice did not arrest Greg Chung until February 2008, in many respects the *Chung* case began in 1985 when Chi Mak and his wife became naturalized citizens in Los Angeles.[119] Described by federal prosecutors as the "perfect sleeper agent," Chinese-born Chi Mak arrived in the United States in the 1970s and built a career working for a defense contractor, Power Paragon, in an effort to develop a submarine propulsion system.[120] His

[116] Dan Levine, *DOJ's Economic-Spy Strategy Emerges*, May 5, 2008, http://www.law.com/jsp/article.jsp?id=1202421126406.
[117] *Id.*
[118] Cha, *supra* note 92.
[119] Peter Grier, *Spy Case Patterns the Chinese Style of Espionage*, CHRISTIAN SCIENCE MONITOR, Nov. 30, 2005.
[120] Joby Warrick & Carrie Johnson, *Chinese Spy 'Slept' in U.S. for 2 Decades*, WASH. POST, Apr. 3, 2008, at A1.

job and security clearance gave him access to Navy ship, submarine, and weapons technology.[121] In 2003, federal authorities began investigating Mak. The FBI discovered that Mak had copied thousands of technical documents onto computer disks which he then arranged to be sent to China.[122]

Mak admitted that he had been placed in the United States to steal defense-industrial secrets. Mak was allegedly handled by "PRC official A," a senior Chinese intelligence official who was the mastermind in *United States v. Bergersen*. In *Bergersen*, a Department of Defense weapons system analyst pled guilty in U.S. District Court in Alexandria, Virginia, to conspiracy to disclose national defense information to persons not entitled to receive it, in violation of 18 U.S.C. §§ 793(d) and (g).[123] Notably, the Justice Department announced the charges against Bergersen on the very same day as they announced charges against Chung.[124]

On October 28, 2005, federal agents arrested Chi Mak, his wife, and his brother.[125] A federal jury convicted Mak of both illegally exporting American defense technology and being an unregistered foreign agent.[126] Mak was eventually sentenced to 293 months in federal prison for exporting technical information about Navy warship technologies and sensitive American military technology to the PRC.[127]

---

[121] *Id.*
[122] *Id.*
[123] Lewis, *supra* note 71; Press Release, U.S. Dep't of Justice, Defense Dep't Official Pleads Guilty to Espionage Charge Involving China, (Mar. 31, 2008), *available at* http://www.usdoj.gov/opa/pr/2008/March/08_nsd_252.html.
[124] Jerry Markon, *Defense Official is Charged in Chinese Espionage Case*, WASH. POST, Feb. 12, 2008, at A1.
[125] Warrick & Johnson, *supra*.
[126] *Jury Convicts Chinese-Born Engineer of Passing U.S. Military Secrets to China*, Associated Press, May 10, 2007, *available at* http://www.foxnews.com/printer_friendly_story/0,3566,271325,00.html.
[127] Press Release, U. S. Att'ys Office, Central Dist. of Cal., *supra* note 73.

The *Mak* case is linked with the *Chung* case.[128] As previously described, on February 11, 2008, federal agents arrested Dongfan "Greg" Chung of Orange, California, on economic espionage charges.[129] Unlike some of the previous cases where prosecutors brought charges under both §§ 1831 and 1832, here, the economic espionage charges in the indictment were solely under §§ 1831(a)(1) and 1831(3).[130] The October 2007 Grand Jury indictment alleges that Chung conspired to steal possess Boeing trade secrets intended to benefit the PRC or its agents.[131] Chung allegedly took Boeing trade secrets relating to the Space Shuttle, a military transport aircraft, and the Delta IV rocket.[132] The indictment is explicit in asserting a direct connection between Chung and the Chinese government. "Defendant received requests from officials of the PRC to provide American technology to the PRC."[133]

The indictment alleges that Gu Weihao of the PRC's Ministry of Aviation wrote Chung a letter dated May 2, 1987, asking Chung for "assistance on technical issues" for various aviation programs.[134] The letter also suggested cover stories for Chung's travel to China.[135] More interesting, however, is a letter from Gu Weihao dated April 12, 1988, in which Weihao "stated that Chi Mak's wife, Rebecca, was in China and had told Gu that the Maks and Chungs had a good relationship."[136] Gu Weihao also wrote "that it was faster and safer to send information through Chi Mak."[137] Although the indictment does not provide further detail on the relationship

[128] Press Release, U. S. Att'ys Office, Central Dist. of Cal., Former Boeing Eng'r Charged with Econ. Espionage in Theft of Space Shuttle Secrets, (Feb. 11, 2008), http://www.usdoj.gov/usao/cac/pressroom/pr2008/011.html.
[129] *Id.*
[130] *United States v. Chung*, Indictment, February Feb. 6, 2008, at 1. (copy on file with author).
[131] *Id.* at 7.
[132] Press Release, U.S. Att'ys Office, Central Dist. of Cal., Former Boeing Eng'r Charged with Econ. Espionage in Theft of Space Shuttle Secrets, *supra* note 128.
[133] *United States v. Chung* at 8.
[134] *Id.* at 15.
[135] *Id.*
[136] *Id.*
[137] *Id.* at 16.

between the Maks and the Chungs, one can infer that Chi Mak and Greg Chung had an ongoing relationship relating to their mutual espionage activities.

The *Chung* case is best viewed as a turning point in the government's approach to prosecuting economic espionage cases in which there was a Chinese connection. In contrast to the *Ye*, *Meng*, and *Lee* cases, where the references to an official Chinese governmental role were not nearly as explicit, in *Chung*, the Government likely felt confident enough not only to publicize an official Chinese governmental role in a § 1831 case, but also to provide clues as to the linkages between *Chung* and both *Mak* and *Bergersen*. The case also demonstrates how bold the Chinese government has been in planting agents in the United States and in stealing American trade secrets that could benefit its military-industrial complex.

Given the escalating threat to American national security of economic espionage, it is worth considering whether federal criminal law is an appropriate mechanism for countering the Chinese military's long-term strategy. Congress should consider modifying the EEA to counter what appears to be a rising, concentrated effort by the PRC to pilfer American military technology. It is to that subject that I shall now turn.

III. The EEA and the Problem of Chinese Espionage

Although the EEA has only been in existence for over a decade, it is not too soon to attempt a critical assessment of § 1831 and its role in combating Chinese-government-sponsored economic espionage in the United States. The § 1831 cases where there was a connection to the Chinese government provide a good basis upon which to begin such an assessment. Because many of the documents in the cases remain sealed, providing a comprehensive picture of the role

of U.S. Attorney's offices in investigating and prosecuting economic espionage crimes remains difficult. Furthermore, in some ways the cases provide more questions than answers. However, in light of the information that is publicly available, I offer three primary assessments of the role of the EEA in combating Chinese economic espionage.

First, the EEA alone cannot solve the problem. While the EEA has proved to be both a necessary and useful tool to prosecute actors who engage in economic espionage on behalf of the Chinese government or with the intent to benefit the PRC, federal criminal law is limited in what it can do to solve the overarching problem of U.S.-Chinese economic and military competition.[138] Here, the problem is not the "overexpansion of federal criminal law,"[139] but whether economic espionage is also a diplomatic problem. Furthermore, it must be noted that there is also a role for private lawsuits in countering Chinese economic espionage.

Second, Congress properly defined economic espionage as the theft of trade secrets and properly defined trade secrets broadly. This has allowed for federal prosecutors to apply the statute in myriad cases where the mail and wire fraud statutes did not apply. Furthermore, the broad, inclusive definition of trade secrets in the EEA makes certain that those who engage in economic espionage to benefit the Chinese government cannot mount a successful defense by contending that the materials they were charged with misappropriating were not trade secrets.

Third, in light of the overarching national security threat posed by trade secret theft, Congress should enhance the penalties for those § 1831 crimes where the defendant's acts are

---

[139] John S. Baker, Jr., *Jurisdictional and Separation of Powers Strategies to Limit the Expansion of Federal Crimes*, 54 AM. U. L. REV. 545, 547 (2005). Although even Baker, a critic of the expansion of federal criminal law, seems to note that the EEA is not necessarily such an example of overexpansion of federal criminal law, as the EEA protects "special economic interests."

intended to benefit a foreign government's military or military-industrial complex. Although this enhancement likely would not serve as a deterrent to ideologically committed agents of a foreign power, it would signal the fact that Congress is taking the threat seriously. This would give prosecutors greater leeway to make deals with defendants to obtain useful information regarding ongoing espionage in the United States.

A. The EEA Alone Cannot Solve the Problem of Chinese Economic Espionage

When Congress passed the EEA in 1996, it was not clear whether any legislators had China specifically in mind. In the Senate hearings prior to the enactment of the EEA, perhaps with diplomatic protocol in mind, no senator specifically referenced China. However, China's rise as an economic competitor and its history of espionage activities were known in the intelligence community. It is just as likely that legislators were as concerned with economic espionage conducted by friendly countries such as France and Israel. However, in light of the fact that the overwhelming number of § 1831 criminal prosecutions have had a Chinese connection, the best assessment of the efficacy of § 1831 of the EEA must be determined with reference to those cases that prosecutors chose to bring in court. It should be noted, however, that just because prosecutors have chosen to bring charges against Chinese persons it does not mean that federal law enforcement has not discovered numerous cases of the French and Israelis engaging in similar conduct. Because of the negative diplomatic and political repercussions of bringing legal charges against agents of friendly powers, it is possible that acts of the French and Israelis have been dealt with quietly, outside the formalities of the American legal system.

Although prosecutors have been successful in combating PRC-sponsored economic espionage in the United States, the problem of Chinese economic espionage is not purely one for

federal law enforcement. Unlike domestic trade secret theft where federal law enforcement should have exclusive jurisdiction, trade secret theft where Chinese agents steal American defense technology has implications for U.S.-Chinese economic, military, and political relations. Indeed, the problem of Chinese-sponsored economic espionage cannot be so easily separated from the numerous areas of tension between the United States and China, ranging from disputes over currency[140], China's rising influence in Africa[141], and climate change.[142]

Diplomacy must play a preeminent role in any effort to deal with the problem of Chinese economic espionage in a comprehensive manner. The U.S. Ambassador to China, for instance, may express concerns about Chinese economic espionage to the Chinese Foreign Ministry. Such conversations would demonstrate that the United States considers economic espionage as much of a diplomatic problem as a legal one. Indeed, the United States could link the problem of economic espionage to wider concerns about China's long-term military intentions and quietly create a deal in which China would agree to end its economic espionage in return for American concessions in some area that Beijing considers vital to China's national interests. Furthermore, diplomats would have the luxury of creating a grand bargain outside the formalities of the American legal system. Such an approach would be proactive, rather than the reactive approach of the EEA.

Corporations themselves should be required to ensure that their trade secrets, particularly those that have national security value, are not stolen. One commentator has cited the threat of a

---

[140] Joe McDonald, *US, China headed for possible currency clash*, ASSOCIATED PRESS, Dec. 3, 2008.
[141] Craig Simons, *China's Influence Among African Nations Spurs Concerns*, ATLANTA J.-CONST., Nov. 30, 2008 (noting that China is the biggest purchaser of oil from Sudan).
[142] *China to Work With Obama's National Security Team*, ASSOCIATED PRESS, Dec. 2, 2008.

foreign power, such as China, planting information-gathering technology into commercial and industrial products sold in the United States and used by U.S. government agencies.[143] Robert Bracknell, citing the threat of technological espionage specifically from China, organized crime, and terrorists, has argued that the law, borrowing from the American legal concept of products liability, "can impose special duties on companies engaged in information technology commerce aimed at U.S. consumers, including the U.S. government, and can require them to take prudent steps mandated by law to ensure that the products they sell are as 'espionage-safe' as possible."[144] Although Bracknell was concerned about the potential of a foreign government to deliberately place information seeking technology in exports, his notion of having private actors involved in counterespionage merits attention. Indeed, although I have previously cautioned against the practicality of American corporations bringing suit against foreign intelligence agencies in state courts[145], there is, nevertheless, a role for private actors in combating Chinese economic espionage.

Here, the case of *In re Caremark* is instructive. In *Caremark*, the Delaware Court of Chancery noted that corporate boards may have a duty to maintain a nominal internal control and reporting system that would keep track of possibly illegal acts by employees, so as to avoid liability under the duty of care.[146] The court held that "a director's obligation includes a duty to attempt in good faith that a corporate information and reporting system, which the board, concludes is adequate exists" and that a failure to do so could result in liability.[147] The court's

[143] Robert Gray Bracknell, *Trust Not Their Presents, Nor Admit the Horse: Countering the Technologically-Based Espionage Threat*, 12 ROGER WILLIAMS U. L. REV. 832 (2007).
[144] *Id.* at 840.
[145] *See supra* Part I.C.
[146] *In re: Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).
[147] *Id.* at 970.

holding in *Caremark* could equally be applied to public corporations whose employees engage in economic espionage to benefit a foreign power.

In order to ensure that public corporations are safeguarding trade secrets from foreign spies, courts should permit shareholders of public corporations to file derivative suits on behalf of those corporations that had trade secrets stolen by persons intending to benefit a foreign power. The potential of a lawsuit would give incentives to corporate directors and officers to make sure that they did proper background checks of all employees and that they had internal reporting mechanisms to properly identify potential espionage. Furthermore, allowing such derivative suits to go forward would cause shareholders of public corporations to be more aware of the threat of economic espionage and to apply pressure upon corporations to ensure that there are adequate internal safeguards for detecting espionage.

B. Congress Properly Defined Economic Espionage

When it enacted the EEA, Congress had to decide what would constitute "economic espionage"; it chose to define economic espionage in terms of the theft of trade secrets.[148] Congress chose an expansive definition, one that did not go unchallenged under the void-for-vagueness doctrine.[149] That said, federal prosecutors in California have been able to utilize the definitions of "economic espionage" and "trade secrets" to successfully inhibit the misappropriation of trade secrets, many of which had vital national security implications.[150]

Congress could have adopted Canadian intelligence's definition of economic espionage as pertaining to a foreign government's attempt "to gain unauthorized access to economic

[148] *See supra*, Part I.A.
[149] *Supra* notes 65-70 and accompanying text.
[150] *See supra* Part II.B.

intelligence, such as proprietary information or technology, for economic advantage."[151] Here, the Canadian intelligence service's definition defines economic espionage, not without reason, as seeking *economic* advantage. However, as the *Chung* case, where the defendant stole Navy technology, demonstrates, economic advantage narrowly construed may not always be the motivating factor in "economic espionage" cases. Indeed, the economic advantage factor may be ancillary to a foreign power's long-term military strategy.[152] Furthermore, although Canadian intelligence's definition referenced proprietary information, it does not reference "trade secrets."

The definition of economic espionage in the EEA as the theft of trade secrets has made the EEA a successful tool for prosecuting trade secret theft intended to benefit a foreign power. The definition of trade secrets was broad enough to include such disparate technologies as night-vision technology, blueprints, and Navy weapons technology.[153] Prosecutors, however, should be aware that the broad definition of trade secrets in the EEA does mean that a defendant with a savvy defense counsel could advance a constitutional vagueness challenge where the technology in question may not be completely unknown to the public.[154]

The House Committee on the Judiciary report on the terminology of the EEA, for instance, noted that "[t]he term 'trade secret' is defined in the bill to include all types of financial, business, scientific, technical, economic, or engineering information, whether tangible or intangible, and regardless of the means by which the information is stored, compiled, or memorialized."[155] Notably absent from the Committee's definition, however, is the adjective "military." However, as the *Chung* case demonstrates, prosecutors are willing to utilize the EEA

[151] *Supra* note 28.
[152] *Supra* Part II.A.
[153] *Cf. United States v. Hsu (Hsu IV)*, 40 F.Supp.2d 623 (E.D. Pa. 1999).
[154] *See* 18 U.S.C. § 1839-3 (1996).
[155] H.R. REP. NO. 104-788 (1996), 1996 U.S.C.C.A.N. 4021, 4022.

to prosecute persons who engage in the theft of trade secrets with direct military value.[156] In *Chung*, the trade secrets were in the form of technical documents on computer disks, within the definition set forth by the Judiciary Committee report.

C. Congress Should Enhance the Criminal Penalties for Economic Espionage

Congress should enhance the statutory penalties for a specific subset of § 1831 EEA crimes, namely when a defendant steals a trade secret with the intent to benefit a foreign government's military-industrial complex. Currently, the maximum statutory penalty for all completed § 1831 crimes, where a defendant steals a trade secret to benefit a foreign government, is fifteen years of imprisonment and a fine of $500,000.[157] The statute does not distinguish between friendly and hostile foreign governments or between foreign governments, in general, and foreign militaries, more specifically. In light of the national security implications of trade secret theft when the trade secrets in question could confer a benefit on a military adversary, Congress should revise the statutory penalties for completed § 1831 crimes and enact a higher statutory term of imprisonment.

Congress has already distinguished between cases of trade secret theft when a foreign government is implicated and when it is not. In contrast to § 1831 crimes that have a statutory maximum of fifteen years of imprisonment, completed § 1832 crimes, when a foreign entity is not benefited, have a statutory maximum of ten years of imprisonment.[158] The difference in the statutory mandatory maximum sentence reflects "the more serious nature of economic espionage

[156] *See supra*, notes 127-130 and accompanying text.
[157] *See* 18 U.S.C. § 1831(a) (1996).
[158] *See* 18 U.S.C. § 1832(a) (1996).

sponsored by a foreign government."[159] Both § 1831 and § 1832 require criminal forfeiture.[160] The forfeiture of proceeds is mandatory.[161] However, the forfeiture of instrumentalities is discretionary.[162] Under the U.S. Sentencing Guidelines, the base offense level for both completed § 1831 and § 1832 crimes is determined by U.S.S.G. § 2B1.1.[163] Here, because the statutory maximum penalties for §§ 1831 and 1832, respectively, are fifteen and ten years, the base offense level is six years.[164] An enhanced criminal penalty for § 1831 crimes should have an increased offense level. By enhancing the statutory penalty for § 1831 crimes, Congress would be signaling that it takes very seriously the increased threat that economic espionage poses to American national security.

Because the EEA covers the theft of trade secrets, § 1831 crimes are subject to the Mandatory Victims Restitution Act of 1996 ("MVRA").[165] The MVRA applies to convictions relating to crimes such as "an offense against property under this title . . . including any offense committed by fraud or deceit."[166] According to the Department of Justice, the theft of trade secrets meets the § 3663A definition of property. "The misappropriation of trade secrets is essentially the theft of property."[167] While the Justice Department is correct to characterize trade secrets as a form of property, its contention that the misappropriation of trade secrets is akin to the theft of property merits further analysis. However, in § 1831 crimes where the agent of a foreign government steals a trade secret from American Corporation C to benefit the military-

[159] U.S. Dep't of Justice, Computer Crime & Intellectual Prop. Section, 171 PROSECUTING IP CRIMES MANUAL, *available at* http://www.cybercrime.gov/ipmanual/04ipma.html.
[160] *See* 18 U.S.C. § 1834 (1996).
[161] 18 U.S.C. § 1834(a)(1) (1996).
[162] 18 U.S.C. § 1834(a)(2) (1996).
[163] U.S. Dep't of Justice, Computer Crime & Intellectual Prop. Section, 266 PROSECUTING IP CRIMES MANUAL, *available at* http://www.cybercrime.gov/ipmanual/08ipma.html
[164] *Id*.
[165] 18 U.S.C. § 3663A. (2000)
[166] 18 U.S.C. § 3663A(c)(1)(A)(ii); *see also*, PROSECUTING IP CRIMES MANUAL at 172.
[167] PROSECUTING IP CRIMES MANUAL, *supra* note 171, at 172.

industrial complex of the foreign government, what has occurred is not merely the theft of property; a national security crime has also occurred. Because of the potential threat to national security, such crimes should have enhanced criminal penalties as a way of deterring future conduct.

According to the Department of Justice manual, "[t]he defendant's sentence is driven largely by the value of the misappropriated property."[168] In § 1832 cases of corporate trade secret theft, value, narrowly construed, can be determined in terms of the fair market value of the stolen trade secret or in terms of the potential value of the trade secret, such as a vaccine, to the corporation in the future. An independent appraisal could determine the latter value with relative accuracy and would focus primarily on economic indicators. However, as Marc Zwillinger and Christian Genetski have noted in their work on calculating loss under the EEA, "as various courts have recognized, determining the fair market value of the trade secret is not the ultimate goal in the sentencing process. The purpose of the Guidelines is to achieve sentences that accurately reflect the relative culpability of offenders in a consistent, uniform, and proportional manner." [169] In § 1831 cases in which there are direct national security implications for the misappropriated trade secrets, culpability is increased by the increased threat to national security and that value has more than a fair market value monetary component. Value must be determined not only by the fair market value of the trade secret and the resulting loss to the corporation, but also by the *national security value*. The national security value should be determined independent of the monetary value of the trade secret.

[168] PROSECUTING IP CRIMES MANUAL, *supra* note 171, at 266.
[169] Marc J. Zwillinger & Christian S. Genetski, *Calculating Loss Under the Economic Espionage Act of 1996*, 9 GEO. MASON L. REV. 323, 352 (2000).

Quantifying a national security value of a trade secret would prove difficult, in comparison to determining the fair market value of a corporate trade secret such as a vaccine or software. However, given that a defendant's sentence is driven largely by the value of the property, the concept of value in completed § 1831 crimes should be expanded to include not just monetary value as defined by loss to the corporation, but also the increased threat to national security. Here, *Halkins v. Helms* is instructive.[170] In *Helms*, the court, in a Freedom of Information Act case, referred to the "national security value of information."[171] Here, national security value in determining the proper application of a statute. In terms of the EEA, I have argued that Congress should amend the statutory maximum penalty for § 1831 crimes so that it includes a heightened maximum term of imprisonment to recognize, national security value.

IV. A New Frontier of Espionage: Hacking and Cyberwarfare

Hacking as the New Warfare

China's economic warfare against the United States and its allies is no longer limited to the theft of trade secrets. Computer hacking is the newest form of warfare employed by the Chinese government.[172] In the 1980s, "hacking" was done by small groups of technologically sophisticated individuals as a means of learning more about computers.[173] In the following decade, computers, email, and the Internet had become synonymous with modern business. Indeed, a March 2008 Pentagon report concluded that China's development of ways to infiltrate and to manipulate worldwide computer networks was "a new and potentially dangerous military

[170] *Halkins v. Helms*, 690 F.2d 977 (D.C. Cir. 1982).
[171] *Id.* at 996.
[172] *See*, *e.g.*, Rhys Blakely, Jonathan Richards, James Rossiter, & Richard Beeston, *MI5 Alert on China's Cyberspace Spy Threat*, TIMES (London), Dec. 1, 2007. Because much of the evidence on alleged Chinese hacking is classified, the best source for material on Chinese hacking and cyber warfare primarily comes from news reports.
[173] WINKLER, *supra* note 5, at 75.

capability."[174] A report by the U.S. Commission on Cybersecurity urged then President-elect Obama to create a Center for Cybersecurity Operations and to have a White House advisor oversee this new quasi-agency.[175] As of late December 2008, Mr. Obama was considering creating an office for cybersecurity as part of a general overhaul of U.S. intelligence agencies.[176]

Britain's MI5 intelligence service has stated that Chinese state organizations have conducted cyber espionage against British banks and financial services firms and that the Chinese Army was using the Internet to steal trade secrets from British companies doing business in China.[177] China was also suspected of a cyber attack on the Oak Ridge National Laboratory.[178] In November 2008, the *Wall Street Journal* reported that Chinese hackers had gained access to a "significant number of unclassified White House emails."[179] Just days later, Fox News reported that the International Monetary Fund ("IMF") computer system had been attacked by hackers.[180] Although authorities found no culprit, speculation centered on the Chinese. Even the Obama and McCain presidential campaigns were hacked; the Chinese were primary suspects.[181] According to John Tkacik, a former intelligence analyst, President-elect Obama will be presented with a National Intelligence Estimate (NIE) report highlighting extensive Chinese cyber espionage.[182]

---

[174] Julian Barnes with Ching-Ching Ni, *Chinese Hacking Worries Pentagon*, L.A. TIMES, Mar. 4, 2008, at A9.
[175] Keith Epstein, *U.S. is Losing Global Cyberwar, Commission Says*, BUS. WEEK, Dec. 7, 2008, http://www.businessweek.com/bwdaily/dnflash/content/dec2008/db2008127_817606.htm?chan=top+news_top+news+index+-+temp_dialogue+with+readers.
[176] Siobhan Gorman, *Obama Picks Military Man, Blair, as Top Spymaster*, WALL ST. J., Dec 20-21, 2008, at A4.
[177] WINKLER, *supra* note 5*,* 75.
[178] Messmer, *Cyber Espionage: A Growing Threat to Business, supra* note 51.
[179] Siobhan Gorman, *Chinese Hackers Get Access to Some White House Emails*, WALL STREET J., Nov. 8-9, 2008, at A2.
[180] Richard Behar, *Cyber-Hackers Break Into IMF Computer System*, Nov. 14, 2008, http://www.foxnews.com/printer_friendly_story/0,3566,452348,00.html.
[181] *Hackers and Spending Sprees*, Nov. 5, 2008, http://www.newsweek.com/id/167581/
[182] Behar, *supra* note 180.

The term 'cyber espionage' merits close attention. One must remember that when Congress passed the EEA in 1996, the United States had yet to enter the dot.com boom of the late 1990s; computers were not yet fully part of everyday American life. Thus Congress chose to criminalize the theft of *trade secrets* in its definition of economic espionage. Today, economic espionage need not be conducted by individuals in a particular locale, clandestinely working for the Chinese government within the physical locale of an American corporation.[183] The Chinese government and its agents may be hacking into American computer systems directly from China or from other locations in or outside the United States.[184] According to Winkler, foreign intelligence agencies rely on the wider hacker community to hide many of their crimes.[185] Thus, Chinese intelligence agencies may be able to misappropriate trade secrets from American corporations without ever having agents physically set foot in any corporate offices.

Cyber espionage refers to both the theft of trade secrets through hacking or hacking designed to disrupt fundamentally the cyber infrastructure of a state or vital components of its economy. The Pentagon has claimed that the Chinese military has viruses designed to attack enemy computer systems.[186] Indeed, American officials are concerned that China is employing cyberspace not only for espionage, but also to prepare for a hot war over Taiwan.[187] Hacking may also play a greater role in hot wars. During the 2008 Russian-Georgian War, Russian hackers successfully brought down Georgian governmental and media websites.[188] Although these attacks played no determinative role in the conflict and may have come from Russian activists rather than from Moscow, they served as a wake-up call for governments.

---

[183] *See supra*, Part II.B.
[184] For a discussion of the difficulty of tracing cyber attacks during the 2008 Russian-Georgian conflict, *see* Andrew Gray, REUTERS, *Georgia Hacking Stirs Fears of Cyber Militias*, Sept. 1, 2008.
[185] WINKLER *supra* note 5.
[186] Behar, *supra* note 184.
[187] *Cybersecurity: Beware the Trojan Panda*, THE ECONOMIST, Sept. 8, 2007, 2007 WL 17415933.
[188] Grey, *supra* note 184.

According to Air Force Gen. Gene Renuart, of U.S. Northern Command, a looming problem is that no one has "defined what would constitute an act of war in cyberspace."[189] Writing in the late 1990s, John J. Fialka argued for "a coherent, modern body of criminal law that deters economic espionage" and contended that the EEA was a good start.[190] In light of the myriad challenges posed by Chinese hacking, Congress should consider passing comprehensive legislation aimed at both preventing and punishing those individuals who actively engage in, or aid those who engage in, cyber espionage against American governmental facilities or corporations. The EEA provides a model for such legislation.

The EEA Provides a Model for Comprehensive Cyber Espionage Legislation

In 1996, when Congress held hearings on the threat posed by economic espionage, the Internet was still in its infancy. Now, as American national security is imperiled by hacking and cyber espionage, Congress should conduct both public and closed hearings on the threat posed by hacking, particularly hacking sponsored or directed by foreign governments. Such hearings would follow up on the US-China Economic and Security Review commission's 2008 annual report to Congress. That report concluded China is likely to take advantage of American cyber space because "the costs of cyber operations are low in comparison with traditional espionage or military activities [and because] determining the origin of cyber operations and attributing them to the Chinese government or any other operator is difficult."[191] Full Congressional hearings should include representatives from both American government and industry. Intelligence officials and think-tank analysts should also contribute to Congressional hearings that would both warn Americans of the threat posed by cyber espionage and send a signal to the Chinese

[189] *Id.*
[190] FIALKA, *supra* note 6, at 206.
[191] http://www.uscc.gov/annual_report/2008/EXECUTIVE%20SUMMARY.pdf., p. 9.

government that the United States is willing to devote significant resources into countering hacking directed against America's critical economic and military infrastructure.[192] Congress should use these hearings as an impetus to enact new, comprehensive legislation to counter cyber espionage.

The primary federal statute that criminalizes hacking is 18 U.S.C. § 1030, which criminalizes fraud and related activity in connection with computers.[193] The statute criminalizes the unauthorized access of a computer and the disclosure of information obtained by such access. Section 1030(a) specifically criminalizes acts where an individual illegally accesses a computer to obtain information that could be used to the advantage of a foreign government.[194] This statute, by its plain language, could be used to prosecute those persons caught hacking into American government computers to access information intended to benefit a foreign government. In light of the massive wave of both government-sponsored and independent cyber attacks that have occurred in recent years, and because of the specific threat posed by alleged Chinese hacking, Congress should pass new legislation directly aimed at countering cyber espionage.

This new legislation should be known as the CEA or Cyber Espionage Act. It would specifically criminalize acts of hacking intended to disrupt American economic or military

---

[192] *See, e.g.*, Mike Mount, *Report: China Trying to Crack U.S. Computers, Buy Nukes*, Mar. 3, 2008, http://www.cnn.com/2008/US/03/03/pentagon.china/index.html.

[193] *See* http://www.usdoj.gov/criminal/cybercrime/1030NEW.htm.

[194] 18 U.S.C. § 1030(a)(1) reads in full: "having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it."

computer infrastructure, military secrets, or trade secrets. The term 'hacking' should be broadly defined, much as "trade secrets" was in the EEA. This would allow prosecutors to investigate and to prosecute a broad array of crimes and would ensure that the CEA would apply to innovative computer crimes. Unlike the EEA, the CEA would be solely directed against acts intended to benefit a foreign government. The CEA should have separate provisions for hacking directed at American economic and corporate infrastructure, and against American defense and military computer infrastructure. The CEA would thus be the cyber espionage equivalent of § 1831 of the EEA.

Although the defense and intelligence communities should take the lead in combating cyber warfare, there are three reasons that a separate statute criminalizing hacking/cyber warfare is necessary. This would give federal prosecutors a tool that they could employ should American intelligence officials discover that persons within the United States are either engaging in hacking or aiding the Chinese or other foreign governments in hacking. Attacks emanating solely from outside the United States would be under the jurisdiction of the Pentagon or a related agency. Although it is difficult to trace the origin of hacking, it is not impossible.[195] A teenage hacker in Massachusetts, for instance, recently pled guilty to acts including hacking into corporate computer systems.[196] Similar to the enactment of § 1831 of the EEA, which allowed the Justice Department to play an active role in prosecuting the theft of trade secrets, the CEA would give federal prosecutors and the Department of Justice a significant role in investigating hacking attacks as they occur and in preparing evidence for potential criminal indictments. Any individuals who engage in hacking on behalf of a foreign government, even if not directly

[195] See Daniel A. Morris, *Tracing a Computer Hacker*, U.S. ATT'YS BULL., May 2001, http://www.usdoj.gov/criminal/cybercrime/usamay2001_2.htm.
[196] Press Release, U.S. Dep't of Justice, Juvenile Hacker Pleads Guilty, Nov. 18, 2008, http://www.cybercrime.gov/dshockerPlea.pdf.

sponsored by the government in question. This would include independent cyber attacks committed by persons who acted, albeit without authority, on behalf of a foreign government, and would be prosecuted under this statute rather than under § 1030(a)(1) or the EEA. The CEA, however, should be viewed as a tool that prosecutors could use in conjunction with the EEA in investigating and prosecuting new and more sophisticated forms of trade secret theft, hacking, and cyber espionage.

Second, a distinct cyber espionage-hacking statute would serve as a public warning to the Chinese government and others, that the United States is willing to devote significant resources into investigating and, if feasible, prosecuting foreign-sponsored hacking. Indeed, the very passage of the statute, and the concomitant press coverage that would follow, could serve as a very significant public acknowledgement by the Obama Administration that it is aware of ongoing Chinese hacking and that it intends to make this matter a national security priority. The enactment of the CEA would serve as a useful counterpart to military initiatives designed to disrupt and counter Chinese hacking and could serve as a basis for a series of frank U.S.-Chinese discussions over American concerns about China's computer warfare technology.

Third, because hacking that intentionally disrupts or disables military computer infrastructure vital to the national defense is more akin to an act of war than a crime, the statutory maximum penalty for prison time under the proposed CEA should be of a significantly higher duration than the penalty for § 1030(a)(1) crimes. The statutory penalty for § 1030(a)(1) illegal access to a computer and obtaining of information "with reason to believe such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation" is defined in 18 U.S.C. § 1030(c)(1)(A) as either a maximum of ten or

twenty years depending on whether the defendant had committed or had attempted another § 1030(a)(1) crime.[197] Rather than ten- and twenty-year maximum sentences, the CEA should allow for prosecutors to seek up to life imprisonment if it could be shown that the defendant's hacking activities both (1) intentionally and significantly disrupted American military and/or defense computer infrastructure and that (2) such an act served as the proximate cause of death of any American government official or service member. This second factor would ensure that minor disruptive cyber attacks were treated differently than cyber attacks that seriously impaired American economic, military, or political, capabilities. For instance, a cyber attack that impaired military command-and-control systems that lead to the death of an American serviceman would be treated differently from a minor cyber attack that proved to be little more than a nuisance. That said, both Congress and the United States Sentencing Commission could be asked to outline the basic parameters of what would be fair and just terms of imprisonment under the proposed CEA.

Conclusion

In this paper, I have argued that the Economic Espionage Act of 1996 has been a necessary, but not sufficient, means of countering Chinese economic espionage in the United States. While Congress rightly defined economic espionage in terms of the theft of trade secrets and defined trade secrets broadly, countering economic espionage is not a job solely for law enforcement and the legal system. Indeed, private actors, the State Department, and the Defense Department, all must work together to counter Chinese espionage. However, in light of the new threat of cyber espionage from Beijing, the EEA provides a useful model for Congress, which should enact new, comprehensive anti-hacking legislation, and for the Obama Administration,

[197] *See* 18 U.S.C. § 1030(a)(1) (2008), 18 U.S.C. § 1030(c)(1)(A-B) (2008).

which should treat the threat of Chinese economic espionage and cyber warfare on a similar to that of terrorism