NOTES

ECONOMIC ESPIONAGE: THE FRONT LINE OF A NEW WORLD ECONOMIC WAR[1]

The means by which enlightened rulers and sagacious generals moved and conquered others, that their achievements surpassed the masses, was advance knowledge. Advance knowledge cannot be gained from ghosts and spirits, inferred from phenomena, or projected from the measures of Heaven, but must be gained from men for it is the knowledge of the enemy's true situation.[2]

The spy of the future is less likely to resemble James Bond, whose chief assets were his fists, than the Line X engineer who lives quietly down the street and never does anything more violent than turn a page of a manual or flick on his microcomputer.[3]

I. INTRODUCTION

A. Background

With the end of the Cold War, although warfare per se has not declined, the threat of nuclear war is steadily declining. At the same time, this has led to an increase in the importance of economic competitiveness in nations' definitions of national security. Prior to the end of the Cold War, many international relationships were defined according to military alliances. These relationships are changing significantly due to a shifting international focus from a military to an economic outlook, and allies now see one another as competitors in the global economy.

Under this new arrangement, industrialized countries striving to maintain their standards of living, and developing nations eager to improve such standards, face enormous pressure to succeed. They will pursue any and all means which bear the potential to ensure their productivity and economic security. When economic objectives begin to play a more dominant role in defining national security, the interest in

---

1. Journalist and business consultant Sam Perry suggests that "[e]conomic espionage is the front line of a new world economic war. It is a war that most companies from open, democratic nations are illprepared to fight." *See* Sam Perry, *Economic Espionage and Corporate Responsibility*, CJ INT'L, Mar.-Apr., 1995 <http://www.acsp.uic.edu/oicj/pubs/cji/110203.html>.

2. SUN TZU, ART OF WAR, *reprinted in* THE COMPLETE ART OF WAR, at 118 (Ralph D. Sawyer, trans., Westview Press 1996).

3. ALVIN TOFFLER, POWER SHIFT: KNOWLEDGE, WEALTH, AND VIOLENCE AT THE EDGE OF THE 21ST CENTURY 311 (1990).

economic espionage expands. The end result for today's society is that economic espionage is the front line of a new world economic war.

This note will examine the problems surrounding economic espionage at the international level. A brief history of the problem will be presented first. Section two will then describe the current problem of economic espionage. Section three will consider the specific effects of economic espionage has on individual countries—from the victims to the perpetrators to the innocent bystanders in the global economic espionage struggle. Section four will discuss relative international agreements, laws, and organizations, as well as the reasons for their ineffectiveness in curbing international economic espionage. Finally, section five will put forth and analyze possible solutions to the problem.

B. Defining Economic Espionage

Many of the world's intelligence units have attempted to define economic espionage. Simply put, economic espionage is the "outright theft of private information."[4] A different and somewhat more definitive description comes from the Canadian Security Intelligence Service ("CSIS"). According to CSIS, economic espionage is "illegal, clandestine, coercive or deceptive activity engaged in or facilitated by a foreign government designed to gain unauthorized access to economic intelligence, such as proprietary information or technology, for economic advantage."[5] Still another, and far more complex definition is contained in the United States' Economic Espionage Act,[6] one of the few forms of legislation enacted by any state to help suppress economic espionage. The Economic Espionage Act criminalizes[7] activity by anyone who:

> intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4)

4. Peter Schweizer, *The Growth of Economic Espionage: America is Target Number One,* FOREIGN AFF., Jan.-Feb. 1996, at 9.

5. Canadian Security Intelligence Service, *Economic Security* (1996) <http://www.csis-scrs.gc.ca/eng/backgrnd/back6e.html>.

6. Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-1839 (1997).

7. Economic Espionage Act § 1831. Penalties for those convicted of this activity include fines up to $500,000, or imprisonment for up to fifteen years, or both.

attempts to commit any offense described in any of paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy. . ..[8]

American legislators have determined that the above activity constitutes economic espionage.

An important concept related to economic espionage is *economic intelligence*. CSIS explains that economic intelligence is "policy or commercially relevant economic information, including technological data, financial, proprietary commercial and government information, the acquisition of which by foreign interests could, either directly or indirectly, assist the relative productivity or competitive position of the economy of the collecting organization's country."[9] Those who conduct economic espionage specifically target this class of information.[10]

C. A Brief History of Economic Espionage

Espionage in the traditional sense is the way in which spies acquire an enemy's military secrets. A few famous incidents of espionage include England's use of spies to acquire military information in defeating the Spanish Armada in 1588; the Allies' use of spies during World War II in defeating the Axis powers; and the former Soviet Union's use of spies in stealing atomic bomb secrets from the United States and Great Britain.[11] Traditional espionage has transformed with the passing of the Cold War and the rise of international economic competition. Nations' economic and national security are closely connected and espionage activities are changing from military to economic foci.[12]

Although the end of the Cold War seemingly brings a surge of economic espionage activity, stealing the ideas of a business competitor is not a new game in the world market. Indeed, economic espionage is a practice that has existed for thousands of years. An early instance of economic espionage occurred over 1500 years ago and involved the secret of silk. A Chinese princess traveled abroad, wearing a flowered hat. She hid silkworms in the flowers and gave them to a man in India.

---

8. *Id.*

9. Canadian Security Intelligence Service, *supra* note 5.

10. *Id.*

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

12. *Id.*

Thus, through economic espionage, the secret of silk escaped from China.[13]

In the eighteenth century, China again lost a secret because of economic espionage. After China had spent centuries of making high-quality porcelain through a process known only to its alchemists, the French Jesuit, Father d'Entrecolles, visited the royal porcelain factory in China, where he learned the secrets of porcelain production and described the process in writings he sent to France.[14]

The early twentieth century and the reality of world-wide conflict led to significant incidents of economic espionage, proving that economic and military intelligence were equally important.[15] Opposing sides in World War I searched for secret weapons, knowing that such weapons would be available in a foreign country's industrial sector.[16] Spies gained information on how to create weapons like poison gas.[17] As was already known, spying saved countries time and financial resources that they would have spent developing poison gas on their own. The spies stole the secret from the Germans, and shortly afterward many countries used poison gas against each other during warfare.[18]

In the present day, economic espionage continually thrives. A few publicized incidents in more recent history include the following. In Japan, the ministry for international trade and industry identifies foreign high-tech companies that are likely to produce significant products in the near future.[19] The ministry supplies crucial information to Japanese companies, leading them toward purchasing the foreign companies through front organizations, false flag operations, or by overt means.[20] In an unrelated incident, a firm in the United States lost a contract bid for international electronics. Shortly thereafter, it learned that a European intelligence agency somehow intercepted its pricing information. The European agency turned this critical data over to another company which eventually won the contract bid.[21] In still another incident, CSIS discovered that a handful of "flight attendants" on Air France were ac-

---

13. JACQUES BERGIER, SECRET ARMIES: THE GROWTH OF CORPORATE AND INDUSTRIAL ESPIONAGE 3 (Harol J. Salemson trans., Bobbs-Merrill Co., Inc., 1975) (1969).

14. *Id.* at 4.

15. *Id.* at 31.

16. *Id.*

17. *Id.*

18. *Id.* at 32.

19. Thomas J. Jackamo, III, *From the Cold War to the New Multilateral World Order: The Evolution of Covert Operations and the Customary International Law of Non-Intervention,* 32 VA. J. INT'L L. 929, 945 (1992).

20. *Id.*

21. *Id.*

tually agents of the French intelligence service, strategically positioned to spy on companies' executives and gather their trade secrets.[22] These present-day examples, together with the afore-mentioned historical evidence, illustrate a crucial point: that economic espionage has been and continues to be on the rise.

II. Current Trends in Economic Espionage

A. Participants in the Trade

Countries involved. Counterintelligence agent George Lepine's description of global involvement in economic espionage is startling: "The question these days," he says, "isn't which country commits economic espionage, but which doesn't."[23] He and others estimate that two dozen countries regularly participate in economic espionage activities.[24] Among these are industrialized countries, including Japan, France, Russia, the United States, the United Kingdom, Germany, the Netherlands, Belgium, Israel, Taiwan, South Korea, and various Middle Eastern and Latin American countries.[25] According to a Canadian survey, the worst offenders are Asian governments, with western European governments following closely.[26] Other offenders can be found in various businesses throughout the United States, as indicated in a 1997 survey by The Futures Group. The survey revealed that in the United States, "[a] full 82 percent of companies with annual revenues of more than $10 billion now have an organized intelligence unit."[27] But economic espionage is not carried out exclusively by first world powers. "Countries that heretofore have not been considered intelligence threats account for much of the economic collection currently being investigated by. . .law enforcement communities."[28] In general, any nation that competes in the world market and has enough motivation to spy will engage in economic espionage.[29]

The significance surrounding the classes of parties involved in economic espionage is twofold. First, friendly and allied nations commit

---

22. Anthony Boadle, *Canada Spy-Catcher Says High-Tech Firms Targeted*, The Reuter European Bus. Report, Apr. 13, 1994.

23. Ian McGugan, *The Spy Who Came in for the Gold,* Can. Bus., May 1, 1995, at 99.

24. *Id.*

25. Jackamo, *supra* note 19, at 944; Schweizer, *supra* note 4.

26. McGugan, *supra* note 23.

27. Katherine Hobson, *Corporate Intelligence Seen as a Necessity* (visited Sept. 30, 1998) <http://www.abcnews.com/sections/business/DailyNews/spy980924/index.html>. The Futures Group is a competitive intelligence consultant in the United States.

28. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* (July 1995) <http://www.nsi.org/Library/Espionage/indust.html>.

29. Canadian Security Intelligence Service, *supra* note 5.

espionage against one another. In the world of economic espionage, there are no true friendly relations, largely due to the fact that countries which engage in the activity are vying for a rung on the global market ladder.[30] As former French intelligence chief Pierre Marion points out, "[i]t is an elementary blunder to think we're allies. . .When it comes to business, it's war."[31] Second, developing nations are heavily involved in the trade, due to recent political developments, especially the decline of communism.[32] Formerly communist states must quickly catch up with the West, and economic espionage often provides an avenue to do just that. Without communism, intelligence agents from Eastern block countries are unemployed and available in the open market.[33] The involvement of Eastern block agents is threatening because their intelligence activities are not restricted by traditional notions of international business ethics.[34] Therefore, such agents may go to any lengths to acquire the information they seek.

Individuals involved. There is no specific person who qualifies as an intelligence gatherer. However, some of the more common international snoops include competitors, vendors, investigators, business intelligence consultants, the press, labor negotiators, and government agencies.[35] Some countries hire individuals, rather than large organizations or intelligence agencies, to do their spying for them.[36] Other countries hire teams of individuals to enter foreign companies and steal ideas.[37]

B. Targets

Realistically, no business is especially immune from economic espionage. Targets include two main forms: industry and proprietary business information.[38] Government and corporate financial and trade data are also stolen on a regular basis. Industries are probably the biggest targets of economic espionage. Among those regularly sought are bio-

30. Marc A. Moyer, *Section 301 of the Omnibus Trade and Competitiveness Act of 1988: A Formidable Weapon in the War Against Economic Espionage,* 15 Nw. J. Int'l L. & Bus. 178, 182 (1994); Jackamo, *supra* note 19, at 944.

31. Stanley Kober, *Why Spy? The Uses and Misuses of Intelligence*, USA Today, Mar. 1, 1998, at 10.

32. Moyer, *supra* note 30, at 183.

33. *Id.*

34. *Id.*

35. Kevin D. Murray, *Ten Spy-Busting Secrets* (visited Sept. 10, 1998) <http://www.tscm.com/murray.html>.

36. John J. Fialka, War by Other Means: Economic Espionage in America 18 (1997).

37. *Id.* at 29

38. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, supra* note 28.

technology; aerospace; telecommunications, including information superhighway technology; computer software and hardware; advanced transportation and engine technology; oil and gas companies; advanced materials and coatings, including "stealth" technologies; energy research; defense and armaments technology; manufacturing processes; semiconductors; and critical technologies: manufacturing processes and technologies, aeronautics and surface transportation systems, and energy and environmental related technologies.[39]

The second targeted category is proprietary business information. Proprietary business information includes bid, contract, customer, and strategy information. What seems mundane and unimportant to companies can be very important to competitors—numerous amounts of stolen information consists of plant layouts, client lists and bids.[40]

C. Reasons Why Countries Conduct Economic Espionage

To Accelerate Modernization. The desire of states to possess the most modern industries and technologies possible is not an unreasonable one. Modernized states realize better overall economic development, self-sufficiency, and political autonomy than do undeveloped states.[41] In order to become more modernized, states with lesser-developed economies are tempted to import foreign technologies by whatever means are available, including economic espionage. Economic espionage appeals to these states because it saves them the time and financial resources they would have spent to develop the technologies on their own.[42]

Success Given in Economic Espionage. Nations also commit economic espionage because it is an area in which many of them are capable of success. Many countries already have the ability to carry out economic espionage because they the have sufficient funds and apparatus to do so. (Appendix) A United States Congressional intelligence committee report in 1994 stated that "reports obtained since 1990 indicate that economic espionage is becoming increasingly central to the operations of many of the world's intelligence services and is absorbing larger portions of their staffing and budget."[43] Additionally, many countries use their leftover Cold War spying apparatus, such as giant com-

39. Boadle, *supra* note 22; Moyer, *supra* note 30, at 184; *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, supra* note 28.

40. Boadle, *supra* note 22.

41. ROBERT GILPIN, THE POLITICAL ECONOMY OF INTERNATIONAL RELATIONS 112 (1987).

42. *Id.*

43. FIALKA, *supra* note 36, at 5 (quoting *Report on U.S. Critical Technology Companies, Report to Congress on Foreign Acquisition of and Espionage Activities Against U.S. Critical Technology Companies,* 1994, p. 5).

puter databases, scanners for eavesdropping, spy satellites, and bugs and wiretaps, to conduct economic espionage activities.[44]

Keeps Agents Employed. Some intelligence agents commit economic espionage to fill voids left from the Cold War, especially those agents from Eastern block countries, where the need for secret services has lessened.[45] These agents need new reasons to continue their spy work, and the economic sector occupies their time where the military sector previously did so.[46]

Leads to More Effective Global Competition. Companies commit economic espionage to increase their chances for success in the world market.[47] Economic espionage helps nations to maintain economic and technological competitiveness[48] and to gain an edge on a competitor because it helps to provide technologically limited countries with the modern devices they need.[49]

Profitable Business. Peter Schweizer writes, "[t]hat so many states practice economic espionage is a testament to how profitable it is believed to be."[50] Some countries gain financial profit as well as technology from economic espionage. In Australia, for example, economic espionage is estimated to be worth $2 billion per year.[51] France acquired a $2 billion deal with India for airplanes because of the economic espionage activities of the Direction Generale de la Securite Exterieure.[52]

Quick and Cheap. Getting the means of production is often more important for some countries than acquiring the actual technology.[53] The manufacture of a particular product, ballbearings for example, may not be a secret, but the means by which it is done well takes years to develop.[54] Countries that steal this information are therefore able to cut down the amount of time it would take to develop effective manufactur-

---

44. FIALKA, *supra* note 36, at 5.

45. McGugan, *supra* note 23.

46. Jackamo, *supra* note 19, at 938.

47. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, supra* note 28.

48. Jackamo, *supra* note 19, at 943.

49. *The Trade in Secrets*, THE BULLETIN, June 28, 1994 <http://www.dap.csiro.au/Interest/Secrets/secrets.html>.

50. Schweizer, *supra* note 4.

51. *The Trade in Secrets, supra* note 49.

52. Schweizer, *supra* note 4. The Direction Generale de la Securite Exterieure is the intelligence service of France.

53. Moyer, *supra* note 30, at 187.

54. *Id.*

ing processes on their own.[55] In sum, the supported philosophy is that it is quick and cheap to steal—crime pays.

Promotes National Security. "It has now been proven that economic strength of a nation is going to determine more than military power."[56] A nation's economic status makes up a large part of its national security.[57] This economic status is dependent upon a nation's ability to compete effectively in the world market. Because of this, economic competition "must be more carefully balanced with traditional military and intelligence concerns in determining policy to protect national security."[58]

D. Popular Methods

Virtually every traditional espionage method used during war is employed in today's business world. There are numerous ways in which countries carry out economic espionage, and many of these methods require little effort on the part of the perpetrators. Author Ira Winkler explains his approach to espionage: "I 'steal' most of my information by simply asking for it, looking on desktops, going up to computers that are left on all day, and digging through the trash. With few exceptions, all real-life James Bonds get their information exactly the same way."[59] The following are some of the most common methods of conducting economic espionage.

Planting "Moles" or Recruiting Agents. "Moles" are spies that are put into seemingly legitimate positions in a competitor's company.[60] Many intelligence gatherers rely on trusted workers within companies or organizations to provide them with proprietary and classified information.[61] A study by the American Society for Industrial Security ("ASIS") concluded that "trusted insiders pose the greatest risk" to the divulgence of trade secrets.[62] Lower-ranking employees, such as secretaries, computer operators, or maintenance workers, are regularly recruited because they often have desirable access to information and are

---

55. *Id.*

56. Steve Barth, *Spy vs. Spy,* World Trade, Aug. 1, 1998, at 34 (quoting John Schiman, special agent of the Federal Bureau of Investigation in Los Angeles).

57. *Id.* at 188-89.

58. *Id.*

59. Barth, *supra* note 56.

60. *Id.* at 180.

61. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, supra* note 28.

62. Barth, *supra* note 56.

easily manipulated by intelligence agencies due to their lower pay and status within their respective companies.[63]

Surveillance, Clandestine Entry, and Bag Ops. Intelligence gatherers often break into their competitors' offices outright and steal the information they want. Many incident reports describe stolen laptop computers, disks, and confidential files. "One common method of stealing laptops at airports is for the thief's accomplice to get into line at the x-ray machine just in front of the victim. While the accomplice slowly empties his pockets of keys and loose change, the thief takes your laptops off the conveyor on the other side of the machine and spirits it away."[64] Additionally, hotel rooms and safes are regular targets.[65] Some spies bribe hotel operators to provide access to the hotel rooms, which is known as a "bag op." During bag ops, gatherers search unattended luggage and confiscate or photograph anything they think may be valuable to them.[66]

Technical Operations. Computer hacking and telecommunication interceptions are common, especially where systems are not fully protected against such intrusions.[67] Easy targets are cellular and cordless telephones.[68] Hacking and interceptions can provide much information to intelligence gatherers, including trade secrets and other forms of competitive information.[69] In one case, "it was suspected that a host government was intercepting telephone conversations between an executive abroad and his Canadian company headquarters. Canadian executives discussed detailed negotiation information including a specific minimum bid. This minimum bid was the immediate counter-offer put forward by the host company the following day."[70]

Student Placements. When students study abroad, some governments task them with acquiring economic and technical information about their host countries.[71] Common perpetrators are graduate students who serve professors as research assistants free of charge. In research

63. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, supra* note 28.

64. Barth, *supra* note 56.

65. McGugan, *supra* note 23.

66. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, supra* note 28.

67. *Economic Espionage: Information on Threat from U.S. Allies,* GAO/T-NSIAD-96-114 (Feb. 28, 1996) <http://www.fas.org/irp/gao/nsi96114.html>.

68. Murray, *supra* note 35.

69. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, supra* note 28.

70. Canadian Security Intelligence Service, *supra* note 5.

71. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, supra* note 28.

positions, the foreign graduate students gain access to the professor's research, learning technological applications which they can then relay to their home governments.[72]

Debriefing Travelers. Debriefing citizens after foreign travel is popular in some countries. Travelers are asked for any information acquired during their trips abroad. The debriefing sessions are considered offensive to some travelers, while others accept them as part of traveling abroad.[73]

Dumpster Diving. Also known as trash trawling, waste archaeology, and trashing, dumpster diving is the act of rummaging through a competitor's garbage to obtain information. Some believe it is the number one method of business and personal espionage.[74]

Bugging and Tapping. Business class seats on airlines, offices, hotel rooms, and restaurants are regularly bugged and tapped by spies. In a specific incident, a European airline bugged its entire business class section, while spies posed as flight attendants.[75]

Drop-by Spies. Some intelligence gatherers pose as technicians and repair persons in order to get to confidential information. Others volunteer for positions that get them close to sensitive information.[76] Some spies even pose as documentary camera crew members to gain access to places where secret information is kept.[77]

E. Harmful Effects

Costs to the World Economy. As long as countries continue to conduct economic espionage activities, there will be serious implications for the world economy. Many scholars and reporters attempt to estimate economic espionage's financial burdens to society. Such costs are difficult to determine, due to the fact that international industry is generally reluctant to discuss them. No company wants to admit it has suffered significant financial loss at the hands of foreign spies, especially when it depends on shareholder support that may discontinue if shareholders feel the company is faltering.[78] IBM, however, came forward and discussed its losses. In 1992, IBM vice-president Marshall Phelps told a United States Congressional committee that his company suffered billions of

---

72. *Id.*
73. *Id.*
74. Murray, *supra* note 35.
75. Boadle, *supra* note 22.
76. *Economic Espionage: Information on Threat from U.S. Allies, supra* note 67.
77. *Id.*
78. Boadle, *supra* note 22.

dollars in losses due to theft of proprietary information.[79] This calculation supports the estimates of economists who claim that individual companies and firms lose billions of dollars annually through economic espionage.[80] For example, in its Intellectual Property Loss Survey Report from May 1998, ASIS estimated that American businesses may lose over $250 billion annually because of economic espionage.[81]

In spite of the difficulties of determining exact costs of economic espionage, two notions are clear: intelligence agencies spend billions of dollars each year in their espionage efforts, and counterintelligence agencies spend billions of dollars each year trying to thwart those efforts.[82]

In addition to direct financial loss, companies face other damages resulting from economic espionage: job loss and diminished or even lost contracts.[83]

Costs to Society in General. In an age where power stems from wealth, there is an ever-increasing fear that acquisition of economic information will lead to the breakdown of international security with economic foes of today becoming military foes of tomorrow. Society therefore lives in fear of economic espionage.

Economic espionage can destroy the incentive to innovate. No one wants to create new ideas if there is a strong likelihood that the ideas will be stolen, used, and sold by competitors. Not only will competitors take credit for ideas which belong to the original creators, but they will also profit from them financially, while the original creator will be left with nothing. This greatly discourages creativity.

F. Preventive Measures

One scholar points out that economic espionage "is an alive and growing art, and it's spawning a lot of protective measures."[84] Many countries respond to the threat of economic espionage in their own ways, by creating preventive measures, awareness and protection programs, and enacting laws. The following are recent examples of such action.

Canada. In January 1992, CSIS created its national Liaison/Awareness Program, which "seeks to develop an ongoing dialogue with organizations, both public and private, concerning the threat posed to

79. Canadian Security Intelligence Service, *supra* note 5.
80. *Id.*
81. Barth, *supra* note 56.
82. Richard Norton-Taylor, *Spooky Business,* THE GUARDIAN, Mar. 26, 1997.
83. FIALKA, *supra* note 36, at 6.
84. *The Trade in Secrets, supra* note 49.

Canadian interests by foreign government involvement in economic and defense-related espionage."[85] The program enables CSIS to collect and assess information that will promote its investigation of economic espionage activities against Canada. CSIS assesses the specific threats and advises the Canadian government accordingly.[86]

France. Recently, France developed INTELCO, a private intelligence company.[87] One of INTELCO's purposes is to teach business people how to safeguard their companies against espionage by foreign competitors.[88] The company is run by J. Pichot-Duclos, a former army general who oversaw France's military school for spies until 1992.[89]

Australia. Australia is in the process of changing its ASIO charter to allow investigations on the use of economic espionage in Australia. (ASIO is Australia's counter espionage agency.) If the charter is changed, non-military secrets will be protected in the same way as politically-motivated violence is protected.[90]

United States. In 1996, Congress passed the Economic Espionage Act, which proposes to deter theft of trade secrets by individuals and teams both within the United States and abroad. The Act purports to punish anyone who:

steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice or deception obtains a trade secret; without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization. . ..[91]

By December 1996, the United States was already prepared to fight one of its first cases under the new law, after two brothers, Patrick and Daniel Worthing, were arrested for misappropriating diskettes and other forms of confidential research information from the company for which they both worked.[92] Since the onset of this case, five other criminal actions have been brought under the Economic Espionage Act, resulting

---

85. Canadian Security Intelligence Service, *supra* note 5.

86. *Id.*

87. FIALKA, *supra* note 36, at 99.

88. *Id.*

89. *Id.*

90. *The Trade in Secrets, supra* note 49.

91. Economic Espionage Act of 1996, 18 U.S.C. §§ 1831(a), 1832(a).

92. R. Mark Halligan, *Reported Criminal Arrests Under the Economic Espionage Act of 1996* (visited Sept. 10, 1998) <http://www.execpc.com/~mhallign/indict.html>.

in two convictions.[93] Despite the presence of the Economic Espionage Act, however, it does not appear that it is being used to its full capacity. The few cases that have actually been brought to trial account for only a miniscule portion of the large number that are believed to exist.[94]

Multistate conferences. In recent years, some of the world's security organizations have held world-wide conferences to educate states on economic espionage and how to best protect themselves against it. In 1997, the National Computer Security Association ("NCSA") held such a conference in Brussels, Belgium.[95] Representatives from over thirty states participated in the "War by Other Means" conference that was geared toward protection of computer-related information.[96] The participants discussed and learned about such issues as open source intelligence and information strategy, information security basics, and information warfare and cyber-terrorism basics.[97] This was the NCSA's sixth conference on information warfare gathering, and it is helping to increase awareness of the "cyber battlefield" for economic espionage.[98]

Other Preventive Measures. Intelligence experts advise companies to protect their classified information carefully and effectively. Some of their suggestions include the following:

Appropriate classification, control and protection of sensitive documents;

Protection of computer databases and network links from unauthorized access;

Proper storage and disposal of sensitive documents;

Discussion of sensitive company matters in appropriate locations;

Realistic controls on employees' and visitors' access to sensitive facilities and materials;

Sensitivity and caution with the choice of medium used for business communications (i.e. cellular phones, open fax and phone lines);

---

93. Gerald J. Mossinghoff, et al., *The Economic Espionage Act: A Prosecution Update*, 80 J. PAT. [& TRADEMARK] OFF. SOC'Y 360 (1998). *See* United States v. Hsu, 982 F.Supp. 1022 (E.D. Pa. 1997), *reversed by* United States v. Hsu, 155 F.3d 189 (3d Cir. 1998); United States v. Pin Yen Yang, Criminal No. 1:97MG0109 (N.D. Ohio 1997); United States v. Davis (MD Tenn. 1997); United States v. Trujillo-Cohen (CR-H-97-251, S.D. Tex. 1997); United States v. Campbell (MD Tenn. 1997).

94. *Id.* at 368.

95. Bill Pietrucha, *NCSA Plans Information Warfare Conference*, IAC (SM) INDUSTRY EXPRESS (SM); NEWSBYTES, Feb. 5, 1997.

96. *Id.*

97. *Id.*

98. *Id.*

Education and sensitization of all employees about the threat that economic espionage may pose to job security and the organization's economic well-being; and

Emphasis on sharing responsibility amongst all employees for adherence to effective security policies and practices.[99]

III. Existing Treaties, Agreements, and an International Organization Related to Economic Espionage

A. General Problems with the Law

Because of the threat of economic espionage, many countries make economic security a priority, enacting laws that purport to deter would-be intelligence gatherers.[100] Although laws in individual countries may help protect economic secrets of the country's nationals, such laws do not solve the problem of economic espionage internationally. Part of the trouble may stem from the history some states have of not respecting the intellectual property rights of other states. Historically, patent law in some nations *encouraged* economic espionage abroad. For example, one of the earliest patent laws, developed in France, gave "to whomsoever shall be the first to bring to France a foreign industry the same advantages as if he were inventor of it."[101] France has since amended its patent law to exclude such encouragement, but the fact that it once existed only supports the idea that when a nation's economy is threatened, ethics will not necessarily keep it from protecting itself in any way possible.

A main legal problem regarding international economic espionage is that there currently is no rule that "prevents western multinational corporations from committing corrupt practices overseas."[102] Although progress has been made to prohibit bribes by western multinational corporations in underdeveloped countries via the United States' Foreign Corrupt Practices Act, very few nations have enacted laws that criminalize the bribing of foreign officials.[103]

Another problem is that when such corrupt practices do occur, victimized states fail to adequately retaliate. For example, after United

---

99. Canadian Security Intelligence Service, *supra* note 5.

100. Salem M. Katsh and Michael P. Dierks, *Globally, Trade Secrets are All Over the Map,* 7 No. 11 J. Proprietary Rts. 12 (1995). For example, Canada, China, Germany, Italy, Japan, Korea, Mexico, the United Kingdom, and the United States have adopted express statutory protection for trade secrets.

101. Bergier, *supra* note 13, at 13.

102. Alex Y. Seita, *Globalization and the Convergence of Values*, 30 Cornell Int'l L.J. 429, 486 (1997).

103. *Id.*

States officials learned of the existence of French spies in the French subsidiaries of Texas Instruments and IBM, the United States government simply sent a letter of diplomatic protest to France.[104] Similarly, the United States took little action against Israeli intelligence officers when they stole technological information from a defense contractor in Illinois, Recon Optical.[105] Until stronger reprimands are made by victims against violators and precedent is set to demonstrate that economic espionage such as this is intolerable, intelligence agents and others will continue to purchase and use stolen information, encouraging economic espionage's continuance.[106]

Furthermore, not all countries provide the same protection for intangible property rights, including trade secrets.[107] International intellectual property law does not help because it is quite weak, as will be discussed in further detail later in this report. At the present time, it does not provide much protection to countries that are regular victims of economic espionage.[108]

B. Treaties and International Agreements

The International Covenant on Economic, Social and Cultural Rights.[109] This agreement focuses in part on exploitation of Third World natural resources, but its coverage may be construed to reach other forms of economic wealth, including technology.[110] If the covenant is interpreted in this way, intellectual "innovation and expertise" would be considered among a state's natural resources, a subject matter which the agreement seeks to protect.[111]Therefore, economic espionage might be covered under this provision, but such a notion is questionable because the covenant refers more to overt ownership than covert theft of resources.[112]

Paris Convention. The Paris Convention for the Protection of Industrial Property, revised in 1967, is a multilateral treaty that provides

---

104. Schweizer, *supra* note 4.

105. *Id.*

106. *Id.*

107. Hoken S. Seki and Peter J. Toren, *EEA Violations Could Trigger Criminal Sanctions, Stiff Penalties are Intended to Deter Economic Espionage by Foreign Companies in the U.S.*, NAT'L L.J., Aug. 25, 1997, at B8.

108. Perry, *supra* note 1.

109. Dec. 16, 1966, 993 U.N.T.S. 3.

110. Jackamo, *supra* note 19, at 961.

111. *Id.*

112. *Id.*

the norms for international patents and trademarks.[113] It is the foremost industrial property law treaty and has extensive membership. Parties to the convention make up a union that protects industrial property. The significance of the union is that it consists of several administrative bodies that were created to ensure that the purposes of the convention would be fulfilled: the Assembly (the chief governing body under Article 13 of the Convention), the Executive Committee (a smaller body elected from the Assembly under Article 14), and the International Bureau of the World Intellectual Property Organization ("WIPO") (a body that performs the union's administrative tasks pursuant to Article 15).[114] The Convention sets forth uniform rules by which member states must abide with respect to industrial property rights.

Although the Convention purports to implement important industrial property laws, it is not effective against economic espionage, as evidenced by the present amount of economic espionage that takes place. Perhaps the reason why the Convention fails to help is because it does not specifically address economic espionage. Article 10 on unfair competition comes close where it states in subsection two that "any act of competition in contrary to honest practices in industrial or commercial matters constitutes an act of unfair competition."[115] However, member states may hold the view that this does not prohibit economic espionage. It should be duly noted that several member states to the Convention engage in economic espionage on a regular basis today.

General Agreement on Tariffs and Trade ("GATT"). On April 15, 1994, an agreement resulted from the Uruguay Round of GATT, establishing the World Trade Organization ("WTO") and promulgating several trade-related agreements.[116] The Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPs"), a product of the Uruguay Round, requires member countries to protect against acquisition, disclosure, or use of a party's trade secrets "in a manner contrary to honest commercial practices."[117] TRIPs specifically refers to "confidential information" rather than "trade secrets," but still emphasizes that such information has commercial value, is not in the public domain, and

---

113. Paris Convention for the Protection of Industrial Property, Mar. 20, 1883, *reprinted in* INTERNATIONAL TREATIES ON INTELLECTUAL PROPERTY 20-43 (Marshall A. Leaffer, ed., Bureau of National Affairs, Inc., 2d ed. 1997).

114. *Id.*

115. *Id.*

116. Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, LEGAL INSTRUMENTS—RESULTS OF THE URUGUAY ROUND vol. 31; 33 I.L.M. 81 (1994), *reprinted in* INTERNATIONAL TREATIES ON INTELLECTUAL PROPERTY, *supra* note 113 at 588-618.

117. *Id.*

is subject to "reasonable steps under the circumstances" to maintain its secrecy.[118] Relief offered to member states under the agreement includes injunctions and damages as well as provisional remedies to prevent infringement and to preserve evidence left behind by infringers.[119] Member states are also required to recognize third party liability.[120] Some countries already comply with TRIPs, but the purpose of the agreement is to *globally recognize* the importance of protecting trade secrets.[121] With this in mind, one of TRIPs' main goals is to foster consistency among nations.[122]

TRIPs' good intentions are not yet realized. The agreement so far has not been successful at curbing economic espionage. Perhaps this is due to the fact that TRIPs does not expressly forbid economic espionage. Furthermore, "the reality is that all parties knowingly tolerate substantial economic espionage activities because all sides believe that, on balance, they have more to gain by a world of information or unrestrained efforts to prevent 'hostile intelligence activities.'"[123]

C. United Nations Resolutions

Two United Nations Resolutions in particular relate to the problem of economic espionage, albeit indirectly. "Peaceful and Neighborly Relations Among States" is the title of Resolution 1236, which was passed in 1957.[124] It addresses the duty of non-intervention in other states' internal affairs, and calls upon states to settle their disputes in a peaceful manner.

A second resolution (Resolution 2131), passed in 1965 and entitled the "Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty" (the "Declaration on Inadmissibility"), declares that "[n]o state has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State."[125] The declaration condemns armed intervention as well as "all other forms of interference or attempted threats against the personality of the State or against its

---

118. Katsh and Dierks, *supra* note 100, at 15.

119. *Id.*

120. *Id.*

121. *Id.* (emphasis added).

122. *Id.*

123. *Relevant Intelligence in the Post-Cold War World* (visited Sept. 10, 1998) <http://www.venable.com/govern/fulltext.htm>.

124. G.A. Res. 1236, 12 U.N. GAOR, 12th Sess., Supp. No. 18, at 5, U.N. Doc. A/3805 (1957).

125. G.A. Res. 2131, 20 U.N. GAOR, 20th Sess. No. 14, at 11, U.N. Doc. A/6014 (1965).

political, *economic*, and cultural elements.. . ."[126] Arguably, however, this resolution was intended to deal more with economic sanctions than theft of private commercial secrets.

Because a state's economy is part of its internal affairs and economic espionage is an activity by which one state intervenes in another state's economic affairs, it could be construed that both resolutions indirectly condemn economic espionage. Each promotes non-intervention, and Resolution 2131 specifically condemns interference in a state's economic elements. However, these resolutions are ineffective in the war against economic espionage for the following reasons.

First, these and other United Nations resolutions on non-intervention lack the specificity to serve as guidelines that pinpoint permissible intervention.[127] Therefore, it is difficult to distinguish between what may and what may not be acceptable intelligence practices. Second, in reference to Resolution 2131, many states felt that the General Assembly merely expressed a political, rather than legal, view.[128] Third, states continually question the authority of General Assembly resolutions. Because these resolutions are persuasive and not binding materials, some states tend to ignore them.[129] The end result is that in spite of United Nations resolutions that are seemingly against it, economic espionage continues to exist.

D. An International Organization

World Intellectual Property Organization ("WIPO"). WIPO is the most important global intellectual property organization. Established by a convention at Stockholm in 1967, it administers international unions related to intellectual property, including the Paris Convention. Its main role is protecting the interests of intellectual property on a world-wide level.[130] In 1995, WIPO concluded an agreement with the World Trade Organization, establishing a cooperative relationship in which WIPO will provide WTO members and their nationals with copies of relevant laws and regulations in the same way that WIPO supplies its own members with such documents.[131]

---

126. *Id.* (emphasis added).

127. Jackamo, *supra* note 19, at 964.

128. *Id.* at 963.

129. *Id.* at 970.

130. INTERNATIONAL TREATIES ON INTELLECTUAL PROPERTY 561 (Marshall A. Leaffer ed., Bureau of National Affairs, Inc., 2d ed. 1997).

131. *Id.* at 577.

IV. RECOMMENDATIONS

"Any discussion about 'economic intelligence' must begin with an awareness that it is indeed a Brave New World for the Intelligence Community, one that must be entered with extraordinary sensitivity, as well as extensive public dialogue."[132] The sensitivity requirement exists because economic espionage is a sensitive subject area for many businesses. As was pointed out earlier in this report, businesses are reluctant to admit that they are victims of economic espionage. Additionally, this is a sensitive area because businesses instinctively try to keep their trade secrets from others, in order to prevent hard economic data from falling into the hands of both competitors and government representatives.[133] The public dialogue requirement exists because states must communicate nationally and internationally if they are to reach any agreements to help stop economic espionage.

What the preceding discussion of economic espionage shows is that there is a tremendous need for countries to create a global economic espionage agreement. Individual corporations and countries attempt to handle matters on their own, but it is difficult for them to counteract economic espionage, especially when foreign corporations and countries sanction and support such activity.[134] The fact that economic espionage continues to exist demonstrates that there is a need to set international business rules—both to promote fair economic competition and to balance competing values in a proper and formal way.[135]

There is presently much debate, both within nations and internationally, about the ways in which economic espionage should be controlled. The debate revolves around unilateral and multilateral action.[136] Industrialized countries are the leaders in implementing this action. They are now attempting to reach an agreement that would prohibit bribes and other corrupt practices in doing business abroad.[137] Corrupt business practices are illegal in all the industrialized countries.[138] Hence, the proposed agreement will simply extend that prohibition to activities abroad, potentially leading to higher ethical standards in developing countries where corruption runs rampant.[139]

---

132. *Relevant Intelligence in the Post-Cold War World, supra* note 123.
133. *Id.*
134. FIALKA, *supra* note 36, at 7.
135. Seita, *supra* note 102, at 484.
136. Moyer, *supra* note 30, at 179.
137. Seita, *supra* note 102, at 486-87.
138. *Id.*
139. *Id.*

Scholars and economists alike suggest many ways to battle economic espionage. The following is a compilation of popular suggestions. First, states must come to terms with what specifically constitutes the key elements of unjustifiable, unreasonable, or discriminatory conduct with respect to economic espionage, thereby defining the problem in explicit detail.[140] States must recognize what is and what is not economic espionage if they are to combat it.

Second, states must incorporate existing law, both national and international, that may apply to economic espionage, and propose new law where existing law fails to control economic espionage.[141]

Third, on the "supply side" of the economic espionage problem, states must make efforts to control their own exports and heighten individual corporate security.[142]

Fourth, on the "government side" of the economic espionage problem, states need to take advantage of existing governments and intelligence agencies of individual nations to curb economic espionage through law enforcement mechanisms.[143]

Fifth, states need to specify the roles that individual nations will play in identifying and countering the threats that economic espionage imposes on the industry of all nations, paying special attention to the manner in which such functions and roles are coordinated.[144]

Sixth, states must identify what constitutes the industrial threat, by discussing the threat to nations' industry of economic espionage and any trends in that threat, including: the number and identity of the governments conducting economic espionage; the industrial sectors and types of information and technology targeted by such espionage; and the methods used to conduct such espionage.[145]

Seventh, states need to work together toward an international criminal law solution, discussing the possibility of creating a coherent, modern body of international criminal law that deters and/or penalizes economic espionage.[146]

Finally, states might consider alternatives to banning economic espionage altogether. This might include the possibility of creating a

---

140. Moyer, *supra* note 30, at 179.

141. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, supra* note 28.

142. Moyer, *supra* note 30, at 179.

143. *Id.*

144. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, supra* note 28.

145. *Id.*

146. FIALKA, *supra* note 36, at 206.

United Nations or international economic intelligence service that works equally for all nations, leveling the field in which economic espionage is played. Perhaps an international economic intelligence agency could inspect and conduct surveillance globally, and share its findings with all nations. This might eliminate the current threats to global economic harmony.[147]

Overall, the importance of states working *together* to combat economic espionage cannot be stressed enough. This already occurs between some states, and others must follow such a lead. For example, some FBI agents in the United States regularly make contact with Scotland Yard or with the French police and work collectively in attempting to stop international criminals who are being investigated by both countries.[148] This kind of activity may open doors for creating relationships at a higher level, such as mutual legal assistance treaties for dealing with economic espionage crimes.[149] The United States Department of Justice already has such treaties, which provide procedures to share evidence and facilitate cooperative law enforcement with many countries throughout the world.[150] However, it does not presently have such treaties with any of the countries of Eastern Europe or the former Soviet Union, which began increasing their economic espionage activity with the end of the Cold War.[151]

V. Conclusion

Economic espionage will continue to be on the rise, unless nations make joint efforts to start dealing with the problem. Because of the dramatic changes to the world's military and economic divisions caused by the end of the Cold War, the probability that nations will continue to commit economic espionage against one another is great. Illicit gathering of competitor nations' economic information is what allows many nations to compete effectively in the world market. Those who take part in economic espionage will not be readily willing to stop, especially if it means losing any clout they have as members of the global economy. World leaders recognize that economic power is fundamental to national power. If nations persist to place their domestic priorities above international norms, the international economy will suffer as a result. For the world to achieve an even somewhat stable economy, individual govern-

147. Bergier, *supra* note 13, at 175.

148. Howard M. Shapiro, *The FBI in the 21st Century*, 28 Cornell Int'l L.J. 219, 224 (1995).

149. *Id.* at 227.

150. *Id.*

151. *Id.*

ments must be willing to put aside their short-term parochial interests and begin harmonizing business practices with one another.[152] It is vital that global leaders form an agreement on economic espionage. The world's economic future depends on it.

Karen Sepura

152. GILPIN, *supra* note 41, at 406.

APPENDIX

ECONOMIC ESPIONAGE ACROSS COUNTRIES:
LEVELS OF SOPHISTICATION

Tier 1	Tier 2	Tier 3
China	Colombia	Iraq
France	India	Libya
Germany	Russia	
Israel	South Korea	
Japan	Ukraine	
United States		

Tier 1: Through their technological and intelligence abilities, these countries eavesdrop electronically and perform computer intelligence gathering.

Tier 2: Although these countries have high-level intelligence gathering organizations, they do not have resources for computer and data intelligence gathering.

Tier 3: These countries' intelligence agencies will have high technology capabilities in the near future.

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