STATE-SPONSORED CRIME: THE FUTILITY OF THE ECONOMIC ESPIONAGE ACT

Susan W. Brenner and Anthony C. Crescenzi***

*NCR Distinguished Professor of Law & Technology, University of Dayton School of Law
**CISSP & Principal Information Analyst, Dolphin Technology, Inc.

I. INTRODUCTION

Economic espionage and trade secret theft threaten our Nation's national security and economic well-being.[1]

The United States is facing an international challenge: economic espionage, the theft of our intellectual assets and proprietary information.[2] The events of September 11, 2001 pushed the seriousness of this activity to the far recesses of the public's consciousness. While this threat to our national security lacks the visceral impact of September 11th, the long term national security implications (a decline in economic competitiveness) stemming from the systemic theft of intellectual property has consequences no less serious than a

1. Economic Espionage Act of 1996, Pub. L. No. 104-294, 1996 U.S.C.C.A.N. 4034 (statement by President William J. Clinton upon signing H.R. 3723).

2. This Article adopts the definition of "economic espionage" included in the Economic Espionage Act of 1996, i.e., economic espionage consists of misappropriating trade secrets belonging to citizens of one country in order to benefit another country. *See infra* subpart III.A.2 (discussing the §1831 offense). The definition used in this Article is in one sense more generic than that incorporated in the Economic Espionage Act. The Act differentiates between the theft of trade secrets, which is carried out without the intent to benefit a foreign sovereign, and economic espionage. *See infra* subpart III.A.2. Those who steal trade secrets are prosecuted under 18 U.S.C. § 1832, while those who engage in economic espionage are prosecuted under 18 U.S.C. § 1831. *See infra* subpart III.A.2. For various reasons, foreign nationals who steal trade secrets belonging to U.S. citizens, presumably for the benefit of their own countries, are often prosecuted under 18 U.S.C. § 1832. *See* discussion *infra* subpart III.B.1. The definition of economic espionage used in this Article is not predicated on the offense charged. It looks to the nature of the conduct at issue and would, therefore, encompass instances in which those prosecuted under 18 U.S.C. § 1832 actually engaged in economic espionage, i.e., actually acted to benefit a foreign sovereign. The broader definition is necessary to implement the Article's focus on economic espionage as a unique type of criminal activity.

real-world terrorist attack. Espionage targeting intellectual assets and proprietary information is driven by the international competition characterizing a global economy.[3] Americans have long ignored the preeminent rule of international economic competition: "Expediency outgrosses morality."[4] The success or failure of our ability to compete will determine U.S. economic well-being and, ultimately, our national security. The global economy that emerged after the Cold War is replete with strong, independent, predatory competitors, a state of affairs that can be attributed largely to U.S. economic globalism and the showcasing of American technology.[5] The desire for American technology is the primary motivation for the continuing economic espionage activities undertaken by a multitude of foreign countries.

It has been obvious for over a decade that economic espionage is a serious problem.[6] Appreciating the seriousness of this threat, Congress passed the Economic Espionage Act of 1996; the President signed the Act into law on October 11, 1996.[7] The Economic Espionage Act (EEA) took a traditional approach to the activity at issue by treating the misappropriation of proprietary economic information as theft and criminalizing it.[8] Congress believed that by prosecuting and sanctioning those who unlawfully appropriate proprietary information, we can deter others from engaging in such conduct.[9]

---

3. J. Thompson Strong, *Tilting with Machiavelli: Fighting Competitive Espionage in the 1990s*, 7 INT'L J. OF INTELLIGENCE & COUNTERINTELLIGENCE (NO. 2) 161, 162 (1994).

4. *Id*. at 161–62.

5. William T. Warner, *International Technology Transfer and Economic Espionage*, 7 INT'L J. OF INTELLIGENCE & COUNTERINTELLIGENCE 143, 143–44 (1994).

6. *See, e.g.*, United States v. Hsu, 155 F.3d 189, 194 (3d Cir. 1998) ("The end of the Cold War sent government spies scurrying to the private sector to perform illicit work for businesses and corporations . . . and by 1996 . . . nearly $24 billion of corporate intellectual property was being stolen each year.").

7. *See, e.g., Hsu,* 155 F.3d at 194–95.

8. *See, e.g.,* Economic Espionage Act of 1996, Pub. L. No. 104-294, 11, 110 Stat. 3488, § 1831 (1996).

9. *See, e.g.*, S. Rep. No. 104-359, at 11 (1996). As stated in the report, "Only by adopting a national scheme to protect U.S. proprietary economic information can we hope to maintain our industrial and economic edge and thus safeguard our national security. Foremost, we believe that the greatest benefit of the Federal statute will be as a

Prosecution and punishment can contribute to preventing economic espionage, but they, alone, cannot accomplish this, for reasons we explain below. Our purpose in writing this Article is to point out the danger of relying on traditional solutions in a nontraditional era; reacting to completed acts of economic espionage by sanctioning the perpetrator(s) is an effective strategy only if they can be identified, located, and apprehended.

Part II explains what economic espionage is and why it is a serious problem. Part III reviews the provisions and enforcement of the Economic Espionage Act and explains why it is not a viable approach to economic espionage in the twenty-first century. Part IV considers how we can more effectively address economic espionage.

II. THE PROBLEM

This Part outlines the problems we face from economic espionage. As subpart II.A notes, trade secrets, which are at the heart of economic espionage, extend beyond classified military information and technologies into a world in which information has become our most important asset. subpart II.B describes how cyberspace has altered the traditional dynamic involved in economic espionage; the Internet has erased significant financing, proximity, scale, and physical constraints while at the same time protecting an attacker's identity and reducing risk. subpart II.C explains that economic espionage has become a worldwide threat, with a long list of "usual suspects." Subpart II.D notes that economic espionage can yield significant business and competitive advantages and explains that an understanding of these advantages is necessary to understand the legal and illegal practices of information gathering. Finally, subpart II.E reviews the overall scope of the problem, while subpart II.F. focuses on hacker tools and the logistical methods of present day economic espionage.

---

powerful deterrent." *Id*.

A. State-Sponsored Economic Espionage

> [S]ome foreign countries, including the major players, . . . continued to employ state actors—including their intelligence services—as well as commercial enterprises, particularly when seeking the most sensitive and difficult to acquire technologies.[10]

The critical element of the EEA, which is analyzed in Part III, *infra,* is the involvement of foreign governments, their agents, or instrumentalities deriving benefits from the acquisition of a nation's trade secrets. U.S. expenditures on research and development initiatives are in excess of two hundred billion dollars annually and are the largest by far of any developed country. This fact, together with the reality that economic competition is an immutable aspect of international relations, makes the United States a target rich environment for economic espionage activity. The critical issue this Article highlights is the fact that espionage is much broader than efforts by traditional adversaries to avail themselves of strictly classified military information. The current threat is posed by traditional and nontraditional adversaries. This threat is directed at the spectrum of proprietary and military technologies that have traditionally provided the United States with a qualitative economic and military advantage. These advantages translate directly to the economic and military strength that has enabled the United States to attain its current status as the world's only true super-power.

The EEA resulted from Congress' recognizing that foreign elements were engaging in active and on-going economic espionage operations.[11] These activities are designed to exploit

---

10. OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXECUTIVE, ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE—2004 ix–x (2004), http://www.nacic.gov/publications/reports_speeches/reports/fecie_all/fecie_2004/FecieAnnual report_2004_NoCoverPages.pdf [hereinafter ONCIX 2004 REPORT].

11. *See, e.g.*, 142 CONG. REC. S12201, S12207-08 (1996). Senator Specter stated:

> In an increasingly complex and competitive economic world, intellectual property forms a critical component of our economy. As traditional industries shift to low-wage producers in developing countries, our economic edge depends to an ever-increasing degree on the ability of our businesses and

the benefits of U.S. research and development without expending the financial capital necessary to develop indigenous technologies or trade secrets. In today's world, a nation's economic viability is the true measure of its power.[12] Military strength is contingent upon an economy's ability to integrate technological advancements having dual use (commercial and military) applications.

> inventors to stay one step ahead of those in other countries. And American business and inventors have been extremely successful and creative in developing intellectual property and trade secrets. America leads the nation's [sic] of the world in developing new products and new technologies. Millions of jobs depend on the continuation of the productive minds of Americans, both native born and immigrants who find the freedom here to try new ideas and add to our economic strength. Inventing new and better technologies, production methods, and the like, can be expensive. American companies and the U.S. Government spend billions on research and development. The benefits reaped from these expenditures can easily come to nothing, however, if a competitor can simply steal the trade secret without expending the development costs. While prices may be reduced, ultimately the incentives for new invention disappear, along with jobs, capital investment, and everything else that keeps our economy strong. For years now, there has been mounting evidence that many foreign nations and their corporations have been seeking to gain competitive advantage by stealing the trade secrets, the intangible intellectual property of inventors in this country. The Intelligence Committee has been aware that since the end of the cold war [sic], foreign nations have increasingly put their espionage resources to work trying to steal American economic secrets. Estimates of the loss to U.S. business from the theft of intangible intellectual property exceed $100 billion. The loss in U.S. jobs is incalculable.

Id.

12. Thierry Oliver Desmet, *The Economic Espionage Act of 1996: Are We Finally Taking Corporate Spies Seriously?*, 22 HOUS. J. INT'L L. 93, 96–97 (1999).

> Since the end of the Cold War, the focus of intelligence and counterintelligence efforts has shifted from military and political targets to technological and economic ones. Nations have been reshaping their intelligence agencies and investigative resources to be more responsive to the competitive and global needs of businesses. The Cold War has been replaced by the Economic War. The increase in trade secret theft has placed the technologies of U.S. companies, ranging from simple textile formulas to complex defense technology, at great risk.

Id. (notes omitted).

B. *Economic Espionage and the Internet*[13]

> *Increasingly, foreign entities need not even come to the United States to acquire sensitive technology but, instead, can work within their own borders. There, U.S. firms have difficulty securing their secrets and have few legal protections once proprietary information has been lost.*[14]

Economic espionage is far from a new phenomenon. The development of the U.S. textile industry in the early 1800s is a direct result of Francis Cabot Lowell visiting England and memorizing the workings of their power looms. Upon returning to New England he recruited a master mechanic to recreate and develop what he had memorized.[15] The Chinese were able to protect their proprietary interests in the silk trade for in excess of two thousand years, further illustrating that economic espionage is not a recent phenomena.[16] The secret was ultimately lost, according to one account, when a Chinese princess married a foreign prince and smuggled silkworm eggs out of China by hiding them in her voluminous hair piece (circa AD 440).[17] A second account credits two Nestorian monks (circa AD 550) with smuggling silkworm eggs in their hollow bamboo staves for delivery to the Byzantine Emperor Justinian.[18] The point of these historical anecdotes is to demonstrate that human behavioral characteristics have not changed over the ages. This behavior continues to provide the incentive for reducing an adversary's competitive advantage by utilizing espionage techniques to elicit proprietary secrets.

The challenge of protecting intellectual and proprietary assets has been made more difficult by the arrival of the information age and the Internet. Information has become a marketable commodity with an inherent value and intrinsic self-

---

13. For more on this issue, see *infra* subpart III.B.2 (discussing real-world crime and online crime).

14. *See* ONCIX 2004 REPORT, *supra* note 10, at 1.

15. *See* John J. Fialka, *While America Sleeps,* 21 WILSON Q. 48, 51 (1997).

16. *See, e.g.*, *History of Silk,* http://silkroadfoundation.org/artl/silkhistory.shtml.

17. *Id*.

18. *Id*.

worth. The fact that technological progress has evolved to the point where information is stored on networks, many of which are linked together by the Internet, has changed the framework relating to information protection and the legal boundaries that traditionally served to constrain the dissemination of sensitive data to nonauthorized users.

Prior to the era of digital connectivity, intellectual property and trade secrets were targeted by foreign intelligence services, competitors and criminals, using collection methods consisting of classic agent recruitments, volunteers, surveillance, surreptitious entry, and specialized technical operations.[19] All of these techniques were characterized by boundaries imposed by conventional three-dimensional limits relating to proximity, scale, physical constraints, and patterns.[20] The Internet and its employment of a new medium, cyberspace, dramatically changed the nature of information collection whether the collector is a foreign intelligence service, competitor or criminal.[21] Cyberspace does not restrict a collector to traditional techniques. It expands collection methods and operations by leveraging existing tradecraft with a dramatic reduction in risk and a corresponding logarithmic increase in potential reward.[22]

Collectors employing Internet collection techniques are not bound by the need to have proximate access to targeted information or agents. The process of spotting, assessing, recruiting, evaluating, and deploying potential agents no longer requires that a case officer make direct contact to accomplish tasks relating to logistics, communications, and security. These

---

19. *See* ONCIX REPORT 2004, *supra* note10. at 3.

20. Susan W. Brenner, *Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?*, 30 RUTGERS COMP. & TECH. L.J. 1, 1–9 (2004) [hereinafter Brenner, *A New Model of Law Enforcement*].

21. *Id*.

22. One source notes, for example, that "[m]any spy agencies around the world are adapting classic spy techniques from military and political espionage endeavors to conduct economic espionage." Edwin Fraumann, *Economic Espionage: Security Missions Redefined,* 57 PUB. ADMIN. REV. 303 (1997). According to this author, these "[a]gencies use a number of 'intrusive' methods to obtain classified proprietary economic information relating to trade secrets," which include "[e]avesdropping through wiretapping, bugging offices, or capturing cellular telephone conversations" and "[p]enetrating a computer system through hacking into the network, hard drive, or software." *Id.*

basic house-cleaning functions frequently permitted counter-intelligence agents to detect, deter, and disrupt an adversary's operations. Their absence necessitates a major shift in counterintelligence operations to counter the absence of traditional indicators of collection activity.

Prior to the employment of digital memory devices and network connectivity, intelligence operatives were limited with respect to the scale of their operations and individual case officer and agent supervisory spans of control. "Cyber case officers" using virtual agents do not have the scale of their operations limited to a finite number of "cyber agents" but, instead, can deploy virtual cyber resources in unlimited quantities simultaneously. These cyber agents can respond to multiple collection requirements, remotely targeting multiple objectives simultaneously with limited risk. The reduction in risk is due to the absence of physical constraints present in traditional intelligence operations.

Perhaps the greatest advantage to the collector is the ability to utilize the absence of proximity, scale, and lack of physical constraints together with deception schemes intended to conceal the identity and location of the actual adversary. The novelty of digital intelligence-gathering and concomitant absence of patterns is a primary factor in the reduction of risk, making these methods so attractive. A victimized government, corporation, or individual today will have an exceptionally challenging task merely identifying the cyber collector who has targeted their information. This is, of course, assuming the victim is even aware of the fact that he or she has been subject to an attack!

Additional factors driving intelligence operatives to fully engage in virtual collection methods and operations is the well-documented reluctance of victims to report digital penetration and the fact that several studies reflect exceptionally low awareness of victims recognizing that they have been subjected to attacks.

C. Economic Espionage: The Usual Suspects?

[T]he Federal Bureau of Investigation . . . has reported that at least twenty-three foreign governments actively target the intellectual property of U.S. corporations. One FBI study also found that of 173 countries, 100 were spending resources to acquire U.S. technology.[23]

Reports published by the Central Intelligence Agency and Government Accounting Office have publicly identified foreign countries engaging in state-sponsored collection activities targeting intellectual property and trade secrets belonging to the United States.[24] Recognizing the severity of foreign collection operations targeting U.S. technology, Congress has required an annual report which will keep it informed of the threat parameters.[25] This report, which is entitled "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage," is published annually in a classified and unclassified version.[26] The 2003 unclassified version notes that "[f]oreign businessmen, scientists, academics, and government officials from more than 90 countries continued targeting sensitive U.S. technologies and corporate trade secrets in both 2002 and 2003, according to a variety of reporting available to

---

23. Chris Carr & Larry Gorman, *The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act,* 57 BUS. LAW 25, 27 (2001–2002).

> The following countries are allegedly extensively engaged in espionage activities against American companies: France, Israel, Russia, China, Iran, Cuba, the Netherlands, Belgium, Germany, Japan, Canada, India, and several Scandinavian countries. The most frequently targeted industries appear to include aerospace, biotechnology, computer software and hardware, transportation and engine technology, defense technology, telecommunications, energy research, advanced materials and codings, 'stealth' technologies, lasers, manufacturing processes, and semi-conductors.

Id.

24. *See*, *e.g.,* OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXECUTIVE, ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE—2003 iii (2004), http://www.nacic.gov/publications/reports_speeches/ reports/ fecie_all/fecie_2003/fecie_2003.pdf [hereinafter ONCIX 2003 REPORT].

25. *See id*.

26. *Id*.

the U.S. Counterintelligence (CI) Community."[27] A primary distinction between the two versions of the report relates to the identification of specific foreign countries engaging in various collection activities. However, despite the omission of specific country identities in the open version of the Annual Report, cursory research of open sources permits an analyst to make judgments likely reflecting those nations most actively engaged in these operations.

A 1996 article in the *Washington Post* referred to a CIA public report identifying the governments of France, Israel, China, Russia, Iran, and Cuba as being extensively involved in economic espionage. According to the article, "[a]s for Japan, which is often accused of high-tech thievery, the CIA said that nation's efforts to collect economic data 'are mostly legal and involve seeking openly available material or hiring well-placed consultants.'"[28] The information reported in the article was released by the CIA as part of a declassified hearing volume on "Current and Projected National Security Threats to the United States."[29]

In addition to the countries acknowledged in the CIA report, recently published news accounts and other documents have included South Korea and Germany as active participants in efforts aimed at collecting U.S. sensitive information.[30] It should be stated that historically the U.S. government has been reluctant to publicly identify foreign governments considered to be its traditional allies as engaging in economic espionage. This reluctance reflects the diplomatic reality that relations between governments occur on many levels simultaneously. Therefore, publicly acknowledging that an ally is aggressively attempting to collect sensitive government information may serve to needlessly escalate diplomatic tensions. Normally, these concerns are addressed via back channels with private warnings

---

27. *Id*. at v.

28. Paul Blustein, *France, Israel Alleged to Spy on U.S. Firms*, WASH. POST, Aug. 16, 1996, at A28.

29. S. Rep. No. 105-1, at 12 (1997).

30. *See, e.g.*, INTERAGENCY OPSEC SUPPORT STAFF, OPERATIONS SECURITY: INTELLIGENCE THREAT HANDBOOK § 5 (1996), http://www.fas.org/irp/nsa/ioss/threat96/part05.htm [hereinafter OPERATIONS SECURITY].

and subtle signals indicating that continued behavior deemed unacceptable may rise to a level outside of normal diplomatic channels, and if the behavior continues, it may be accompanied by embarrassing political consequences. Additionally, it is generally acknowledged that all countries engage in various aspects of espionage to one degree or another. The inclination to promulgate a "holier than thou" attitude with respect to espionage has the potential to be perceived as highly hypocritical in the event of a retaliatory response.

The advent of the information age and corresponding global connectivity has increased the vulnerabilities of U.S. intellectual assets. The 2003 Annual Report to Congress reports that multiple sources of evidence suggest that foreign interests are increasingly looking to cyber tools as a means of enhancing their ability to illegally acquire sensitive information.[31] Digital incursions are difficult to detect, and there is a lack of factual data conclusively establishing the dollar value of assets lost annually by these methods. However, estimates by the American Society of Industrial Security, U.S. Chamber of Commerce, and PricewaterhouseCoopers, derived from a 2002 survey of Fortune 1000 corporations and 600 small to mid-sized U.S. companies, state that proprietary information and intellectual property losses accounted for between fifty-three and fifty-nine billion dollars.[32] There is a consensus that the

---

31. *See* ONCIX 2003 REPORT, *supra* note 24, at v. The 2004 Annual Report to Congress specifically notes that:

> [g]lobal connectivity via the Internet adds to U.S. vulnerability. A variety of evidence suggests that foreign interests continue looking to cyber tools as a means to illegally acquire trade secrets. The number of information security incidents reported to the U.S. Computer Security Readiness Team is an indicator of the rapid rate at which cyber activity has grown in recent years. The number of such incidents rose from about 500,000 events in 2002 to 1.4 million in 2003 and then to 56 million events in the first six months of 2004, according to press reports.
>
> Detection of such intrusions is difficult but, even when detected, a recent private U.S. survey indicated that more than half of the impacted firms do not report the breach for fear of reducing shareholder value. As a result, no one is certain how much technology and sensitive proprietary information are lost annually to cyber theft.

See ONCIX 2004 REPORT, *supra* note 10, at 2.

32. ASIS Int'l, U.S. Companies Lost up to $59 Billion in Proprietary Information

Internet has provided traditional and nontraditional adversaries with a low-risk, inexpensive collection mechanism capable of targeting and circumventing security countermeasures.[33] Anecdotal country information obtained exclusively from open sources is presented to illustrate the international variety of threats and cyber tactics employed by various foreign governments.

1. France[34]

The French view of economic competition is characterized by the belief that a state of continuous competition exists among nations where market advantages are pursued by all available means.[35] This helps to explain the lengthy history of French government intelligence agencies targeting U.S. economic and proprietary data. The French General Directorate of External Security (DGSE) has been reported as targeting economic intelligence since at least 1964.[36] Corporations reported to be targeted by the DGSE in the past have included Loral Space Systems and Hughes Aircraft, the former Lockheed Missile and Space Company, TRW, and GTE.[37] Information targeted included satellite and telecommunications data.[38]

Former director of French Intelligence Pierre Marion is frequently quoted as stating, "getting intelligence in economic, technological, and industrial matters [from] a country [with] which you are allied . . . is not incompatible with the fact of being allied."[39] A unique aspect of French economic espionage collection efforts, detailed by Peter Scwweizer in his book

---

and Intellectual Property, http://www.asisonline.org/newsroom/pressReleases1093002 trends.xml (last visited Jan. 27, 2006).

33. ONCIX 2003 REPORT, *supra* note 24, at 1.

34. For more on France's economic espionage activities, *see, e.g.*, JOHN J. FIALKA, WAR BY OTHER MEANS: ECONOMIC ESPIONAGE IN AMERICA 87–100 (1997).

35. *See, e.g.*, JOHN A. NOLAN III, A CASE STUDY IN FRENCH ESPIONAGE: RENAISSANCE SOFTWARE, U.S. OFFICE OF COUNTERINTELLIGENCE 1 (2000), http://www.hanford.gov/oci/maindocs/ci_r_docs/frenchesp.pdf.

36. *See, e.g.*, OPERATIONS SECURITY, *supra* note 30, § 5.

37. *Id*.

38. *Id*.

39. PETER SCHWEITZER, FRIENDLY SPIES: HOW AMERICA'S ALLIES ARE USING ECONOMIC ESPIONAGE TO STEAL OUR SECRETS 99 (1993) (alteration in original).

Friendly Spies, involves the use of "honorary correspondents" or part-time agents.[40] This network of part timers is comprised of corporate officials living overseas, French bankers in New York City and bureaucrats at the European Community in Brussels.[41] Employees of nationalized French companies are particularly prone to act as part time collectors.[42]

In 1996, the French established the Ecole de Guerre Econimique (School of Economic Warfare).[43] It was established by the Defense Consultancy International, a semi-public company linked to the French Defense Ministry.[44] "French academics, journalists, retired military and intelligence officials work for the school."[45] The school's director Christian Harbulot is quoted as stating:

[T]he U.S. is the top priority. There is true industrial competition and there are many fields where we have everything to lose. We cannot let ourselves be pushed around. A huge number of companies have disappeared because they were bought out or destroyed by the Americans. We have to protect ourselves.[46]

It is evident that the French view the cyber arena as a significant resource in satisfying their collection requirements. It has been reported as early as 1987 that French intelligence co-opted a French hacker by threatening prosecution unless he cooperated with their request that he infiltrate the French hacking community. French intelligence desired information relating to the latest hacking techniques and tools.[47] It is highly unlikely that the interest exhibited by French Intelligence has declined in the intervening years subsequent to this event, and

40. *Id*. at 100.

41. *Id.*

42. *Id*. at 100–01.

43. *See* Kelly Uphoff, *Tilting the Playing Field: Economic Espionage Hasn't Gone Away Since 9/11,* JEWISH INST. FOR NAT'L SEC. AFF. (2005), http://www.jinsa.org/articles/articles.html/function/view/categoryid/2518/documentid/2835/history/3,2360,656,1082,2518,2835.

44. *Id*.

45. *French Economic Spies Target U.S.*, WORLD NET DAILY, Dec. 11, 2004, http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=41873.

46. *Id*.

47. *See* JAMES ADAMS, THE NEXT WORLD WAR 160 (Simon & Schuster 1998).

with the explosion of spyware and other virtual resources, the capabilities of the French intelligence service are presumed to have increased in sophistication and effectiveness.

2. Russia

During the Cold War, Russian efforts to collect sensitive military information were considered the primary intelligence threat targeting the United States. A recent article in the November 15, 2004 issue of *U.S. News & World Report* has a report stating intelligence insiders furnished information revealing that Vladimir Putin had recently increased Russian resources targeting the United States to levels reaching the high water mark of the Cold War.[48] However, current collection efforts are aimed at trade and manufacturing secrets of major U.S. corporations, like IBM and ExxonMobil, with the intent of obtaining information relating to contracts that corporate America is pursuing. The United States' involvement in the War on Terror is perceived as a major distraction facilitating these collection efforts.[49]

This information makes incidents like the one occurring in October 2000, where Microsoft staff noticed a problem with new accounts being created that did not match their audit logs, potentially more significant.[50] In researching the anomaly, it was discovered that an employee received an e-mail carrying a worm and inadvertently installed it.[51] The worm, subsequently identified as the QAZ worm, functioned as a backdoor tool giving remote users control of an infected PC.[52] After gaining entry to the infected computer, the worm disguised itself as a

48. Paul Bedard et al., *The Reds Are Dead, But the Spies Are Still Around*, U.S. NEWS & WORLD REPORT, Nov. 15, 2004, at 10. Russia is also targeting other countries. *See, e.g.*, *German Intelligence Worried About Increasing Russian Espionage,* GLOBAL NEWS WIRE, Feb. 3, 2005.

49. Bedard, *supra* note 48, at 10.

50. John Schwartz, *Irregular New Accounts Alerted Microsoft to Network Intruder*, N.Y. TIMES, Oct. 29, 2000, § 1, at 28.

51. Liam Lahey, *Microsoft Gets Hacked*, ITWORLDCANADA, Oct. 17, 2000, http://www.itworldcanada.com//Pages/Docbase/ViewArticle.aspx?D=idgml-e164b03b-6041-4229-b34a-899cd0d968d2.

52. *Id*.

NOTEPAD.EXE file and could be spread through the network as a shared resource.[53] The worm then sent a remote signal to a computer in Asia identifying the location of the newly infected computer[54] and also, according to some analysts, automatically downloaded and installed various hacking tools from another remote site.[55] The intruder then used a program to collect passwords and automatically sent them to an e-mail address in Russia.[56] Using the collected passwords, the intruder posed as a Microsoft employee working at a remote location and accessed sensitive proprietary information.[57] It cannot be conclusively established if this action was state-sponsored; however, this does not lessen the significance of this espionage activity since the loss of sensitive information was the ultimate result.

An incident like this, referred to as worm-based espionage, establishes that it is not necessary for a collector to "hack" a computer directly, but rather, it may employ virtual agents (worms) to perform the penetration and report back to the case officer. The utilization of virtual agents poses significant challenges to those responsible for security countermeasures and complicates the legal remedies traditionally intended to serve as deterrents. Virtual agents are not constrained by international borders. Consequently, when remotely deployed, their detection and subsequent investigation may involve multi-national investigative coordination, jurisdictional disputes, and legislative disparity with respect to whether a criminal act has been committed.

---

53. *Id.*

54. Charles R. Fagg, *QAZ*, SANS Inst., Aug. 6, 3002, at 3, http://www.sans.org/rr/whitepapers/malicious/47.php.

55. Ted Bridis & Rebecca Buckman, *Microsoft Hacked! Code Stolen?*, ZDNET, OCT. 26, 2000, http://news.zdnet.com/2100-9595_22-525083.html.

56. *Id.*

57. George A. Chidi, Jr. & Laurea Rohde, *Microsoft's Network Suffers Hack Attack*, NETWORK WORLD, Oct. 27, 2000, http://www.networkworld.com/news/2000/1027 bighack.html.

3. Japan

Japan's economic espionage and intelligence collection activities directed against the United States are unique in several respects. The Japanese government has a limited formal intelligence organization; however, its major corporations, in conjunction with the Japanese Ministry of International Trade and Industry (MITI), have active corporate intelligence organizations that collect economic and political information. [58] Japan has used human sources within U.S. corporations, bribed corporate employees to purchase proprietary data, and used Japanese graduate students and researchers to collect sensitive information from universities and research institutes.[59]

An example of Japanese researchers involved in espionage activities occurred in May 2001, when Japanese researchers Hiroaki Serizawa and Takashi Okamoto were indicted on charges of stealing genetic materials pertaining to Alzheimer's disease from the Cleveland Clinic Foundation in May 1999. A plea bargain resulted in a reduction of charges against Serizawa from industrial espionage to one count of perjury. Okamoto resigned from the clinic in July 1999 and returned to Japan. The

---

58. *See, e.g.*, Christopher G. Blood, Comment, *Holding Foreign Nations Civilly Accountable for Their Economic Espionage Practices*, 42 IDEA 227, 230 (2002).

> Japanese agents, operating out of the Japanese consulate in San Francisco, worked with a researcher at Fairchild Semiconductors in Silicon Valley to steal corporate plans and secrets on computer developments. As much as 160,000 pages of confidential information may have been passed through consular officials to Japanese corporations that were in competition with Fairchild. Indirect support for such activities by foreign governments is not uncommon. As early as 1972, the Japanese Parliament established the Economics Industry Deliberation Council to direct intelligence gathering. Oversight of this council was by the Ministry for Trade and Industry, which decades earlier had been the conduit for the Japanese government to subsidize worldwide travel by thousands of Japanese businessmen for the purpose of gathering information on foreign technological advances. By the late 1980s, a CIA classified report indicated that more than three-fourths of Japan's intelligence resources were aimed at acquiring secrets and information on technological advances from the United States and Western Europe.

Id.

59. OPERATIONS SECURITY, *supra* note 30, § 5.

United States claimed Okamoto acted with the intent of profiting by delivering the materials to Japan's Institute of Physical and Chemical Research, popularly known as RIKEN. RIKEN employed Okamoto after he returned to Japan.[60]

In another incident, a Japanese television network (NHK) played a prominent role in aiding Japanese corporate and governmental interests in penetrating the trade secrets of American biotechnology firms.[61] Using the pretense of a documentary film to gain access to several biotechnology firms, NHK personnel, attempted to film proprietary information processes and documents.[62] Detailed interview data was solicited from scientists relating to their research activities and combined with film footage permitting NHK to obtain significant insights into the technologies, R&D activities and strategic capabilities of these firms.[63]

Estimates that eighty-five to ninety percent of intelligence collected by Japanese government and industry sources is economic information largely based on proprietary data have been reported by publications such as "The OPSEC Journal."[64] A 1987 CIA report identified two top Japanese intelligence priorities as 1) intelligence relating to access to foreign sources of raw materials and 2) detailed information on technological and scientific developments in the United States and Western Europe.[65] "The report states that nearly eighty percent of all Japanese intelligence assets are focused on gathering technical and economic information from the United States and Europe."[66]

Currently, a debate is occurring in Japan with respect to the legality of deploying cyber weapons. The Japanese

---

60. Tetsuya Morimoto, *First Japanese Denial of U.S. Extradition Request: Economic Espionage Case*, 20 No. 7 INT'L ENFORCEMENT L. REP. 288 (2004).

61. *See* William M. Fitzpatrick, *Uncovering Trade Secrets: The Legal and Ethical Conundrum of* Creative *Competitive Intelligence*, 68 SAM ADVANCED MGMT. J., 4, 7 (2003).

62. *Id*.

63. *Id*.

64. OPERATION SECURITY, *supra* note 30, § 5.

65. Jeff Augustini, *From Goldfinger to Butterfinger: The Legal and Policy Issues Surrounding Proposals to Use the CIA for Economic Espionage*, 26 L. & POL'Y INT'L BUS. 459, 478 (1995).

66. *Id*. (discussing the Congressional Cox Committee Report).

Constitution prohibits its military from engaging in offensive operations. Determining whether the deployment of computer viruses and hacking techniques is considered an offensive military tactic requires clarification. However, there is no prohibition against using cyber tactics to elicit sensitive information. Published reports reflect that the Japanese Self Defense Forces have budgeted for the establishment of a cyberforce. It would be highly unusual if capabilities developed for this cyberforce are not deployed. It is conceivable that virtual assets developed for the self-defense forces could be provided to private sector intelligence gathering organizations for operational use.

4. China

In 1999, the Congressional Cox Committee Report on the People's Republic of China's (PRC) espionage activities directed at the United States was released.[67] This document provided a comprehensive examination of Chinese espionage targeting various U.S. industries for the express purpose of accelerating the acquisition and development of dual-use science and technology intended to enhance Chinese economic performance. The Cox Report's findings include a determination that in 1986 a major initiative identified as the 863 Program was approved by the Chinese leadership to advance the Chinese economy. According to the Report, this program produced nearly 1,500 research achievements by 1996. Approximately 30,000 scientific and support personnel were actively engaged on this project.[68]

Numerous accounts of Chinese economic espionage activities have been reported by the press supporting the findings of the Cox Report. In its March 22, 1999 issue, *Newsweek* magazine outlined a shopping list of PRC technology requirements that included those listed below. A comparison of this list and the types of technology reported in legal

67. *Id.*

68. Scott L. Wheeler, *How Beijing Gets U.S. Defense Plants*, INSIGHT ON THE NEWS, Mar. 6, 2003, http://www.insightmag.com/media/paper441/news/2003/03/18/World/How-Beijing.Gets.U.Defense.Plants-384405.shtml.

proceedings as being sought by agents of the PRC tends to validate the *Newsweek* information.[69]

Newsweek List

Avionics: Aircraft engines, air frames, gyroscopes and simulation equipment and software . . .
Materials: High-strength polymers and strong plastics used in . . . stealth technology . . .
Supercomputers: Aerospace . . . guidance systems, launchers, telemetry technology and . . . communications gear
Biotechnology: Manipulation of living cells to create new drugs . . .
Medical technology: . . . [P]harmaceuticals and . . . advanced equipment for testing and treatment.[70]

Economic Espionage Incidents

Three Chinese immigrants, two of whom were employees of Lucent Technologies, were arrested for attempting to take the source code for the PathStar Server, build a company around it, and market it in China to a conglomerate officially owned by the Chinese government. The subsequent FBI investigation revealed e-mails allegedly showing the partners listing intellectual assets identical to those of PathStar. Unfortunately for Lucent, the investigation further revealed that the source code had been conveyed to the Chinese corporation and is unlikely to be recoverable.[71]

In December 2003, a Silicon Valley grand jury indicted Fei Ye and Ming Zhong for allegedly conspiring to steal computer-chip trade secrets from Sun Microsystems, NEC Electronics, Trident Microsystems, and Transmeta. The two were allegedly involved in a plot to hatch a research project called Supervision, which was funded by the Chinese government to finance a high-

69. *See* Daniel Klaidman et al., *Open Secret*, NEWSWEEK, Mar. 22, 1999, at 28.

70. *Id*.

71. Massimo Calabresi, *The Company of Spies*, TIME, May 14, 2001, at 51.

tech company that would compete with U.S. chipmakers.[72]

In a second Silicon Valley case, Qing Jiang was arrested in Cupertino, California on charges that he illegally exported microwave amplifiers to China. These items are dual-use products that can be used for civilian and military applications.[73] "According to the affidavit, the components were being sent to a company with the same address as [the Chinese] Ministry of Communication[s], Telemetry and Telecontrol, also known as the 54th Research Institute, which develops missile-guidance systems."[74]

The close correlation between the *Newsweek* "shopping list" and the items targeted by Chinese representatives described in the legal sampling provided is indicative of an organized collection effort targeting sensitive U.S. information. It can be surmised that for every successful legal intervention relating to these collection efforts, an undetermined number of covert operations never detected by U.S. law enforcement agencies are likely to have occurred.

5. Germany

German targeting efforts aimed at sensitive or proprietary information have not received the degree of public reporting that characterizes those countries publicly identified in the 1996 CIA public report. However, despite not being publicly identified by the CIA, several writers have accused Germany of using computer-intrusion techniques to gather information on foreign competitors with the intention of passing this information to German corporations.[75] These reports further allege that "[t]he German Federal Intelligence Service (BND) [has] created a classified, computer intelligence facility outside [of] Frankfurt

---

72. Edward Iwata, *More U.S. Trade Secrets Walk Out Door with Foreign Spies,* USA TODAY, http://www.usatoday.com/tech/news/2003-02-12-espionage_x.htm (last visited Jan. 31, 2006).

73. Laurie J. Flynn, *Chinese Businessman acquitted of Illegal High-Technology Exports*, N.Y. TIMES, May 10, 2005, at C15.

74. Edward Iwata, *More U.S. Trade Secrets Walk Out Door with Foreign Spies*, USA TODAY, http://www.usatoday.com/tech/news/2003-02-12-espionage_x.htm (last visited Jan. 31, 2006).

75. OPERATIONS SECURITY, *supra* note 30, § 5.

designed to permit intelligence officers to enter . . . networks and databases from countries around the world."[76] This program is alleged to have been code named RAHAB and to have accessed computer networks in the United States as well as other countries.[77]

Anecdotal evidence supporting German collection activity became public in 1991 when IBM accused the German intelligence service of eavesdropping on its telecommunications and passing this information to German competitors. IBM lost several significant business opportunities at this time and speculated that these losses were likely due to inside information obtained by German competitors in this fashion.[78] Other reports point to 1970 as the year the BND was given a mandate to collect more information within the United States.[79] The breakup of the former Soviet Union has permitted the BND to focus its efforts on economic intelligence, and consequently, the United States has become its primary economic intelligence target.[80]

6. Israel

Israel is unique in that it has a special relationship with the United States extending to its inception. However, there has never been any doubt that Israeli interests are not subjugated by this relationship to the extent that its perceived national security interests are compromised. Israel views itself as being in a permanent state of war and, consequently, deploys its intelligence services in a very aggressive manner. A former intelligence official was quoted in the September 3, 2004 issue of the *Los Angeles Times*, stating, "There is a huge, aggressive, ongoing set of Israeli activities directed against the United States. Anybody who worked in counterintelligence in a professional capacity will tell you the Israelis are among the most aggressive and active countries targeting the United

76. *Id.*

77. *Id*.

78. Peter Schweizer, Op-Ed., *Our Thieving Allies*, N.Y. TIMES, Jun. 23, 1992, at A21.

79. Augustini, *supra* note 65, at 481.

80. *See id.*

States."[81] Several anecdotal incidents are presented to illustrate the aggressive nature of Israel's intelligence services.

An article appearing in the *Washington Times* on December 16, 2004 is the most recent charge in a long running history of published reports alleging Israeli espionage activities directed at the United States. The article reports that Israeli defense officials in the United States have been accused by the FBI of industrial espionage. The Israeli Defense Ministry denied that its representatives have been accused of industrial espionage but acknowledged that the U.S. government has complained about overly insistent information-gathering by Israelis at military equipment exhibitions.[82] A Defense Ministry spokesman maintained that no accusations were made, but rather asserted concern about the aggressive collection of information that was not classified.[83] The Israeli spokesman, however, did acknowledge that some of the information is still protected by U.S. officials, and this served to create a grey area that became the source of friction.[84]

The *Wall Street Journal* reported in 1992 that Israeli agents attempted to steal Recon Optical's top secret airborne spy camera.[85] Recon Optical, an Illinois company, received a contract from the Israeli Air Force to manufacture aerial reconnaissance cameras. The terms of the contract permitted Israel to have members of its Air Force on site at Recon's manufacturing facility. Israeli Air Force Officers were observed by company security officials attempting to remove Recon Optical trade secrets from the plant in violation of the contractual agreement.[86]

In a third instance receiving minimal publicity, foreign reporting sources *Jane's Information Group* and *Le Monde* both

---

81. Bob Drogin & Greg Miller, *Israel Has Long Spied on U.S., Say Officials*, L.A. TIMES, Sep. 3, 2004, at A1.

82. Joshua Mitnick, *U.S. Accuses Officials of Spying*, WASH. TIMES, Dec. 16, 2004, at A17.

83. *Id*.

84. *Id*.

85. Israeli Spying: The Mother of All Scandals, http://www.whatreally happened.com/motherofallscandals (last visited Nov. 4, 2005).

86. *See* Blood, *supra* note 58, at 230.

commented on the absence of U.S. news organizations to follow up on a story reported by *Fox News*.[87] This story reported that the U.S. Drug Enforcement Agency (DEA) and other members of the U.S. intelligence community were concerned about the dominance of highly sensitive areas of U.S. telecommunications by Israeli companies Verint (formerly Comverse Infosys) and Amdocs.[88] These firms provided U.S. law enforcement agencies with wiretapping equipment and software record-keeping data of virtually all calls placed by the twenty-five largest U.S. telephone companies.[89] Speculation that the hardware and software permitted "catch gates," which comprise the content of wiretaps, was responsible for the concern of U.S. officials.[90] DEA's alleged intense interest was prompted by its 1997 purchase of twenty-five million dollars in interception equipment from Israeli companies.[91]

7. South Korea

The Defense Intelligence Agency has reported that South Korean economic espionage activities directed against the United States "have included stealing information from computerized databases maintained by U.S. government agencies and U.S. companies."[92] South Korea is alleged to aggressively pursue its economic espionage activities by accessing closed source environments utilizing electronic access, physical access and access to personnel to obtain proprietary information.[93]

South Korean intelligence officers are purported to be "extremely active in collecting political, economic, and

---

87. John F. Sugg, *Israeli Spies Exposed*, ALTERNET, Apr. 22, 2002, http://www.alternet.org/story/12928.

88. *Id.*

89. *Id*.

90. *Id*.

91. *Id*. For more on Israel's economic espionage efforts, *see, e.g.*, Ed Blanche, *With Friends Like These. . .*, THE MIDDLE EAST, Jun. 30, 2002.

92. OPERATIONS SECURITY, *supra* note 30, § 5.

93. Edwin Fraumann, *Economic Espionage: Security Missions Redefined*, 57 PUB. ADMIN. REV. 303, 306 (1997).

technological secrets."[94] The best-known public example of this collection effort was the apprehension and conviction of U.S. citizen and Navy employee Robert Kim. Court documents indicated that Mr. Kim's dealings with the "South Koreans focused on his knowledge of a classified computerized command system that linked ships to satellites."[95] The South Korean National Planning Agency is technically proficient, well funded and has a well-organized network of informers who are paid large sums for their efforts in collecting proprietary information.[96] In addition to assigning members of its intelligence service to its overseas embassies under diplomatic cover, South Korean intelligence agents are also given nonofficial cover positions with South Korean industrial conglomerates such as Hyundi, Samsung, and others.[97]

D. Business/Competitive Espionage

Competitive espionage has two aspects: the legal and ethical pursuit of information that is of value in the day-to-day activities by businesses attempting to gain a competitive advantage and the unethical or illegal pursuit of information relating to a competitor's products or information. In essence, both types of activity are characterized by intelligence collection methods and operations. It is the mechanics of these operations that distinguishes their legality.

The majority of business entities today have some form of a competitive intelligence organization. Typically, these operations may be formally labeled as "competitive intelligence" departments by large corporations, or their functions may be accomplished more informally by marketing or other departments within smaller organizations. Ultimately, their location on an organizational chart is irrelevant. Their mission is intended to enable decisionmakers to more effectively manage information that will enhance the competitive position of the

---

94. *Id*.

95. David Johnston, *Korean Spy Case Called More Serious than was Thought*, N.Y. TIMES, Oct. 3, 1996, at A8.

96. Edwin Fraumann, *Economic Espionage: Security Missions Redefined*, 57 PUB. ADMIN. REV. 303 (1997).

97. *Id*.

company. It is interesting to note that competitive intelligence is a body of knowledge that has attained professional status, with a governing body requiring its membership to adhere to strict levels of professional ethics.[98] The Society of Competitive Intelligence Professionals (SCIP) is a global nonprofit membership organization for individuals involved in creating and managing business knowledge. Competitive intelligence, as defined by SCIP, is the legal and ethical collection and analysis of information regarding the capabilities, vulnerabilities, and intentions of business competitors.[99]

Collecting information for capability and vulnerability analysis can be accomplished ethically by utilizing data-mining techniques, patent tracking, war game exercises, psychological profiling of competitor decisionmakers, and attending industry trade shows.[100] The process of remaining cognizant of a competitor's intentions coupled with the ability to recognize unanticipated market developments can be facilitated by effective use of the Internet and mass media.[101] These methods, when supplemented by recurring conversations with customers, suppliers, partners, employees, industry experts, and other knowledgeable parties, enable information gathering to be accomplished successfully within ethical parameters.[102]

Unfortunately, not all efforts to collect business information are conducted in accordance with the SCIP guidelines for ethical behavior. Ethics are compromised when traditional espionage tradecraft is employed to gather data on targeted business adversaries. Techniques utilized to induce a breach of confidence on behalf of a targeted individual may include misrepresentation, bribery, fraud, improperly obtaining financial data from third parties, illicit access, wiretapping, and a variety of Internet collection tools. The cyber techniques that

---

98. *See* Society of Competitive Intelligence Professionals, http://www.scip.org/2_faq.php (last visited Jan. 29, 2006).

99. Society of Competitive Intelligence Professionals, http://www.scip.org/2_overview.php (last visited Jan. 29, 2006).

100. Stephen H. Miller, *Competitive Intelligence—An Overview*, COMPETITIVE INTELLIGENCE, at 3–4, http://www.scip.org/Library/overview.pdf.

101. *Id* at 4.

102. *Id*.

can be deployed present a significantly greater risk due to the pervasive growth of networks used by businesses to store and manage sensitive information. In contrast, the collector of sensitive information faces a reduced risk in information gathering due to the fact that information can be gathered remotely. Combining this reduced risk with the fact that many cyber attacks are not detected and business are reluctant to acknowledge successful attacks, the advantages of cyber collection are easily recognizable. Social engineering practices combined with tools such as key stroke loggers, viruses, worms, and Trojans can all be deployed with great effect.

E. Scope of the Problem

A 2002 survey sponsored by PriceWaterhouseCoopers and the American Society of Industrial Security (ASIS), titled "Trends in Proprietary Information Loss," is an attempt to quantify the magnitude of the problem.[103] Computer hackers and foreign intelligence services were identified as significant risks. The experience of ASIS council members suggests that these groups represent the greatest threat to an organization's proprietary information, which reinforces the necessity of examining new approaches in confronting the challenge of cyber information collection operations.[104]

Cyber tactics employed by adversaries are fundamentally similar to traditional methods involving fraud, deception, covert access, insider recruitment, vendor visits, and specialized technical operations. However, each of these tactics has its potential effectiveness magnified when current technology is used to leverage its impact.

These tactics are illustrated by incidents like the one reported in August 2002, when Niku Corporation discovered its server logs contained information that an IP address belonging to Business Engine, a competitor, had used Niku passwords to access the company's network more than 6,000 times.[105] In

---

103. PRICEWATERHOUSECOOPERS, CHAMBER OF COMMERCE & ASIS FOUND., SURVEY REPORT, TRENDS IN PROPRIETARY INFORMATION LOSS 26 (2002).

104. *Id.*

105. Joel McNamara, Secrets of Computer Espionage: Tactics and

excess of 1,000 documents were downloaded during the intrusions. Compromised information contained data about upcoming features, lists of potential customers, and pricing and sales.[106] The ensuing FBI investigation revealed that since October 2001, outsiders had logged onto the internal Niku network using fifteen different accounts and passwords to access proprietary information.[107]

The future is likely to be replete with similar cyber collection techniques used to target sensitive information. It is not difficult to anticipate that current Phishing schemes intended to generate cash could easily be configured for purposes of industrial espionage. Deceptive websites replicating various divisions of a corporation would not be difficult to construct. Information requested for ostensibly legitimate purposes, if elicited, could be used to access other more sensitive sites. This entire process could be accomplished remotely with minimal risk even in the event the Phishing site was actually discovered. The same counterfeit site could be used to download Trojans containing spyware programs. An employee following instructions believed to be disseminated by corporate authorities could inadvertently download keystroke loggers, password grabbers, or other malware, which would reveal passwords providing access to sensitive files. The possibilities for using known cyber techniques to accomplish espionage goals are limited only by the imagination of the perpetrators.

Distributed denial of service attacks (DDoS), viruses, and bot networks could also be deployed in efforts to impede a competitor's efforts to compete or to extort cash. Law enforcement agencies have begun to informally advise industry counterparts, collaborating within Electronic Crime Task Forces or the Infragard Membership Alliance, of an increase in the number of cyber extortion incidents.[108] One such case reported in the *Wall Street Journal* involved an entrepreneur who allegedly employed third parties to launch DDoS attacks against three

---

Countermeasures 5 (Wiley Publishing, Inc. 2003).

106. *Id*.

107. *Id*.

108. *See* Brenner, *A New Model of Law Enforcement, supra* note 20, at 52–53.

competitors.[109] Using bot-virus software, five to ten thousand hijacked computers were directed to attack the designated target competitors. According to the legal complaint, the three targeted companies suffered damages estimated to exceed two million dollars. Computer Economics Inc., a research firm in Aliso Viejo, California, estimated that the cost of viruses in terms of lost revenue and repair has increased from thirteen billion dollars in 2003 to seventeen and one half billion dollars in 2004.[110] Despite the highly subjective nature of these cost estimates, the fact that the trend reflects an ongoing increase is not in dispute.

F. Criminal Espionage

Criminal activities intended to obtain intellectual property or sensitive information are traditionally characterized by a profit motive derived by exchanging information for cash or receivables easily convertible to cash. These actions were typically crimes of opportunity whereby disgruntled or former employees availed themselves of insider access to procure information of value and market it to interested third parties. Frequently, the distinctions between purely criminal motives and competitive espionage were blurred. This was due to the marketability of the data obtained being limited primarily to competitors or state-sponsored agents performing their duties in an attempt to assist indigenous enterprises to compete in the global marketplace.

Terrorists employing asymmetric tactics targeting critical infrastructure sectors have added a new dimension to the scope of the problem. Critical infrastructure sectors were recognized as prime targets, and consequently, the intellectual property and sensitive information maintained by these infrastructure sectors have become legitimate terrorist objectives. The vulnerability of these targets to cyber reconnaissance and attack techniques challenges the effectiveness of law enforcement's traditional investigative practices. Cyber collection

---

109. Cassel Bryan-Low, *Growing Number of Hackers Attack Web Sites for Cash*, WALL STREET J., Nov. 20, 2004, at A1.

110. *Id.*

methodologies circumventing traditional security countermeasures and law enforcement practices have made gathering sensitive data easier. Cybercrime's lack of historic characteristics crucial to today's law enforcement model relating to proximity, scale, physical constraints, and patterns requires the application of innovative security countermeasures and law enforcement strategies. The traditional "reactive" approach to criminal/terrorist incidents will not be successful in achieving the goal of mitigating detrimental impact to critical infrastructure sector customers and the accompanying negative economic consequences caused by service disruptions.

A collaborative approach to the protection of sensitive critical infrastructure information will be required to counter digital collection techniques. Law enforcement agencies lack the expertise needed to independently address advancing software developments in spyware, keystroke loggers, password crackers, and the variety of malware being developed by criminal elements. The fact that these criminal elements are emerging in geographic locations ranging from Brazil to Eastern Europe and the Former Soviet Union, and are capable of launching their criminal operations remotely demonstrates the changing nature of criminal espionage. A key characteristic of traditional crime—proximity between victim and offender—is no longer a requirement for the targeting of sensitive critical infrastructure information.[111] Spyware and keystroke loggers can be inserted into networks by insiders or by Trojan software downloaded surreptitiously and written for the express purpose of permitting remote access to sensitive data present on information networks.[112]

DDoS attacks are becoming a preferred extortion method of organized criminals taking advantage of the absence of scale permitted by the wholesale harvesting of computers for attack purposes. Anecdotal reporting from law enforcement officers participating in Electronic Crime Task Forces indicates organized crime gangs are contracting out cyber disruption

111. Brenner, *A New Model of Law Enforcement*, *supra* note 20, at 1–9.

112. *See, e.g.*, Ravi Nessman, *Israelis Nab 18 in Computer Espionage Case,* A.P., May 29, 2005, http://abcnews.go.com/Technology/wireStory?id=802259&CMP=OTC-RSSFeeds0312.

services for purposes of extortion. These DDoS attacks are accomplished by employing harvesting techniques that use a variety of malware to gain control of thousands of computers for subsequent attacks by bot networks. Intruders gain unauthorized access to systems via backdoors inserted by mass-mailing worms. This access permits the intruder to execute command-and-control software capable of directing these bot networks as they execute DDoS attacks. The nature of this type of criminal attack presents challenges to law enforcement procedures steeped in a tradition of conditioned responses bound by physical constraints. Similarly, the evolving nature of digital networking has not matured sufficiently to permit the recognition of patterns necessary for the application of an effective law enforcement methodology.

III. THE LAW: ECONOMIC ESPIONAGE ACT (EEA)

The EEA is Congress' attempt to deal with the problem outlined in Part II, *supra*. Subpart III.A reviews the provisions of the EEA—its definition of "trade secrets" and its imposition of criminal liability on those who steal U.S. trade secrets. Subpart III.B examines the systemic and contextual factors that erode the EEA's effectiveness as a tactic for dealing with such activity.

A. Provisions

Until 1996, there was no federal statute that specifically criminalized economic espionage, that is, the theft of commercial trade secrets.[113] Federal prosecutors charged those who engaged in such activity with various other crimes, including the interstate transportation of stolen property or mail or wire fraud.[114] This approach, however, was ultimately unsatisfactory: Because federal prosecutors sometimes had trouble "shoe-

---

113. *See, e.g.*, COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL § VIII.A (2001), http://www.cybercrime.gov/ipmanual/08ipma.htm#VIII.A [hereinafter PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL]. "Trade secrets" are defined in the text above.

114. *See id.*; s*ee also* 18 U.S.C. § 2314 (2000) (governing interstate transportation of stolen property); 18 U.S.C § 1341 (2000) (governing mail fraud); 18 U.S.C. § 1343 (2000) (governing wire fraud).

horning" the theft of trade secrets into the above statutes and because of the increased recognition of the increasingly important role that intellectual property plays in the well-being of the American economy, Congress enacted the Economic Espionage Act of 1996, effective October 11, 1996.[115]

Codified at 18 U.S.C. §§ 1831-1839, the EEA criminalizes the theft of U.S. trade secrets.[116] As Part I noted, the EEA takes a traditional approach to economic espionage by treating the misappropriation of proprietary economic information as theft and criminalizing it.[117] The premise is that by prosecuting and

115. PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.A.

116. *See id*.

117. *See, e.g.*, 142 CONG. REC. S12201, S12208 (daily ed. Oct. 2, 1996) (statement of Arlen Specter). Senator Specter stated:

> [A] major problem for law enforcement in responding to the increase in such thefts has been a glaring gap in Federal law. For many years, the United States has had a variety of theft statutes in the United States Code. These laws are derived primarily from the common law of theft. For example, it violates Federal law to move stolen property across State lines. In order to violate such laws, however, the courts have held that the property stolen cannot be intangible property, such as trade secrets or intellectual property. In addition, theft usually requires that the thief take the property with the intention of depriving the lawful owner of its use. But such a test [is] useless when a person copies software and leaves the original software with the lawful owner, taking only the secrets on the software but leaving the physical property. The lawful owner still has full use of the property, but its value is significantly reduced.
>
> In order to update Federal law to address the technological and economic realities of the end of the 20th century, I began working earlier this year with Senator [Kohl] and officials from the Department of Justice and the Federal Bureau of Investigation on developing legislation. We developed two separate bills, that were introduced as S. 1556 and S. 1557. The former bill broadly prohibited the theft of proprietary economic information by any person. The latter bill was more narrowly drawn to proscribe such thefts by foreign nations and those working on behalf of foreign nations. At the end of February, I chaired a joint hearing of the Intelligence Committee and the Judiciary Subcommittee on Terrorism, Technology, and Government Information on the issue of economic espionage. Continuing to work closely with members of the Judiciary and Intelligence Committees, the administration, and various industry groups, Senator [Kohl] and I were able to produce the bill the Senate is today considering.

Id. at S12208.

sanctioning those who unlawfully appropriate proprietary information, we can deter others from engaging in such conduct.

1. Trade Secret

The EEA contains an unusually broad definition of trade secrets.[118] Under 18 U.S.C. § 1839(3), a trade secret "includes . . . all types of information, however stored or maintained, which the owner has taken reasonable measures to keep secret and which has independent economic value."[119] The EEA encompasses intangible property, including "information stolen in electronic form or merely memorized, [but] is not intended to cover general knowledge or skills learned on a job when an employee leaves one company and moves to another in the same or similar field."[120]

Unlike patents, trade secrets need only be "minimally novel."[121] This means "a trade secret must contain some element that is not known and sets it apart from what is generally

---

118. *See* PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.2.C (noting that the EEA's definition "is broader than other definitions of trade secret,' including notably the definition . . . in the Uniform Trade Secrets Act"); *see, e.g.*, Unif. Trade Secrets Act § 1, 14 U.L.A. 537–51 (Supp. 1986); *see also* RESTATMENT (THIRD) OF UNFAIR COMPETITION § 39 (2005) (providing an alternate definition of trade secret).

119. PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.2.C; *See also* 18 U.S.C. § 1839(3) (2000):

> [T]he term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if
>
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public . . . .

120. Onimi Erekosima & Brian Koosed, *Intellectual Property Crimes,* 41 AM. CRIM. L. REV. 809, 813–14 (2004).

121. *See, e.g.*, PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.2.C.

known."[122] The key attribute of a trade secret under the EEA is that it is information which "is not . . . generally known to, and not being readily ascertainable through proper means by, [sic] the public."[123] It is not necessary that every aspect of the information be confidential; a trade secret can consist of a "combination of elements that are in the public domain," if the trade secret itself constitutes "a unique, effective, successful and valuable integration of the public domain elements."[124]

To qualify as a trade secret, information must also derive independent economic value from not being generally known to the public.[125] The statute does not require that a trade secret be valued at a specific jurisdictional amount for criminal liability to be imposed upon those who misappropriate it.[126] According to the U.S. Department of Justice (Department of Justice),

> the value of the trade secret need not be established with precision and can be determined through a variety of different methods, including: (1) the amount similar trade secret information sold for on the legitimate open market, if available; (2) a reasonable royalty calculation based on what a willing buyer would pay a willing seller for the technology in an arms-length transaction; (3) the amount of research and development costs expended by the trade secret owner; and, (4) as a last resort, the thieves' market price that the defendant actually received or paid in exchange for the technology.[127]

The final requirement for bringing information within the EEA's definition of a "trade secret" is that the owner(s) of the

---

122. *Id.* In the legislative history of the EEA, Congress noted that "[w]hile we do not strictly impose a novelty or inventiveness requirement . . . for material to be considered a trade secret, looking at the novelty or uniqueness of a piece of information or knowledge should inform courts in determining whether something is a matter of general knowledge, skill or experience." 104 CONG. REC. S12201, S12212 (daily ed. Oct. 2, 1996) (Managers' statement for H.R. 3723, the Economic Espionage Bill).

123. Prosecuting Intellectual Property Crimes Manual, *supra* note 113, § VIII.B.2.c.

124. *Id.* (quoting Buffets, Inc. v. Klinke, 73 F.3d 965, 968 (9th Cir. 1996)).

125. *See supra* note 119 and accompanying text.

126. *See* PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.2.C.

127. *Id.*

information must have taken reasonable measures to keep the information secret. [128] In this respect, trade secret law differs fundamentally from the laws that protect other types of property; theft and other statutes do not impose a similar requirement.[129] To come within the provisions of the EEA, the owner of information must have utilized protective measures that were reasonable under the circumstances; the nature and extent of security employed is not an absolute.[130] To impose criminal liability for violating the EEA, "prosecutors must be able to establish that the security measures used by the victim to protect the trade secret were reasonably commensurate with the value of the trade secret."[131]

According to the Department of Justice, the EEA ensures that information does not lose its status as a trade secret as the result of disclosures made to law enforcement agencies that are investigating or prosecuting an EEA case.[132] The Department of Justice bases this conclusion on two provisions of the EEA. First, section 1835 of title 18 of the U.S. Code authorizes courts dealing with EEA prosecutions to "enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws."[133] Second, 18 U.S.C. § 1835(2) states that the

---

128. *See supra* note 119 and accompanying text.

129. *See* PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.2.c ("[A] defendant can be convicted for stealing a bike even if the victim failed to protect it by leaving it unlocked on his front porch.").

130. *See id.*; *see, e.g.*, Reingold v. Swiftships, Inc., 126 F.3d 645, 650 (5th Cir. 1997).

131. PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.2.c. To that end, "prosecutors should determine the extent of the security used to protect the trade secret, including physical security and computer security, as well as the company's policies on sharing information with third-parties." *Id.*

132. 18 U.S.C. § 1835 (2000). As the Department of Justice notes, such disclosures are essential if EEA cases are to be successfully prosecuted. *Id.*

133. *Id.* The Department of Justice continues:

> This section is aimed at protecting the victim's trade secret information during . . . a criminal prosecution. Such protection would be unnecessary unless it was contemplated that victims would first provide the government with the trade secrets for use in the criminal investigation and prosecution. In addition to the protection afforded . . . there are additional restrictions on

EEA does not prohibit "the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation."[134] The Department of Justice deduces, from the combined effect of these provisions, that "it is unnecessary for federal prosecutors or law enforcement agents to sign protective orders with victims before accepting trade secret information."[135]

2. Offenses

The EEA creates two different offenses: a § 1831 offense and a § 1832 offense, each of which was intended to encompass a specific type of activity. The EEA also imposes liability for attempts and conspiracies, as explained below.

§ 1831 Offense

Section 1831 of title 18 of the U.S. Code criminalizes "economic espionage," which it defines as a theft of trade secrets that benefits a foreign government, foreign instrumentality or foreign agent. More precisely, § 1831 makes it a crime to steal, copy, download, purchase, or possess a trade secret intending or knowing that doing so will benefit a foreign agency.[136] The EEA

> the disclosure of trade secret information. . . . As a result, trade secret owners who disclose information to law enforcement representatives should not be deemed to have waived trade secret protection.

PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.2.c. For more on the use of protective orders, *see id.* § VIII.B.9.

134. 18 U.S.C. § 1833(2)(2000).

> The inclusion of this section, together with 18 U.S.C. § 1835, demonstrates that Congress intended to ensure that someone who becomes aware of an EEA violation has no disincentive to report criminal activity to law enforcement. If disclosures to law enforcement, whether by the owner of a trade secret or a third-party, eliminated trade secret protection, Congressional intent would be frustrated.

PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.2.c.

135. PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.2.c.

136. *See* 18 U.S.C. § 1831 (2000). Like its counterpart, the § 1832 offense, the § 1831 crime has three basic elements:

> Under either section, to obtain conviction . . . the government must prove

defines "foreign instrumentality" as "any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government."[137] It defines "foreign agent" as "any officer, employee, proxy, servant, delegate, or representative of a foreign government."[138]

In a § 1831 prosecution, the "government must show that the defendant knew or had a firm belief that misappropriation would benefit a foreign entity. When this entity 'is not, *per se*, a government entity (e.g., a business), there must be evidence of foreign government sponsorship or coordinated intelligence activity.'"[139] The requirement that the conduct has been undertaken to benefit a foreign entity "is to be interpreted broadly and is not limited to an economic benefit, but includes a reputational, strategic, or tactical benefit."[140]

For "foreign instrumentalities" such as corporate and other business entities, the EEA requires that the instrumentality have been "substantially owned" or controlled by a foreign government.[141] While the EEA does not define "substantially," the Department of Justice takes the position that the use of this term "suggests that the prosecution does not have to prove complete ownership, control, sponsorship, command, management, or domination."[142] The EEA's legislative history

---

> beyond a reasonable doubt that: (1) the defendant stole, or without authorization of the owner, obtained, destroyed or conveyed information; (2) the defendant knew or believed that this information was a trade secret; and (3) the information was in fact a trade secret.

PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.2. The § 1832 offense then adds an intentional element: intent to benefit a foreign government, foreign instrumentality or foreign agent. *See id.*

137. 18 U.S.C. § 1839(1) (2000).

138. 18 U.S.C. § 1839(2) (2000).

139. PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.3 (citing 142 CONG. REC. S12201, S12212 (daily ed. Oct. 2, 1996)).

140. *Id*. (quoting H.R. REP. NO. 104-788 (1996)).

141. *See* 18 U.S.C. § 1839(1).

142. PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.3.

states the following:

> Substantial in this context, means material or significant, not technical or tenuous. We do not mean for the test of substantial control to be mechanistic or mathematical. The simple fact that the majority of the stock of a company is owned by a foreign government will not suffice under this definition, nor for that matter will the fact that a foreign government only owns 10 percent of a company exempt it from scrutiny. Rather the pertinent inquiry is whether the activities of the company are, from a practical and substantive standpoint, foreign government directed.[143]

Section 1831, therefore, does not apply when "a foreign corporation misappropriates the trade secret and there is no evidence of sponsorship or coordinated intelligence activity' by a foreign government." [144]Such a corporation could, however, be prosecuted under § 1832.

§ 1832 Offense

The offense created by 18 U.S.C. § 1832 shares three elements with the § 1831 offense: To obtain a conviction, the government must prove that (i) the defendant stole, or without authorization of the owner, obtained, destroyed, or conveyed information which (ii) the defendant knew or believed was a trade secret, and (iii) the information was in fact a trade secret.[145]

Unlike the § 1831 offense, the § 1832 crime does not require the government to prove that the defendant acted with the intent to benefit a foreign entity to secure a conviction.[146] The government must, however, prove two additional *mens rea*

143. *Id.* (quoting 142 CONG. REC. S12201, S12212 (daily ed. Oct. 2, 1996) (Manager's statement for H.R. 3723, the Economic Espionage Bill).

144. *Id.* (quoting 142 CONG. REC. S12201, S12213 (daily ed. Oct. 2, 1996)); *see* David W. Simon, *Prosecution of IP Theft Increases; Under the Economic Espionage Act and Other Laws, the DOJ is Targeting Stolen Corporate Intellectual Property*, NAT'L L.J., Aug. 11, 2003, at 15.

145. *See supra* note 136.

146. *See* PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.2.

elements. First, it must prove that the defendant's act of misappropriating the trade secret "was intended for the economic benefit of a person other than the rightful owner (which can be the defendant, a competitor of the victim, or some other person or entity)."[147] The government must also prove that the defendant intended to "injure" the owner of the trade secret.[148] "According to the legislative history of the EEA, this provision does not require the government to prove malice or evil intent, but merely that the actor knew or was aware to a practical certainty that his conduct would cause some disadvantage to the rightful owner.'"[149] As the Department of Justice explains, this requirement should not prove onerous for prosecutors:

> By definition, in order for a trade secret to have value, it must confer a commercial advantage to the owner. Once the information is disclosed to another for the recipient's benefit, the trade secret loses its value. Accordingly, in many cases, establishing this element may not require additional evidence beyond that required to establish that the defendant acted for the economic benefit of someone other than the owner. For example, when a trusted employee of a computer chip manufacturer steals a prototype chip and conveys it to a known direct competitor of the owner, the disclosure of the information to the competitor may be sufficient circumstantial evidence to establish the requisite intent.[150]

The government must also prove another non-*mens rea* element to obtain a conviction under § 1832: that the trade secret "is related to or included in a product that is produced for

147. *Id*. § VIII.B.4.a; s*ee also* 18 U.S.C. § 1832(a) (2000). Consequently, "a person who misappropriates a trade secret but who does not intend for anyone to gain economically from the theft cannot be prosecuted under 18 U.S.C. § 1832." PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.4.a.

148. PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.4.b.

149. *Id.* (quoting H.R. REP. NO. 104-788 (1996)); *see* 18 U.S.C. § 1832(a).

150. PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.4.b.

or placed in interstate or foreign commerce."[151] This element establishes federal jurisdiction.[152] As the Department of Justice explains, it is usually not difficult to establish the "commerce" nexus:

> [W]here the trade secret is related to a product actually being manufactured and sold, this element would be easily established by evidence of interstate sales. Where a product is still in the development phase but is being developed to be sold in interstate commerce, the victim's intent to distribute the product in the future can be adequately demonstrated either by direct witness testimony or by documentary evidence describing the intended goals of the project.[153]

Attempt and Conspiracy

Sections 1831 and 1832 each impose liability for attempting and/or conspiring to commit the respective offenses they define.[154] In *United States v. Hsu,*[155] the Third Circuit held that the attempt offense created by § 1832(a)(4) requires that the defendant have taken a "substantial step" toward the

---

151. 18 U.S.C. § 1832(a); s*ee* PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.4.c ("This element encompasses two issues: that the trade secret be related to a product, and that the product was produced for or placed in interstate or foreign commerce.").

152. *See* PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.4.c.

153. *Id.* Furthermore, it is not difficult to establish the "commerce" nexus for products still in the research and development stage:

> It is possible that a defendant might argue that products still in the research and development stage are not yet being produced for interstate commerce' because such items are not yet being produced' for sale. This argument should not be persuasive. If this argument were to prevail, much of the protection of the EEA would be lost, since a trade secret is often most valuable during the development phase. Once the product embodying the trade secret is released to the public, the value of the trade secret is often lost because the product can be examined and the trade secret obtained or deduced.

Id.

154. *See* 18 U.S.C. § 1831(a)(4)-(5) (2000); 18 U.S.C. § 1832(a)(4)-(5).

155. 155 F.3d 189 (3d Cir. 1998).

commission of the substantive offense.[156] Both of the conspiracy offenses specifically require the commission of an overt act.[157]

The *Hsu* court also rejected defense arguments that one charged with attempt or conspiracy to violate the EEA could invoke the defense of legal impossibility.[158] The defendants in that case, who were charged with both conspiracy and attempt under 18 U.S.C. § 1832, argued that they could not be held liable if the information they allegedly misappropriated was not, in fact, a trade secret.[159] The Third Circuit disagreed, noting first that under modern law, attempt liability is properly predicated on the circumstances as the defendant believed them to be. "The government can satisfy its burden under § 1832(a)(4) by proving beyond a reasonable doubt that the defendant sought to acquire information which he or she believed to be a trade secret, regardless of whether the information actually qualified as such."[160] The Third Circuit also held that legal impossibility is not a defense to a charge of conspiracy under § 1832(a)(5) because the gravamen of conspiracy is the illicit agreement to commit a criminal act, not the actual commission of such an act.[161] Since the offense of conspiracy is predicated on the agreement, it is only necessary that the goals of the conspiracy, that is, the theft of actual trade secrets, were objectively unattainable.[162] At least two other circuits have reached similar conclusions.[163]

156. *See id.* at 202. Since the statute is silent on the issue, the court construed it in accordance with the Model Penal Code, which requires a substantial step for the imposition of attempt liability. *See id.*

157. *See* 18 U.S.C. §§ 1831(a)(5), 1832(a)(5).

158. *See Hsu*, 155 F.3d at 202–04.

159. *See id.* at 199.

160. *Id.* at 203.

161. *See id.* at 203–04.

162. *See id.* at 203.

163. *See* United States v. Lange, 312 F.3d 263, 268 (7th Cir. 2002); United States v. Yang, 281 F.3d 534, 541–44 (6th Cir. 2002).

Extra-territorial Jurisdiction

Section 1837 of the EEA confers extra-territorial jurisdiction in EEA prosecutions.[164] It is intended to rebut the presumption against the extra-territorial applicability of U.S. laws[165] and, in that regard, departs from other intellectual property law. Neither U.S. copyright nor patent law explicitly incorporates extra-territorial jurisdiction.[166] Section 1837 states that the provisions of the EEA apply:

> to conduct occurring outside the United States if (1) the offender is a natural person who is a citizen or . . . resident alien of the United States, or an [entity] organized under the laws of the United States or a State or political subdivision thereof; or (2) an act in furtherance of the offense was committed in the United States.[167]

B. Enforcement

> *"[R]isks remain small, while potential rewards skyrocket."*[168]

This subpart examines issues that undermine the EEA's effectiveness as a means of dealing with economic espionage. Subpart III.B.1 describes how systemic factors—forces influencing the criminal justice process in the United States—

---

164. *See* 18 U.S.C. § 1837 (2000).

165. *See* PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL, *supra* note 113, § VIII.B.10. As the U.S. Supreme Court has stated:

> It is a longstanding principle of American law 'that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.' . . . This 'canon of construction . . .' serves to protect against unintended clashes between our laws and those of other nations which could result in international discord.

Equal Employment Opportunity Comm'n v. Arabian Am. Oil Co**.,** 499 U.S. 244, 248 (1991) (quoting Foley Bros., Inc. v. Filardo, 336 U.S. 281, 285 (1949) and citing McCulloch v. Sociedad Nacional de Marineros de Honduras, 372 U.S. 10, 20–22 (1963)).

166. *See, e.g.*, Andrew Beckerman-Rodau, *Trade Secrets—The New Risks to Trade Secrets Posed by Computerization,* 28 RUTGERS COMPUTER & TECH. L.J. 227, 234 (2002).

167. *See* 18 U.S.C. § 1837.

168. James Srodes, *Washington Seeks Terrorists While Allies Steal Trade Secrets,* WORLD TRADE, Apr. 2002, at 12, *available at* 2002 WLNR 10520016.

impede its enforcement. Subpart III.B.2 examines contextual factors—the environment in which economic espionage occurs. As noted earlier, the EEA approaches economic espionage as a type of crime.[169] Therefore, it incorporates traditional assumptions about crime in the physical world—assumptions that do not hold when criminal activity moves online—into a virtual environment.[170] The influence of these assumptions therefore makes the EEA an increasingly problematic strategy for dealing with online economic espionage.[171]

1. Systemic Factors

Initially, enforcement of the EEA proceeded cautiously. An early version of the Act included the requirement that all prosecutions be approved by the Attorney General.[172] While this provision was not included in the final version, then-Attorney General Janet Reno sent the Senate a letter in which she promised that the Department of Justice would not, "for a period of five years after implementation of the Act," file charges under the EEA "without the personal approval of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division."[173] Reno's letter also pledged that this requirement would be "implemented by published regulation,"[174] and it was. Section 0.64-5 of title 28 of the Code of Federal Regulation, which remained in effect until October 11, 2001, incorporated the approval requirement and

169. *See supra* subpart III.A; *see also infra* subpart III.B.2.

170. *See infra* subpart III.B.2.

171. *See infra* subpart III.B.2.

172. One reason for adding the requirement was apparently a concern that the statute would be misused to "interven[e] in commercial disputes best handled through civil litigation." Memorandum from U.S. Attorney Gen. John Ashcroft Renewing the Approval Requirement for § 1831 Prosecutions under the Economic Espionage Act of 1996 (Mar. 1, 2002), http://www.cybercrime.gov/eea1996.htm [hereinafter Ashcroft Approval Requirement Memo]. Another concern was the potential international consequences of filing a case under § 1831. *See, e.g.*, John Mangels, *Clinic Case is First Use of New Law,* CLEV. PLAIN DEALER, July 30, 2001, at A1, *available at* 2001 WLNR 250929.

173. Economic Espionage Act of 1996, 142 CONG. REC. S12201, S12214 (daily ed. Oct. 2, 1996) (letter from Attorney General Reno).

174. *Id.*

declared that violations of the requirement "are appropriately sanctionable and will be reported by the Attorney General to the Senate and House Judiciary Committees."[175]

The original approval requirement implemented encompassed prosecutions under both § 1831 and § 1832.[176] That requirement expired on October 11, 2001, but it was restored by then-Attorney General Ashcroft.[177] In March of 2002, Ashcroft issued a memorandum in which he "revive[d] the prior approval requirement for initiating prosecutions under § 1831 . . . ."[178] Under the revived policy, such prosecutions must be approved by the Assistant Attorney General for the Criminal Division of the Department of Justice.[179] Ashcroft chose not to revive the approval requirement for prosecutions under § 1832, but he "strongly urge[d]" prosecutors to consult with the Department of Justice's Computer Crime and Intellectual Property Section "regarding § 1832 prosecutions prior to filing charges." [180] Since Ashcroft's memorandum did not set an expiration date for the approval requirement, it remains in effect.[181]

Since the Economic Espionage Act was first passed in 1996, the Department of Justice has prosecuted forty-seven people in thirty-four cases.[182] The Department filed its first prosecution under § 1831 in May of 2001, shortly before the original approval requirement expired.[183] After that requirement expired,

---

175. 28 C.F.R. § 0.64-5 (2000).

176. *See id.*; *see also supra* subpart III.A.2.

177. *See* Ashcroft Approval Requirement Memo, *supra* note 172.

178. *Id.*

179. *See id.*

180. *Id.*

181. *See* U.S. DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-90.020(A), http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/90mcrm.htm#9-90.020.

182. Paul Elias, *Espionage Act Proves Difficult to Prosecute,* SAN DIEGO UNION-TRIBUNE, Aug. 5, 2002, at A4, *available at* 2002 WLNR 11191024. For a detailed statistical review of the few prosecutions brought under the EEA, see Michael L. Rustad, *The Trouble with the Economic Espionage Act: Straining Out Gnats, Swallowing Camels,* 22 SANTA CLARA COMPUTER & HIGH-TECH L.J. (forthcoming 2006).

183. *See, e.g.*, Mangels, *supra* note 172; s*ee also* Press Release, U.S. Dep't of Justice, First Foreign Economic Espionage Indictment (May 8, 2001), http://www.usdoj.gov/criminal/cybercrime/Okamoto_SerizawaIndict.htm. Foreign nationals are also prosecuted under 18 U.S.C. § 1832. *See, e.g.*, *Hsu*, 155 F.3d 189.

the Department began bringing more cases,[184] but the number of EEA prosecutions is small compared to prosecutions for other intellectual property violations.[185]

There are several reasons for the relative paucity of EEA prosecutions. One is that the statute was new in 1996, and it took a while for prosecutors and investigators to learn how to apply the new law.[186] That, of course, was a transient phenomenon which cannot account for the relative scarcity of prosecutions almost a decade after the EEA was enacted.

A factor of continuing importance is the complexity of the cases. As one reporter noted, EEA cases are "thick with scientific jargon and processes that take time for prosecutors . . . to sift through."[187] EEA cases tend to involve complex, novel technologies that are case-specific. This, aside from anything else, differentiates them from other intellectual property cases, such as prosecutions for file sharing and copyright piracy.

Another factor is the Department of Justice's desire only to bring cases it can win.[188] In renewing the approval requirement

---

184. *See, e.g.*, Robin J. Effron, Note, *Secrets and Spies: Extraterritorial Application of the Economic Espionage Act and the Trips Agreement,* 78 N.Y.U. L. REV. 1475, 1491 (2003). According to one source, the Department of Justice had brought a total of forty EEA prosecutions by February 2003. *See* U.S. DEP'T OF JUSTICE, REPORTED CRIMINAL ARRESTS AND CONVICTIONS UNDER THE ECONOMIC ESPIONAGE ACT OF 1996, http://my.execpc.com/~mhallign/indict.html (last visited Jan. 31, 2006)([hereinafter REPORTED CRIMINAL ARRESTS]. The Department of Justice's website lists twenty-seven prosecutions for the period 2000–2004. *See* COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, ECONOMIC ESPIONAGE ACT (EEA) CASES, http://www.usdoj.gov/criminal/cybercrime/eeapub.htm (last visited Jan. 31, 2006).

185. *Compare* REPORTED CRIMINAL ARRESTS, *supra* note 184*, with* U.S. DEP'T OF JUSTICE, INTELLECTUAL PROPERTY CASES, http://www.cybercrime.gov/ipcases.htm (last visited Jan. 31, 2006). Writing in 2001, a reporter noted that "[b]y 2000, the FBI had more than 800 ongoing economic espionage investigations. But fewer than 25 of the probes had resulted in criminal charges." Mangels, *supra* note 172. As of 2002, ninety-two EEA cases had been referred for prosecution. BUREAU OF JUSTICE STATISTICS, INTELLECTUAL PROPERTY THEFT 2002, U.S. DEP'T OF JUSTICE 3 (2004), http://www.ojp.usdoj.gov/bjs/pub/pdf/ipt02.pdf [hereinafter INTELLECTUAL PROPERTY THEFT]. Compare this with the 210 referrals for copyright offenses and the 103 referrals for trademark crimes during the same period. *See id.* Copyright and trademark cases were more likely actually to be prosecuted. *See id* at 4.

186. *See, e.g.*, Mangels, *supra* note 172.

187. *Id*.

188. *See* Ashcroft Approval Requirement Memo, *supra* note 172.

for § 1831 prosecutions, Attorney General Ashcroft noted that an "indication of the measured and thorough approach the Department [of Justice] has taken with respect to investigating and charging theft of trade secrets [was the fact that] there has not been an acquittal under the EEA since passage of the legislation."[189] That is no longer true; in 2002, for example, the conviction rate in economic espionage prosecutions was seventy-five percent.[190]

A factor specific to § 1831 prosecutions, which accounts for the fact that they are quite rare, is the diplomatic repercussions of bringing forth such a claim.[191] It is this concern that prompted Attorney General Ashcroft's retaining the approval requirement for these prosecutions. As a reporter covering the first § 1831 prosecution noted, such a "case is potential diplomatic dynamite"[192] because it necessarily involves allegations that a foreign government was involved in the misappropriation of trade secrets.[193] While § 1832 prosecutions target a type of traditional, individual crime, a § 1831 prosecution alleges the commission of state-sponsored crime.[194] The implications of

---

189. *Id.*

190. *See* INTELLECTUAL PROPERTY THEFT, *supra* note 185, at 5. The conviction rate for copyright cases was ninety-five percent, and eighty-five percent for trademark cases. *See id.*

191. *See, e.g.*, REPORTED CRIMINAL ARRESTS, *supra* note 184.

192. Mangels, *supra* note 172.

193. *See supra* subpart III.A.2 (discussing the §1831 offense).

194. The term "state-sponsored crime" denotes crimes the commission of which is carried out by, or with the acquiescence of, a sovereign state. *See, e.g.*, Barbara M. Yarnold, *Doctrinal Basis for the International Criminalization Process,* 8 TEMP. INT'L & COMP. L.J. 85, 109 (1994).

> The first category of "state crimes" are crimes that involve state-sponsorship. This type of crime cannot be perpetrated without such sponsorship. The second category includes crimes that are conducted with state acquiescence. In other words, the criminal condition can only exist due to the implicit acceptance of the crime by the state in which it is perpetrated. The third category of state crimes includes those crimes that are committed by public officials on behalf of the state or with explicit state authorization. Finally, the fourth category includes those crimes that can only be conducted by states or that have only been conducted by states in the past.

Id. While the phrase "state-sponsored crime" usually refers to internal crime, i.e., crimes a state commits against its own citizens, it can also refer to external crime, i.e., State A's involvement in crimes committed against citizens of State B. *See, e.g.*, Raquel Aldana-

lodging such a claim have led the Department of Justice to be particularly cautious in bringing cases for economic espionage.[195]

A final, more general factor also contributes to the relative paucity of EEA prosecutions: the "inherent tension between the statute and defendants' constitutional protections."[196] In one of the first EEA prosecutions,[197] the Department of Justice sought a comprehensive protective order that would severely limit the defense's access to documents concerning the trade secrets which the defendants allegedly sought to obtain.[198] In support of its motion, the government argued:

> First . . . it has a legitimate interest in protecting the integrity and confidentiality of trade secrets . . . . Second, it contends that in the absence of *in camera* review and redaction, the defendants will receive information that is irrelevant and immaterial to their defense . . . . Third, the Government raises the specter of "graymail," which occurs when defendants press for the release of sensitive information and then threaten publicly to disclose the information in an attempt to force the Government to drop its charges . . . .[199]

Pindell, *In Vindication of Justiciable Victims' Rights to Truth and Justice for State-Sponsored Crimes,* 35 VAND. J. TRANSNAT'L L. 1399, 1408 (2002). For more on this, *see infra* Part IV.

195. *See, e.g.*, Mangels, *supra* note 172.

196. United States v. Hsu, 982 F. Supp. 1022, 1025 (E.D. Pa. 1997), *rev'd on other grounds*, 155 F.3d 189 (3d Cir. 1998).

197. The case was brought under § 1832 even though the defendants were foreign nationals. *See Hsu*, 155 F.3d at 193.

198. *See Hsu*, 982 F. Supp. at 1023.

199. *Id.* One of the reasons the Department of Justice raised the "graymail" issue was its concern that a protective order might be of little use. *See id.* at 1026 ("The Government can . . . be forgiven for not reposing much trust in defendants who it contends are linked to wrongdoers far removed from the borders of our contempt power."). According to one source, the tactic could have worked: "After the district court denied the government's proposed protective order, Assistant United States Attorney Richard Goldberg announced that if the court's ruling were upheld, he would take further steps to prevent the trade secrets from being revealed, possibly even dismissing the case." Susan V. Metcalfe, Comment, *Protecting Trade Secrets: Is the Remedy Worse than the Wrong?*, 104 DICK. L. REV. 503, 518 (2000) (citing Frances A. McMorris, *Corporate-Spy Case Rebounds on Bristol*, WALL. ST. J., Feb. 2, 1998, at B5). This has led some commentators to question the EEA's effectiveness, especially in a prosecution for substantive crimes. *See, e.g.,* Dennis J. Kelly & Paul R. Mastrocola, *The Economic*

The defendants claimed that only a less restrictive protective order would permit them to prepare an effective defense.[200] In granting the defense's request, the district court noted the tension between the requirements of the EEA and certain constitutional provisions:

> [I]f . . . we deny to the defendants complete access to the . . . technology, we inhibit their constitutional right to effective cross-examination as well as their right to have a jury . . . determine whether a "trade secret" exists . . . . [I]f we grant the defendants complete access to the . . . technology, we impair the very purpose of the EEA. When faced with such a choice, . . . "the constitution . . . must govern."
>
> Therefore, while we recognize that the . . . technology documents require some measure of protection, we cannot give them a perfect shield without violating the defendants' . . . rights under the Fifth and Sixth Amendments.[201]

The government appealed to the Third Circuit, which avoided this issue by finding that the defendants were charged only with inchoate crimes: attempt and conspiracy to violate § 1832.[202] The Third Circuit held that since impossibility is not a defense to either an attempt or conspiracy charge under the

---

Espionage Act of 1996, 26 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 181, 190 (2000):

> [T]he requirement to prove the existence of a trade secret under the EEA and the attendant possibility of "graymail" raises a serious issue concerning the feasibility and efficacy of EEA prosecutions. If a victim company ultimately is going to be forced to disclose its trade secrets, it may be disinclined to refer a trade secret theft to the government or to cooperate with the prosecution if the government initiates an EEA case by means of other sources. . . . [R]estrictions imposed by the court on the use and disclosure of the trade secret information by the defendants may mitigate this problem somewhat, but certainly not to the extent a defendant actually goes to trial.

Id. *See also* Chris Carr, Jack Morton & Jerry Furniss, *The Economic Espionage Act: Bear Trap or Mousetrap?*, 8 TEX. INTELL. PROP. L.J. 159, 189–90 (2000).

200. *See Hsu*, 982 F. Supp. at 1023.

201. *Id.* at 1025 (citing Marbury v. Madison 1 Cranch 137, 5 U.S. 137, 178, 2 L.Ed. 60 (1803)).

202. *See Hsu*, 155 F.3d at 198–99 n. 15; s*ee also supra* subpart III.A.2 (discussing attempt and conspiracy).

EEA,[203] the defendants had no constitutional right of access to documents that would indicate whether they had, in fact, sought to purchase a trade secret.[204]

So far, no reported cases address the issue left unaddressed by the Third Circuit, that is, the extent to which a court can shield proprietary information in a prosecution for commission of a substantive EEA offense.[205] Commentators generally conclude that the *Hsu* district court was correct—that there is a fundamental, unresolvable tension between a defendant's constitutional right to discovery in a substantive prosecution under the EEA and the provisions of 18 U.S.C. § 1835.[206] Many believe this creates a continuing disincentive for companies to report being the victims of economic espionage, a disincentive which erodes the efficacy of the EEA.[207]

Even if we were to assume, for purposes of analysis, that the *Hsu* district court and the commentators are wrong and a court can protect trade secret information implicated in an EEA prosecution, there are other factors that can discourage companies from reporting EEA crimes. For example, publicly announcing that a trade secret has been compromised can negatively affect a company's stock value. A 2001 empirical analysis of the twenty-three EEA prosecutions that had been brought to that point found that "public disclosures of trade secret theft are on average associated with a negative stock market response that is *both* statistically and economically

---

203. *See supra* subpart III.A.2 (discussing attempt and conspiracy).

204. *See Hsu*, 155 F.3d at 201.

205. It is settled that an essential element of a substantive prosecution is the defendant's appropriating an actual trade secret. *See, e.g.*, United States v. Lange, 312 F.3d 263, 264–65 (7th Cir. 2002).

206. *See supra* note 196; s*ee also supra* note 133 and accompanying text. Section 1835 was included in the EEA to preserve the confidentiality of trade secret information implicated in an EEA prosecution. *See, e.g.*, Economic Espionage Act of 1996, H.R. REP. NO. 104-788, at 14 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4033. Congress recognized that "[w]ithout such a provision, owners may be reluctant to cooperate in prosecutions for fear of further exposing their trade secrets to public view, thus further devaluing or even destroying their worth." *Id.* at 13.

207. *See supra* note 199; s*ee also* ONCIX 2004 REPORT, *supra* note 10, at 10.

significant."[208] The study concluded the following:

> enough of a track record [exists] to formulate a tentative progress report regarding the Act. . . . [O]ne of the fears surrounding the passage of the EEA was that publicly traded companies might be hesitant to report the theft of their trade secrets to the government for fear that doing so might adversely affect their stock prices. At least at this point, our findings suggest that this concern has merit, i.e., the stock market and investors care.[209]

They also noted that their findings "raise the important practical question of why an agency should divert and allocate scarce budget resources toward a law enforcement mechanism that victims may have little incentive to use."[210]

A related issue is the likelihood of effective prosecution. "[P]rior to the passage of the EEA, the prevailing wisdom was that existing . . . laws, not to mention the extraterritoriality and enforcement issues, made it virtually impossible to effectively prosecute foreign economic espionage."[211] The EEA addressed these issues by adding new crimes to the federal criminal code and by authorizing extraterritorial jurisdiction over EEA violations.[212] Unfortunately, the EEA did not, and indeed could not, resolve all of the problems that arise in pursuing foreign nationals who misappropriate U.S. trade secrets. Perhaps the most difficult issue is extradition. As noted earlier, economic espionage is by definition state-sponsored crime in that trade secrets are stolen at the behest of a foreign sovereign.[213] Those responsible for such thefts are therefore likely to be foreign nationals who are not in the United States when they are charged with violating the EEA, either because they left the country after committing a traditional act of economic espionage

208. Carr & Gorman, *supra* note 23, at 50 (emphasis in the original).

209. *Id.* at 51–52. The Annual Report submitted to Congress for 2004 reached a similar conclusion. *See* ONCIX 2004 REPORT, *supra* note 10, at x ("US firms have . . . been reluctant to raise alarms about possible technology theft out of concern for the potential impact on investor and consumer confidence and stock prices.").

210. Carr & Gorman, *supra* note 23, at 52.

211. *Id.* at 28 (citing Carr, Morton & Furniss, *supra* note 199, at 168–70).

212. *See supra* subpart III.A.2.

213. *See supra* subpart III.A.2 (discussing the § 1831 offense).

or because they committed the crime remotely, via cyberspace.[214] In either event, the Department of Justice cannot proceed with prosecution unless and until it is able to extradite the offender from the country that is harboring him.[215]

An EEA case involving two "firsts" suggests extradition will not be forthcoming in these cases. In the first prosecution under 18 U.S.C. § 1831,[216] Japan refused to extradite one of the defendants, a Japanese scientist accused of stealing genetic materials from the Cleveland Clinic Foundation to benefit RIKEN, the Institute of Physical and Chemical Research funded by the Japanese government.[217] The Japanese court charged with deciding whether the scientist would be extradited found that there was no probable cause to believe he had acted with the intent to benefit RIKEN, "his new employer."[218] It was "the first time in the 24-year history of the Japan-U.S. extradition treaty that Japan has refused to extradite a fugitive."[219] Since there is no appeal from the Japanese court's decision, the denial effectively ended the prosecution.[220] The result in this case seems to be anything but an aberration.[221]

The individual and combined effect of the systemic factors discussed above is to erode the EEA's effectiveness as a weapon against economic espionage. It is a solution in promise, but not in fact. The next subpart examines contextual factors that further undermine the EEA's utility as a means of discouraging economic espionage.

---

214. *See supra* subpart II.B.

215. *See, e.g.*, Morimoto, *supra* note 60, at 288.

216. *See supra* subpart III.B.1.

217. *See, e.g.*, Morimoto, *supra* note 60; *see also* Mangels, *supra* note 172.

218. Morimoto, *supra* note 60.

219. *Id.*

220. *See id.*

221. *See, e.g.*, Srodes, *supra* note 168, at 12 ("[S]ix years [after enactment of the EEA], there have only been a few dozen indictments and prosecutions and many of the accused have high-tailed it back to their home countries where their governments refuse to extradite them.").

2. Context

In adopting the EEA, Congress chose to approach economic espionage as a type of crime, to be investigated and prosecuted using the methods we use for other, more traditional types of crime.[222] What Congress did not anticipate was that the EEA came into existence at a time when crime, in all its guises, was about to undergo a radical transformation—one that has significant consequences for our ability to combat it effectively with traditional law enforcement strategies.[223] As the Parts below explain, crime is increasingly migrating online, into cyberspace. This shift, in the context in which criminal activity occurs, requires that we re-think how we deal with crime, including economic espionage.

Order

Crime threatens social order, and societies must maintain a baseline of internal order if they are to endure.[224] Societies use

---

222. *See, e.g.*, Economic Espionage Act of 1996, Pub. L. No. 104-294, 1996 U.S.C.C.A.N. 4034, 4034–35 (statement by President William J. Clinton upon signing H.R. 3723).

> This legislation makes the theft or misappropriation of trade secrets a Federal crime . . . . Trade 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.
>
> Until today, Federal law has not accorded appropriate or adequate protection to trade secrets, making it difficult to prosecute thefts involving this type of information. . . .
>
> This Act will protect the trade secrets of all businesses operating in the United States . . . from economic espionage and trade secret theft and deter and punish those who would intrude into, damage, or steal from computer networks. I am pleased to sign it into law.

Id.

223. *See, e.g.*, Susan W. Brenner, *Toward A Criminal Law for Cyberspace: Distributed Security,* 10 B.U. J. SCI. & TECH. L. 2, 6–11 (2004) [hereinafter Brenner, *Toward A Criminal Law for Cyberspace*].

224. *Id*. at 8–10.

rules to maintain order.[225] "A rule is a compulsory principle that governs action and inaction; [it] specifies which actions are allowable and which are not."[226] Societies use two types of rules to maintain order: constitutive and proscriptive (criminal).[227] Civil constitutive rules define the structure of a society by defining relationships among those who comprise that society; they also allocate essential tasks among the members of the society and ensure that the tasks are performed.[228]

Historically, societies have been bounded systems situated in a delimited spatial area and composed of a defined populace (for example, "the people of Rome"). These constraints facilitate the operation of the constitutive rules. Spatial and demographic isolation make it easier to socialize members of a society so that most members accept and abide by its constitutive rules; they also make it easier to identify and suppress those who do not.[229]

Because societies are composed of intelligent entities who can ignore rules, they cannot rely only on constitutive rules to maintain order.[230] Societies, therefore, implement a second set of rules—"criminal rules"—which target rule-violators.[231] These rules impose criminal (proscriptive) liability and sanctions upon those who do not abide by constitutive rules.[232] Societies assume that sanctioning rule-violators maintains order by preventing violations. This basic assumption incorporates two subordinate assumptions: (i) sanctions deter violations by presenting us with a simple choice—obey rules or suffer the consequences, and (ii) rule-violators will be identified, apprehended, and sanctioned.[233]

For purposes of analysis, we will assume the validity of the first assumption, as our concern is with the second assumption. Under the second assumption, if criminal rules are to maintain

---

225. *Id*.

226. *Id*. at 6.

227. *Id*. at 21, 34.

228. *Id.* at 17–18, 36–40.

229. *See id.* at 49–52, 58–60.

230. *Id.* at 39–41.

231. *See id.* at 41–42.

232. *Id.* at 43.

233. *See* PRESIDENT'S COMM'N ON LAW ENFORCEMENT AND ADMIN. OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 7 (1967).

order, there must be a system in place that ensures rule-violators are identified, apprehended, and sanctioned. There must be a credible threat of retaliation for violating criminal rules; absent such a threat, they cannot discourage deviance and maintain order. For most of human history, societies relied upon citizens to maintain this threat.[234] That began to change in 1829 when Sir Robert Peel created the London Metropolitan Police.[235] The Metropolitan Police was something new: an independent agency staffed by full-time professionals whose sole task was to maintain order by reacting to crimes and apprehending the perpetrators.[236] Peel's model spread around the world, the consequence being that in the twenty-first century, we, as citizens, assume no responsibility for maintaining order.[237] That is the sole province of professionalized police forces that ensure order by reacting to completed crimes.[238]

Real-World Crime

Because real-world crime occurs in a physical environment, it has four characteristics that are relevant to this discussion: proximity, scale, physical constraints, and patterns.[239] Perhaps the most fundamental characteristic of real-world crime is that the perpetrator and victim are physically proximate to each other when the offense is committed or attempted. For instance, it is not possible to rape or realistically attempt to rape someone if the rapist and the victim are fifty miles apart. In a nontechnological world, it is physically impossible to pick someone's pocket, rob them, or defraud them out of their

234. *See id.* at 59–65.

235. *See* David A. Sklansky, *The Private Police*, 46 UCLA L. Rev. 1165, 1202–1203 (1998–1999).

236. *Id*. at 1202–04.

237. *See, e.g.*, William D. Eggers & John O'Leary, *The Beat Generation: Community Policing at Its Best*, 74 POL'Y REV. 1 (1995), *available at* http://www.policyreview.org/fall95/thegg.html.

238. *See, e.g.*, DAVID GARLAND, THE CULTURE OF CONTROL: CRIME AND SOCIAL ORDER IN CONTEMPORARY SOCIETY 34 (2001) (assuming crime control "must be a specialist, professional task of •law enforcement'").

239. The analysis in this subpart is taken from Brenner, *Toward a Criminal Law for Cyberspace, supra* note 223, at 49–57.

property if the thief and victim are in different cities, states or countries.

The scale of real-world crime is limited: It tends to be one-to-one crime, involving one perpetrator and one victim. The crime begins with the victimization of the target and ends when the victimization is concluded. During the event, the perpetrator focuses all of her attention on consummating that crime; when it is complete, she can move onto another crime and another victim. Like proximity, the one-to-one character of real-world crime derives from the constraints physical reality imposes upon human activity: A thief cannot pick more than one pocket at a time; a forger cannot forge more than one document at a time; and prior to the rise of firearms. It was very difficult for one to cause the simultaneous deaths of more than one person. Real-world crime, therefore, tends to be serial crime.

Real-world crime is also subject to the physical constraints that govern activity in the physical world. Every crime, even street-level drug dealing or prostitution, requires a level of preparation, planning, and implementation if it is to succeed. A bank robber must visit the bank to familiarize herself with its layout, security, and routine; this exposes her to public scrutiny and that can lead to her being identified and apprehended. While in the bank, she leaves trace evidence and is subject to observations that can result in her being identified. As she flees after committing the robbery, she is again exposed to public view and risks being identified. In addition to these obvious risks, she probably had to secure a weapon and a disguise before the robbery and needed help disposing of the cash afterward. Each step takes time and effort, which incrementally augments the exertion required to commit the crime and increases the risks involved in its commission.

Finally, over time it becomes possible to identify the general contours and incidence of the real-world crimes committed in a society. Victimization tends to fall into demographic and geographic patterns for two reasons. First, only a small segment of a functioning society's populace will persistently engage in criminal activity. Those who fall into this category are apt to be from economically deprived backgrounds and reside in areas that share geographic and demographic characteristics. They

will be inclined to focus their efforts on those with whom they share a level of physical proximity because they are convenient victims; consequently, much of a society's routine crime will be concentrated in identifiable areas. Second, each society has a repertoire of crimes—rules that proscribe behaviors ranging from more to less serious in terms of the harm each inflicts. Theft causes a loss of property; murder causes a loss of life, and so on. In a society that is successfully maintaining internal order, the more egregious crimes will occur much less often and less predictably than minor crimes.

These characteristics shaped the crime-control strategy incorporated in the current model of law enforcement. Proximity contributed a presumed dynamic: victim-perpetrator proximity and consequent victimization; perpetrator efforts to flee the crime scene and otherwise evade apprehension; investigation; identification; and apprehension of the perpetrator. The dynamic reflects a time when crime was parochial, when victims and perpetrators tended to live in the same village or neighborhood. If a victim and perpetrator did not know each other, they were likely to share community ties that facilitated identification and apprehension. Thus, there was a good chance a perpetrator could be identified by witnesses or reputation. If a perpetrator and a victim did not share community ties, he would "stand out" as someone who did not belong, which would likely contribute to his being apprehended. Law enforcement dealt effectively with this type of crime because its spatial limitations mean investigations were limited in scope. The strategy still assumes that the investigation of a crime should focus on the physical scene of the crime.

The crime-control strategy assumes one-to-one victimization that, along with another assumption, yields the proposition that the scale of crime will be limited in a functioning society. The other assumption is that crimes are extraordinary events—that law-abiding conduct is the norm and crime is unusual. This second assumption derives not from the physical characteristics of real-world crime, but from the need to maintain order. A society's constitutive and proscriptive rules work together to achieve this; the constitutive rules define the acceptable behaviors that are encouraged, while the proscriptive rules

emphasize that certain behaviors will not be tolerated. Individuals are socialized to accept the constitutive rules as prescribing the correct standards of behavior. Proscriptive rules reinforce this by emphasizing that the behaviors they condemn are not only bad, but they are unusual, extraordinary, and outside the norm. The combined effect of these rules is that crime becomes a subset, generally a small subset, of the total behaviors in a society. The limited incidence of criminal behavior, coupled with one-to-one victimization as the default crime mode, means law enforcement personnel can focus their efforts on a limited segment of the conduct within a given society.

The crime-control strategy also incorporates the concept that crime falls into patterns, and that it will be limited in incidence and in the types of harms it inflicts. It also assumes that an identifiable percentage of crime will occur in geographically and demographically demarcated areas. The combined effects of localized crime and the differential frequency with which various crimes are committed gives law enforcement the ability to concentrate its resources in areas where crime is most likely to occur, which enhances its ability to react to completed crimes.

Online Crime

Online crime, or cybercrime, is illegal activity that involves the use of computer technology.[240] Unlike real-world crime, cybercrime does not require any degree of physical proximity between victim and perpetrator for the consummation of an offense.[241] The victim and perpetrator can be in different cities, states or countries; all a cybercriminal needs is a computer linked to the Internet.

Furthermore, one-to-one victimization is not typical of cybercrime: Unlike real-world crime, online crime can be automated, which means perpetrators can commit thousands of

240. *See* Susan W. Brenner, *Is There Such a Thing As Virtual Crime?*, 4 CAL. CRIM. L. REV.1, ¶ 3 (2001), *available at* http://boalt.org/CCLR/v4/v4brenner.htm [hereinafter Brenner, *Is There Such a Thing As Virtual Crime?*].

241. The analysis in this subpart is also taken from Brenner, *Toward a Criminal Law for Cyberspace, supra* note 223, at 65–74.

crimes quickly and with little effort. One-to-many victimization is the default assumption for cybercrime. Under the strategy outlined in subpart III.B.2 (Real-World Crime), officers react to a crime by investigating and apprehending its perpetrator; the strategy assumes crime is committed on a limited scale so officers can react to discrete crimes. Cybercrime violates this assumption in two ways. First, although cybercrime is carried out by a small percentage of the population, this relatively small group can commit crimes on a scale far surpassing what they could achieve in the real-world. The total number of cybercrimes will therefore exponentially exceed real-world crimes. Second, cybercrime is added to the real-world crime with which law enforcement must continue to deal; people will still rape, rob, and murder in the real-world. These factors combine to create an overload in that law enforcement's ability to react to cybercrime erodes because the resources that were minimally adequate to deal with real-world crime are totally inadequate to deal with cybercrime-plus-real-world-crime.

Cybercriminals also avoid the physical constraints that govern real-world crime; funds can be extracted from a U.S. bank and moved into offshore accounts with little effort and less visibility. The reactive strategy is far less effective against online crime because the reaction usually begins well after the crime has been successfully concluded and the trail is cold. Another problem is that since most or all of the conduct involved in committing the crime occurs in an electronic environment, the physical evidence, if any, is evanescent and volatile. By the time police react, evidence may have been destroyed, advertently or inadvertently. Since perpetrators are seldom present at the crime scene, assumptions about their having been observed while preparing for, committing or fleeing from the crime no longer hold. Indeed, officers may not be able to determine from where the perpetrator carried out the crime or who he is; cybercriminals, unlike their real-world counterparts, can enjoy perfect anonymity or perfect pseudonymity. Even if officers can identify the perpetrator of a cybercrime, gathering evidence and apprehending him can be difficult. The country that hosts him may not regard what he did as illegal and may therefore decline to extradite him, or there may be no extradition treaty in place that governs the conduct at issue.

Finally, we cannot, at least as of yet, identify offender-offense patterns comparable to those we have for real-world crime. Several factors account for this. First, cybercrime is not well documented. Even if agencies track cybercrimes, they tend not to break them out into separate categories. Cyberfraud, for example, is usually listed as fraud. Second, it can be difficult to parse cybercrime into discrete offenses: Is a virus that causes billions of dollars of damage in many countries one crime, several crimes or thousands of crimes? The most important factor, though, is the lack of accurate statistics. Cybercrimes are often not detected, and if they are detected, many cybercrimes are not reported to the authorities.

Online Economic Espionage

What is true of generic cybercrime is also increasingly true of economic espionage. As subpart II.B explained, economic espionage is increasingly moving online:

> Only a few years ago, stealing customer information was a cumbersome task. One example is Jose Lopez, the former executive at General Motors, who was indicted by a federal grand jury in Detroit for allegedly stealing boxes of confidential and proprietary information in 1993 from General Motors and transferring them to his new job at Volkswagen. Today, there is . . . no need to steal boxes of paper documents. The information . . . is . . . stored on computers. Such information can be instantly sent anywhere in the world via the Internet.[242]

As economic espionage moves online, it takes on the characteristics of cybercrime and becomes ever-more resistant to traditional law enforcement efforts.[243]

Economic espionage's resistance to law enforcement efforts is further exacerbated by a contextual characteristic it does not share with other types of cybercrime: Economic espionage is state-sponsored crime.[244] In contrast, our current model of law

---

242. Carr & Gorman, *supra* note 23, at 31 (notes omitted) (citing Christian Tyler, *The Enemy Within*, FIN. TIMES (London), Apr. 12, 1997, at 1).

243. *See supra* Parts II.B, III.B.2 (discussing online crime).

244. *See supra* note 192 and accompanying text.

enforcement assumes crime is the local product of individual effort. This assumption derives from the physical constraints that govern real-world crime; as explained above, these constraints become irrelevant when crime, including economic espionage, moves online.[245]

The assumption that crime is the product of individual effort also derives from the strictures of the real-world. For millennia, human groups used physical boundaries—territory—to insulate themselves from threats posed by other human groups.[246] With the rise of nation-states, the concept of territory became fixed; each nation-state occupied a specific, defined territory and assumed the responsibility to protect its citizens from internal threats (crime) and external threats (war).[247] The two categories remained discrete until relatively recently, when technology began to make physical boundaries irrelevant and to blur the distinction between crime and war.[248] Economic espionage is often characterized as a type of warfare;[249] while it does not involve a physical attack upon a nation-state's territory,[250] it does represent an attack by one sovereign upon the essential interests of another.[251]

Economic espionage is at once "crime" and "not-crime." Like crime, it inflicts various types of harm upon members of a society. Thus, like online theft, economic espionage harms citizens by diminishing the value of assets they have acquired

---

245. *See supra* subpart III.B.2 (discussing real-world crime).

246. *See* Brenner, *Toward a Criminal Law for Cyberspace, supra* note 223, at 106–09.

247. *Id.*

248. *See, e.g.*, John Arquilla & David Ronfeldt, *The Advent of Netwar (Revisited), in* NETWORKS AND NETWARS: THE FUTURE OF TERROR, CRIME AND MILITANCY 1–22 (John Arquilla & David Ronfeldt, eds., 2001).

249. *See, e.g.*, FIALKA, *supra* note 34, at 90. *See also* Robert Loring Allen & Erwin D. Canham, SOVIET ECONOMIC WARFARE 28 (1960) ("Economic warfare is defined as the conscious attempt to increase the relative economic, military, and political position of a country through foreign economic relations.").

250. DAVID M. ACKERMAN, RESPONSE TO TERRORISM: LEGAL ASPECTS OF THE USE OF MILITARY FORCE, Congressional Research Service CRS-1 (Sept. 13, 2001), http://fpc.state.gov/documents/organization/6217.pdf (defining "war" as the use or threatened use of force by one nation-state against another).

251. *See supra* Part II.

through legitimate means.[252] However, unlike a conventional criminal, the perpetrator of economic espionage does not act solely for personal gain. Economic espionage is analogous to warfare because at the very least, it represents an attempt to undermine the security and stability of a sovereign nation.[253] This aspect of economic espionage differentiates it from other types of crime in ways that alter the context in which law enforcement has traditionally operated.[254]

As noted above, economic espionage, like cybercrime, increasingly violates the assumption that crime is local. The perpetrators of economic espionage are often foreign nationals who either leave the victim-state after misappropriating trade secrets or consummate the act remotely, via cyberspace.[255] They

---

252. *See* Brenner, *Is There Such a Thing as Virtual Crime?*, *supra* note 240, ¶ 32–49.

253. *See* Michelle Van Cleave, Nat'l Counterintelligence Executive, Remarks at the Conference on Counterintelligence for the 21st Century: The National Counterintelligence Strategy of the U.S. 5–6 (Mar. 4–5, 2005), http://www.nacic.gov/publications/reportsspeeches/speeches/CI21Conf/TexasspeechCI.pdf.

> America's national defense rests on its continuing technological superiority . . . .
>
> Espionage has long proven the most cost-effective means of defeating U.S. capabilities. We may spend billions of dollars to develop a given weapons system, the effectiveness of which rests on . . . technological . . . secrets that give us advantage. If those essential secrets are stolen, both our investments and our advantage can be lost.

Id. at 5–6.

254. Though economic espionage is, in certain senses, analogous to an act of war, it is unlikely that countries will treat it as an act of warfare. So far, it is the act of one or more individuals, rather than the use of military force by another sovereign. *See* ACKERMAN, *supra* note 250. We are accustomed to approaching acts of espionage, including economic espionage's more sinister counterparts, as crimes. *See, e.g.*, Henry Mark Holzer, *Why Not Call It Treason?: From Korea to Agfhanistan,* 29 S.U.L. Rev. 181, 182–85 (2002).

255. *See supra* note 211 and accompanying text; ONCIX 2004 REPORT, *supra* note 10, at 1 ("Increasingly, foreign entities need not even come to the United States to acquire sensitive technology but, instead, can work within their own borders."); *see, e.g.*, *Industrial Spy Arrested in London Probably Worked from Germany,* BBC INT'L REPORTS (Europe), May 31, 2005.

> A suspected industrial spy, who was arrested in London last week, probably worked from Baden-Wuerttemberg. . . . This was reported by the Federal State Office of Criminal Investigations (LKA) in Stuttgart . . . . The 41-year old computer expert was reportedly the mastermind of a group that spied on

are, therefore, not in the victim-state when its law enforcement officials seek to react to an economic espionage crime by arresting, prosecuting and sanctioning those responsible.

Nation-states long ago evolved processes for ensuring that those who flee a jurisdiction after committing conventional crimes can be returned to face justice. For centuries, countries have used the process of extradition to return fleeing criminals to the jurisdiction in which they committed their crimes.[256] Bilateral treaties are the means used to implement extradition; each party to the treaty agrees to extradite those whom the state requesting extradition has charged with or convicted of an extraditable offense.[257] Extraditable offenses can be specifically defined in the treaty or, more often, the treaty will encompass crimes that are punishable by the laws of both parties with a specific degree of severity.[258] The nation-state seeking extradition submits a request, with supporting documents, to the country harboring the fugitive. If that country grants the request, it arranges for the fugitive to be surrendered to the country seeking extradition.[259]

While it is cumbersome,[260] this process works reasonably well for conventional crimes because the conduct involved in these crimes threatens the stability of all states.[261] As long as a state is assured that certain procedural requirements are met, it will cooperate in seeing that one who fled justice in another state is returned for prosecution and/or incarceration.

This process is unlikely to work for economic espionage. The

---

internal information of industrial companies via the Internet.

See id.; see also CY4OR: Tackling the Tactics of Cyber Spies, M2 PRESSWIRE, Sept. 7, 2004.

256. Monica L. McHam, Comment, *All's Well That Ends Well: A Pragmatic Look at International Criminal Extradition*, 20 HOUS. J. INT'L L. 419, 430–31 (1997-1998).

257. *Id*. at 31; *see, e.g.,* Extradition Treaty with Lithuania, U.S.-Lith. Oct. 23, 2001, S. TREATY DOC. No. 107-4 (2001).

258. *See*, *e.g., id.* art. 2(1).

259. *See*, *e.g., id.* arts. 8, 12(3).

260. *See*, *e.g.*, Thomas G. Snow, *The Investigation and Prosecution of White Collar Crime: International Challenges and the Legal Tools Available to Address Them,* 11 WM. & MARY BILL RTS. J. 209, 235–43 (2002) (discussing a few of the legal and political hurdles faced during the extradition process).

261. *See supra* subpart III.B.2 (discussing order and real-world crime).

conduct involved in economic espionage departs from the conventional crime model in that it does not threaten the stability of all nation-states. Economic espionage is predicated on the emerging dynamic of cross-border victimization. Cross-border victimization is common in conventional cybercrime, [262] but it takes on a unique aspect in economic espionage because the state itself is involved in the crime. Agents of State A victimize citizens of State B to confer a competitive advantage upon State A. Since the agents act to benefit State A, neither they nor their conduct pose a threat to the stability of that state or to any other state that relies upon scientific and technological advancements for competitive and tactical advantages. Most nations, therefore, do not regard economic espionage as a particularly serious matter. Even the United States "has no specific national legislation that would prohibit espionage against other nations."[263]

The effects of this laissez-faire attitude toward economic espionage are exacerbated by the unique position a requested state is in when another country, say the United States, seeks extradition or other assistance in pursuing someone charged with economic espionage. When conventional crime is involved, the state from which assistance is requested is, in essence, a neutral party. That is, while the state may have concerns about the regularity of the process, it has no stake in the dispute between the person whom it harbors and the state that seeks assistance.[264] The generic harms encompassed by conventional crimes threaten all states.[265]

The situation is very different when state-sponsored crime is involved. If the economic espionage was committed for the benefit of the state from which assistance is requested, it is no longer a neutral party; it now has a conflict of interest. Assume the United States asks State A to extradite Suspect X, whom the

---

262. *See supra* subpart III.B.2 (discussing online crime).

263. Blood, *supra* note 58, at 233.

264. When the person is a citizen of the state from which assistance is requested, that state may approach the request with special care, focusing on issues such as the penalties that can be imposed and the extent to which the person's rights will be protected in any criminal proceedings. *See e.g.*, Snow, *supra* note 260, at 235–40.

265. *See supra* subpart III.B.2 (discussing order and real-world crime).

United States has charged with economic espionage. If the espionage was undertaken to benefit State A, then State A is the beneficiary of the crime for which extradition is being sought. If State A encouraged or otherwise sponsored the crime, it is an accomplice in the commission of that crime. In either case, it is in State A's best interest to decline extradition, if only to limit publicity concerning its role in the offense. The same conclusion holds, perhaps to a lesser extent, when assistance is requested for other purposes, such as evidence-gathering.

While the EEA may be a useful approach to the domestic theft of trade secrets,[266] it is a futile attempt at dealing with economic espionage—especially online economic espionage. The next Part considers how we can improve our approach to this problem.

IV. THE FUTURE

> *We don't want to . . . discover, years and years after the fact, that while we have investigated every reported security breach, spies have stolen our secrets . . . .*[267]

The source of the EEA's futility in dealing with online economic espionage is its reliance on the reactive model of law enforcement. [268] Law enforcement's ability to react effectively to criminal activity, including economic espionage, erodes dramatically when that activity moves online. The fundamental, operational assumptions that structure the reactive model do not apply to online crime. [269] The erosive effects of this failure of assumptions are exacerbated by state involvement in economic espionage because the resulting conflicts of interest make it exceedingly unlikely that the culpable state will render assistance to a country seeking to bring the perpetrator(s) of economic espionage to justice. [270]

---

266. *See supra* subpart III.A.2 (discussing the § 1832 offense).

267. Van Cleave, *supra* note 253, at 4–5.

268. *See supra* subpart III.B.2 (discussing online crime and online economic espionage).

269. *See supra* subpart III.B.2 (discussing online crime and online economic espionage).

270. *See supra* subpart III.B.2 (discussing online economic espionage).

Logically, we have two alternatives for improving our approach to economic espionage:[271] We can improve the reactive model of law enforcement's applicability to online crime, including economic espionage, or we can implement a different approach that supplements the reactive model.

A. Improved Reaction

An obvious way to improve law enforcement's ability to react to online crime, including economic espionage, is to increase the number of officers available to react and the resources they utilize in reacting to online crime.[272] However, there are two problems with this option. First, societies already find it difficult to allocate the resources needed to support law enforcement agencies. Therefore, it is improbable that they can summon the resources needed to recruit, train and equip enough officers to make the reactive strategy a viable approach to online crime while retaining its viability for real-world crime. Second, since online crime is automated, there is no guarantee that simply increasing the number of officers will improve the efficacy with which law enforcement can react. Certain factors suggest that adding officers is unlikely to improve law enforcement reaction. Since online activity tends to be less visible, economic espionage often goes undetected.[273] Furthermore, since online activity can be automated, a perpetrator can commit serial acts of economic espionage while officers are still attempting to react to his initial effort.

---

271. For an argument as to how civil liability can be used to this end, see Rustad, *supra* note 182.

272. *See* Susan W. Brenner, *Distributed Security: Moving Away from Reactive Law Enforcement,* 9 INT'L J. COMMS. L. & POL'Y (SPECIAL ISSUE) 1, 18 (2004), *available at* http://www.digital-law.net/IJCLP/Cy_2004/pdf/Brenner_ijlcp-paper.pdf [hereinafter Brenner, *Distributed Security: Moving Away from Reactive Law Enforcement*].

273. *See, e.g.*, Van Cleave, *supra* note 253, at 6:

> The most successful espionage—the kind that goes undetected—is all the more effective, because what is not known cannot be remedied. And the risks are growing. The marvels of modern information technology and microelectronics have revolutionized espionage tradecraft, enabling the clandestine extraction of vast volumes of data in miniaturized storage media or across computer networks at the press of a "send" button.

Another option is to react differently, by striking back at those who commit online crime. Writing in a different context, Professor Reidenberg proposed that nations authorize their law enforcement officers to use "electronic sanctions" to react to online crime.[274] He argued that states could electronically sanction offenders:

> [S]tates may electronically sanction rule offenders by using technologies to penalize or destroy the offenders' online presence . . . . [A] state might launch a denial of service . . . attack. This is an online death penalty' and prevents an offender from interacting on the [I]nternet. A state may also use hacking techniques to 'seize' or paralyze rule-violating web pages . . . . [T]he state may use techniques similar to the MS Blaster worm for law enforcement purposes.[275]

What Professor Reidenberg proposed is an official version of an alternative that has been discussed for some time: civilian self-help or strikeback techniques that supplement law enforcement reactions to cybercrime.[276] However, neither the official nor the unofficial version of this alternative is an acceptable solution. Both create a new type of state-sponsored crime,[277] and the state-sanctioned use of official or private strikeback techniques could be seen as an act of warfare.[278]

A final option for improving the reactive model's efficacy against economic espionage is to implement the approach the Council of Europe has taken in its Convention on Cybercrime (Convention).[279] The Convention is based on the premise that an

---

274. *See* Joel R. Reidenberg, *States and Internet Enforcement,* 1 U. OTTAWA L. & TECH. J. 213, 228–29 (2004), *available at* http://ssrn.com/abstract=487965 (follow "Document Delivery" hyperlink).

275. *Id.* at 228 (notes omitted).

276. *See, e.g.*, Curtis E.A. Karnow, *Strike and Counterstrike: The Law on Automated Intrusions and Striking Back*, BLACKHAT WINDOWS SECURITY, Feb. 27, 2003, at 5, http://www.blackhat.com/presentations/win-usa-03/bh-win-03-karnow-notes.pdf.

277. *Id.; see* Reidenberg, *supra* note 273, at 228–29.

278. *See, e.g.*, Walter G. Sharp, *Cyberspace and the Use of Force* (1999) (on file with Author).

279. Convention on Cybercrime, Nov. 23, 2001, E.T.S. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [hereinafter Convention on Cybercrime].

international network of consistent substantive and procedural laws will improve national law enforcement's ability to react across jurisdictional borders, which will restore the effectiveness of the current crime control strategy. To that end, the Convention seeks to harmonize national laws that define various types of cybercrime, authorize mutual assistance in evidence-gathering and permit extradition of cybercriminals.[280] However, the Convention does not encompass economic espionage,[281] and it is doubtful that a comparable treaty encompassing economic espionage could be implemented given the state involvement in that activity.[282] Thus, it seems we have little hope of improving the efficacy of law enforcement reaction to economic espionage, we must consider alternative approaches.[283]

B. Prevention

There are two ways to deal with crime: react to it or prevent it. The reactive model of law enforcement discussed above incorporates prevention insofar as it is seeks to incapacitate and deter offenders; but this is not its primary concern.[284] Prevention is the primary concern of the community policing model, which emphasizes police-civilian cooperation to create a climate in which crime is not tolerated.[285] We cannot, for various reasons, apply the community policing model to online crime.[286] We can, however, use its focus on prevention to develop a more effective approach to online economic espionage.

Various sources have outlined specific techniques individuals and industry can use to prevent economic

280. *See id.* at Explanatory Report ¶¶ 1–16.

281. *See id.* arts. 2–10.

282. *See supra* subpart III.B.2 (discussing online economic espionage).

283. Even if we abandon the reactive strategy as our approach to economic espionage and other types of online crime, we will still need to retain it. It has proven an effective strategy for real-world crime, and there is no reason to believe that will change.

284. *See supra* subpart III.B.2 (discussing real-world crime).

285. *See, e.g.*, Barry N. Leighton, *Visions of Community Policing: Rhetoric and Reality in Canada*, 33 CANADIAN J. CRIMINOLOGY 485, 487 (1991) (on file with Author).

286. For one thing, the concept of a physical community does not translate into cyberspace. *See, e.g.*, Brenner, *Distributed Security: Moving Away from Reactive Law Enforcement*, *supra* note 272, at 23.

espionage.[287] This discussion is concerned not with techniques, but with how we can implement a paradigm shift, to move from relying exclusively on the reactive model as our strategy for dealing with economic espionage to a strategy based on prevention. Basically, there seem to be three possible implementation strategies.

1. Implementation Strategies

One implementation strategy is to mandate prevention by implementing rules that require businesses to protect their trade secrets and by imposing sanctions upon those that do not comply.[288] However, mandating prevention is a bad idea because, in effect, it retains the reactive model and adds another layer of enforcement that further stretches already-slim resources.[289] If a mandatory system is to be effective, someone has to police enforcement, that is, check to see if specified prevention measures have been implemented and ensure the imposition of sanctions when they are not.[290]

A second implementation strategy is to continue to do what we are already doing, that is, make prevention purely voluntary.[291] This strategy is clearly not working.

A third and potentially more promising implementation strategy is to use civil or criminal liability to create additional incentives (beyond the economic incentives that already exist and are obviously not compelling) to prevent economic espionage. This strategy is analogous to mandated prevention in that it imposes consequences for not preventing the misappropriation of trade secrets, but it differs in certain critical respects. Instead of mandating the implementation of specific preventative measures, this strategy would simply create a legal duty to prevent the misappropriation of trade secrets and would

---

287. *See, e.g.*, PRESIDENT'S INFO. TECH. ADVISORY COMM., CYBER SECURITY: A CRISIS OF PRIORITIZATION 37–48 (2005), *available at* http://www.hpcc.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

288. For an analysis of this strategy in a different context, *see* Brenner, *Toward A Criminal Law for Cyberspace, supra* note 223, at 90–94.

289. *Id*. at 92–93.

290. *Id.* at 91–93.

291. *Id.* at 89–90.

apply to a defined group, presumably those who own and/or control trade secret information. Those encompassed by the duty would be under a legal obligation to take reasonable measures to protect the trade secrets they control.

The virtue of this strategy is that it puts the risk of failure on those who are in the best position to protect trade secrets. If they fail, they are held liable, either civilly or criminally, as explained below. While this approach may seem harsh because it may seem like blaming the victim, it is in fact a logical way to go about changing assumptions. Holding the owners of trade secrets liable for the compromise of their information will make it clear that they are the first and only line of defense for the trade secrets they control. If a preventative strategy is to succeed, owners of trade secrets must understand that it is up to them to protect that information. In this context we must eliminate the assumption that the government or law enforcement is exclusively responsible for maintaining the security of property. Mandating prevention with specific rules and enforcement agencies would tend to perpetuate this assumption because the state would be directing the process. The state, not the civilian owners of trade secrets, would still be assuming primary responsibility for protecting property, although in a slightly different guise. Also, like any regulatory scheme, mandated prevention could take on a life of its own and lead owners of trade secrets to focus more on the process, that is, on what is involved in complying with the rules rather than on protecting their proprietary information.

We will therefore assume that the best implementation strategy uses civil or criminal liability to hold those who control trade secrets liable for the compromise of that information. The issue we now need to address is the type of liability that should be imposed.

2. Liability

The first option is to hold businesses or individuals or both civilly liable for not preventing the misappropriation of trade secrets in their possession and control. The obvious problem with this option is identifying the person who would seek

redress because civil litigation is initiated by such a person.[292] We would, therefore, need an injured person, with standing to bring the litigation.[293] Since owners of trade secrets are at once the victims of the misappropriation and the party to be held liable for failing to prevent misappropriation, we obviously cannot rely on them. When a business is involved, we could let the shareholders bring the suit, but there may be disincentives for them to do so.[294] Another alternative is to let the government bring suit as a civil enforcement action analogous to civil antitrust enforcement actions.[295]

The second option is to hold individuals or businesses or both criminally liable for defaulting on their obligation to prevent the misappropriation of trade secrets. We could not do this without modifying and extrapolating certain principles of criminal liability. We would be holding the victim of a crime (the owner of trade secrets) criminally liable for not preventing his/her/its own victimization. We would literally be blaming the victim. We currently conceptualize crime as a zero-sum event in which the perpetrator bears sole responsibility for the offense. We do not incorporate victim fault into our crime calculus, presumably due to the influence of the reactive model of law enforcement. [296] Under the reactive model, the victim's fault is irrelevant because civilians bear no responsibility for preventing crime. We are entitled and obliged to assume law enforcement will control crime sufficiently to maintain internal order in the society.[297]

If we wanted to pursue this option, could we eliminate this assumption without doing violence to our basic approach to criminal law? Could we articulate a justification for treating owners of trade secrets differently from, say, owners of

---

292. 67A C.J.S. *Parties* § 6 (2005).

293. BLACK'S LAW DICTIONARY 1442 (8th ed. 2004) (defining standing as a "party's right to make a legal claim or seek judicial enforcement of a duty or right").

294. *See supra* notes 207–08 and accompanying text.

295. *See* U.S. DEP'T OF JUSTICE, U.S. ATTORNEY'S MANUAL § 7-5.420, *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title7/5mant.htm.

296. *See* Brenner, *Toward A Criminal Law for Cyberspace, supra* note 223, at 85–87.

297. *See id* at 86–87*; supra* subpart III.B.2 (discussing real-world crime).

convenience stores?[298]

We could base the justification on the status of economic espionage as a state-sponsored crime. As noted earlier, economic espionage is an act of economic warfare,[299] which differentiates it from other types of online crime, including conventional theft. In conventional theft, the perpetrator acts to benefit himself and, perhaps, some associates; thus, the crime is intrinsically individual and involves only civilians.[300] The state's interest in this type of activity is, therefore, sufficiently vindicated if it is able to discourage it with the degree of effectiveness necessary to keep it at acceptably low levels within a society.[301]

Economic espionage represents a different dynamic and therefore requires a different calculus. The perpetrator of economic espionage directly attacks a civilian victim and, in so doing, indirectly attacks the state of which that victim is a citizen. Since economic espionage can erode a state's viability,[302] states have an enhanced interest in this type of criminal activity, one that goes beyond discouraging the activity with an efficacy sufficient to maintain a baseline of internal order.[303] Criminal law evolved to address only the latter interest.[304] We therefore have principles of criminal law that address the harm to the individual victim,[305] but lack principles that would encompass the harm to the state and provide the predicate for redressing that harm.

Such a principle must recognize that economic espionage inflicts harm both upon the individual victim and upon the

---

298. We need a principled justification to distinguish the two because we will retain the reactive model of law enforcement for other types of crime. *See supra* note 283.

299. *See supra* notes 249–50 and accompanying text.

300. *See* Brenner, *Is There Such a Thing As Virtual Crime?, supra* note 240, ¶ 23.

301. *See supra* subpart III.B.2 (discussing order).

302. *See* ONCIX 2004 REPORT, *supra* note 10, at 1 ("The . . . ability of foreign entities to acquire . . . US technology . . . has undermined US national security by enabling foreign firms to push aside US businesses in the marketplace and by eroding the US military lead.").

303. *See supra* subpart III.B.2 (discussing order).

304. Brenner, *Toward A Criminal Law for Cyberspace, supra* note 223, at 35–46.

305. *See, e.g.*, Brenner, *Is There Such a Thing as Virtual Crime?, supra* note 240, ¶ 40 (discussing theft offenses as a means of redressing harm resulting from loss of individual property); *see also supra* subpart III.A.1.

state. The harm to the individual victim is the loss in the value of the compromised trade secret.[306] Conceptually, the harm to the individual victim is a mixture of theft (the victim loses part of the value of its property) and property damage (the property is worth less than it was before).[307] We do not have a vocabulary that can describe the harm to the state because we are accustomed to thinking of crime as a civilian matter in which one citizen harms another. The state's only interest is to control this activity with an efficacy sufficient to maintain internal order.[308]

Crime is, and will remain, a primarily civilian matter.[309] What we need to realize, though, is that in an era of modern transportation and computer technology, crime is not *exclusively* a civilian matter. Conduct that falls within our conception of traditional varieties of crime can also inflict harm upon the state, and we need to be able to address this distinct, incremental harm.[310] To do that, we need to be able to articulate why the misappropriation of trade secrets inflicts discrete harms upon the individual owner and the state in which the owner is a citizen. To do that, we need to assess the nature of the property at issue in light of the concerns addressed above.[311]

Unlike the funds in the cash drawer of a convenience store, a trade secret cannot be considered purely private property. Trade secret data, like other types of information, has become

---

306. *See supra* subpart III.A.1.

307. *See* Brenner, *Is There Such a Thing as Virtual Crime?, supra* note 240, ¶ 44–47. Misappropriation of a trade secret is analogous to theft in that the perpetrator takes something from the victim. In that sense, it is analogous to other intellectual property crimes, such as copyright. *See, e.g.*, Geoffrey Neri, Note, *Sticky Fingers or Sticky Norms? Unauthorized Music Downloading and Unsettled Social Norms*, 93 GEO. L.J. 733 (2005). Misappropriation of trade secrets is also analogous to property damage crimes like vandalism in that the victim still has its property, i.e., the trade secret, but it is now damaged goods. *See* Brenner, *Is There Such a Thing as Virtual Crime?, supra* note 240, ¶ 71 (discussing cyber crime as analogous to vandalism in that another's property is still in their possession, but is damaged).

308. *See supra* subpart III.B.2 (discussing order).

309. *See* Brenner, *Toward A Criminal Law for Cyberspace, supra* note 223, at 31–49.

310. *See generally* Brenner, *Distributed Security: Moving away from Reactive Law Enforcement supra* note 272, at 34–35.

311. *See supra* subpart III.B.2 (discussing online economic espionage).

part of our critical national infrastructure.[312] It is therefore reasonable to conceptualize trade secrets as a new type of mixed property: information that belongs both to its civilian owner(s) and to the state.[313] Each has a distinct interest in the property: The owner's primary interest is in utilizing the trade secret for commercial purposes; the state's primary interest is in seeing that the trade secret's value is not compromised by losing its status as a secret.[314] With this mixed concept of trade-secrets-as-property, we can address both the harm to the individual owner(s) and the harm to the state. Addressing the latter requires implementing rules that hold the owners of trade secrets criminally liable, perhaps in varying degrees, for not preventing their misappropriation.[315] The gravamen of such liability is not the individual owner's loss, but the erosion of the commercial, tactical, and/or other advantages that accrued to the state from the information's remaining secret.[316]

The imposition of liability as hypothesized above is not as Draconian as it may sound. More than a century ago, American criminal law began to use regulatory offenses to create "forward-looking incentives yielding socially optimal outcomes."[317] While

---

312. Presidential Decision Directive NSC-63 (May 22, 1998), http://www.fas.org/irp/offdocs/pdd/pdd-63.htm; *see* ONCIX 2004 REPORT, *supra* note 10, at 1–2; Brenner, *Distributed Security: Moving Away from Reactive Law Enforcement*, *supra* note 271, at 35.

313. *See supra* subpart III.B.2 (discussing online economic espionage).

314. These interests are not completely discrete. The owner also has an interest in seeing that the secrecy of the information is not compromised, and the state has an indirect interest in seeing that it is utilized for commercial purposes.

315. For the implementation of an analogous type of criminal liability, *see* Brenner, *Distributed Security: Moving Away from Reactive Law Enforcement*, *supra* note 272, at 34–36 (discussing criminal product liability for software manufacturers).

316. The premise of such liability is analogous to that imposed in criminal antitrust proceedings:

> In a traditional criminal proceeding, the state acts to vindicate its obligation to protect a member of the social system it represents. In a criminal antitrust enforcement proceeding, the state acts to vindicate its obligation to protect essential components of the system. The "harm" caused by an antitrust "crime" is an erosion of the principle of competition. Criminal antitrust proceedings therefore target "systemic" crimes, i.e., crimes that impact upon a nation's infrastructure instead of upon individuals . . . .

Id. at 35 (notes omitted).

317. Louis Michael Seidman, *Points of Intersection: Discontinuities at the Junction*

the commission of a regulatory offense does result in the imposition of criminal liability, regulatory offenses differ from traditional crimes in several important respects. Like the liability hypothesized above, they target systemic harms instead of the imposition of a specific harm on an individual.[318] Since the goal is to create incentives to engage in certain socially-desirable conduct, they often target a failure to act where the law imposes a duty to act.[319] Also, conviction of a regulatory offense of the type proposed above does not carry the moral stigma or severe penalties that are associated with conviction of a traditional, common law crime like rape or murder.[320]

The primary difference between the criminal liability proposed above and the regulatory offenses we currently have is that the proposed liability blames the victim. It holds individuals and entities criminally liable *because* they failed to prevent their own victimization. The regulatory offenses that exist essentially impose liability for not preventing the occurrence of conditions that (i) create the potential for generalized harms, such as threats to public health and safety, or (ii) result in the occurrence of specified systemic harms such as environmental damage.[321] Thus, they sanction violators either for inflicting or creating conditions that can inflict external harm, that is, harm directed at someone other than the violator. For the reasons noted above, we have not yet sanctioned those who create conditions that produce internal harm, that is, the victimization of the violator.[322]

The difference between the two types of regulatory offenses is that the criminal liability proposed above is intended to target a type of activity distinct from the activities encompassed by our

---

Of Criminal Law and the Regulatory State, 7 J. CONTEMP. LEGAL ISSUES 97, 142 (1996).

318. *See id; see also* Brenner, *Distributed Security: Moving Away from Reactive Law Enforcement*, *supra* note 272, at 34–36.

319. *See* Seidman, *supra* note 317, at 142; *see also* Brenner, *Distributed Security: Moving Away from Reactive Law Enforcement*, *supra* note 272, at 36.

320. Seidman, *supra* note 317, at 142–43; *see also* Brenner, *Distributed Security: Moving Away from Reactive Law Enforcement*, *supra* note 272, at 37.

321. *See, e.g.*, United States v. Park, 421 U.S. 658 (1975); United States v. FMC Corp., 572 F.2d 902 (2d Cir. 1978).

322 *See supra* notes 295–96 and accompanying text.

current repertoire of regulatory offenses. The current set of regulatory offenses may be based on a different rationale than the rationale responsible for traditional crimes, but it has the same focus on undesirable activity occurring within the territorial boundaries of a society. When the locus of both the perpetrator and the harm is within the territorial boundaries of a state, a regulatory offense can be predicated upon the structure and assumptions we have traditionally utilized for crime. It can incorporate the reactive model, which focuses on sanctioning the person who inflicted the harm at issue in a particular offense, and the basic dynamic—offender, harm, reaction, sanction—can apply.

The criminal liability hypothesized above is intended to address a different scenario: undesirable state-sponsored activity that transcends the territorial boundaries of the society in which the harm occurs. Since the reactive model cannot deal effectively with this type of criminal activity, we must shift focus. If we cannot deter external actors from misappropriating our trade secrets, we must motivate the internal actors who control trade secrets to secure them and prevent their being misappropriated. The only way we can use criminal liability to this end is to reconceptualize the crime of economic espionage so that it has two components: (i) the conventional crime (economic espionage) which a state-sponsored agent commits against an owner of trade secrets, and (ii) the regulatory offense which the owner of trade secrets commits by not preventing the misappropriation of his/her/its proprietary information.

Parsing economic espionage into these analytically-distinct components gives us an equitable way to use criminal liability to implement a focused paradigm shift that emphasizes prevention, not reaction, as the strategy we employ to protect trade secrets. We apply an attenuated level of criminal liability in the form of a regulatory offense to the person who is responsive to the reactive model, that is, the domestic owner of trade secrets. This attenuated liability is based on existing principles of criminal law. By not preventing the misappropriation of trade secrets, the owner of those secrets contributes to the commission of economic espionage. In a harsher mode, we hold those who contribute to the commission

of a crime liable as accomplices to that offense.[323] Here, we apply a much narrower principle: The owner is held liable not as an accomplice to the completed crime, but for the separate and distinct offense of failing to institute security measures sufficient to prevent the theft of trade secrets.[324]

C. Sum

The strategy articulated immediately above may seem nothing more than a reiteration of the reactive model of law enforcement. Concededly, like that model, it encompasses a reaction to a crime—theft of trade secrets—and the consequent imposition of criminal liability. There is, however, a critical difference between the two. The current approach, as embodied in the EEA, is based on the assumptions that (i) law enforcement can react effectively to the compromise of trade secret information by agents of a foreign state, and (ii) a presumptively effective reaction will discourage such future attacks sufficiently to protect the security of trade secrets. Earlier Parts of this Article demonstrate that neither assumption is viable given that economic espionage is state-sponsored crime and is increasingly transnational in character.

The strategy articulated in subpart IV.B does not encompass either of these assumptions. It is based on a very different logic. It assumes that the best way to protect our trade secrets is to ensure that those who have possession and control of them take reasonable efforts to prevent their being compromised. Thus, its focus is on the owners of trade secrets (potential victims), not on those who seek to compromise trade secrets (potential criminals). It also assumes, for the reasons noted earlier, that a purely voluntary system of preventing the theft of trade secrets is likely to be ineffective, at least for the foreseeable future. This approach imposes criminal liability not in an attempt to deter the commission of crimes, but in an effort to create a climate in

---

323. *See, e.g.*, Brenner, *Distributed Security: Moving Away from Reactive Law Enforcement*, *supra* note 271, at 30–33.

324. For the implementation of an analogous type of criminal liability, *see id.* at 38–39.

which those who control trade secrets understand that they are the only ones who can prevent the compromise of that information.