Cyber-Espionage: A Growing Threat to the American Economy

Gerald O’Hara†

"It's the great irony of our Information Age—the very technologies that empower us to create and to build also empower those who would disrupt and destroy."

I. INTRODUCTION

The American economy is currently the world’s largest and most advanced. It is this status that allows the United States to remain among the most powerful and influential countries in the world. However, the country’s economy is at risk of marginalization in a way that many policymakers could not have envisioned just a decade ago. The potential result threatens not only the economic standing of the United States in the global economy, but its national security as well. Although threats of economic and industrial espionage have long existed, the international proliferation of the Internet makes cyber economic and

† J.D. 2010, The Catholic University of America, Columbus School of Law. The author would like to thank Ed Schellhorn and Jenny Childs for their thoughtful suggestions throughout the writing process, as well as the editors and staff of the COMMLAW CONSENTUS for all of their hard work in preparing Volume 19.


3 Economic and industrial espionage refer to the theft of trade secrets for the benefit of
industrial espionage an especially daunting and potentially economy-crippling threat.\textsuperscript{4} Policymakers in Washington have primarily focused their efforts on implementing a cybersecurity policy that will combat doomsday scenarios such as transportation and electricity-grid shut downs.\textsuperscript{5} However, a more specific form of cyber attack—cyber-espionage—has emerged as an equally potent threat.\textsuperscript{6} Therefore, Congress, the Administration, and the private sector must work quickly and collectively to form a more focused and specific response to protect American economic interests.

A report commissioned by the security firm McAfee surveyed more than 1000 large corporations internationally and found that in 2008, the responding firms lost an average of $4.6 million due to cybersecurity breaches that resulted in lost or stolen intellectual property.\textsuperscript{7} Based on these findings, McAfee estimates that in the aggregate, companies across the globe lost more than $1 trillion from security breaches and from the resulting expenditures necessary to mitigate their effects.\textsuperscript{8}


\textsuperscript{5} Ellen Nakashima, War Game Reveals U.S. Lack Cyber-Crisis Skills, WASH. POST, Feb. 17, 2010, at A3 (describing a hypothetical war game in which a mock presidential administration reacted to power and cell phone outages across the United States that resulted from a cyber attack); see also, CYBERSPACE POLICY REVIEW, supra note 4, at 2-3 (setting forth a sixty-day cybersecurity review, directed by President Obama at the outset of his presidency, which focuses on broad cybersecurity agenda but does not specifically address or propose solutions for the problem of trade secret theft through cyber attacks).

\textsuperscript{6} CYBER-ESPIONAGE, TECHNOLYTICS INSTITUTE, TECHNOLOGY TRAINING BRIEF: CORPORATE ESPIONAGE, 10-11 (2009), available at http://www.technolytics.com/Technolytics-CorporateEspionage-111509.pdf. Cyber-espionage is “the intentional use of computers or digital communications activities in an effort to gain access to sensitive information about an adversary or competitor for the purpose of gaining an advantage or selling the sensitive information for monetary reward.” Id. at 11.

\textsuperscript{7} McAfee, Unsecured Economies: Protecting Vital Information 1,7 (2010).

\textsuperscript{8} Press Release, McAfee, Inc. Research Shows Global Recession Increasing Risks to Intellectual Property (Jan. 29, 2009),
In the United States, reports of cyber attacks aimed at industrial information surface almost daily, sparing no company, regardless of its size or technological experience. Notably, in 2010, the Internet search giant Google announced that its proprietary source code was the target of cyber attacks originating from mainland China. Google’s vulnerability to such an attack is the most glaring signal to government and industry leaders of the severity of the problem of cyber-espionage and the urgency with which the United States must undertake a coordinated response. Furthermore, the problem of detection further contributes to firms’ inability to prevent this new form of spying. Private firms are often unaware of data breaches, sometimes discovering cyber attacks only after they have been ongoing for months or even years. Non-detection was explained by one expert this way: “If I [physically] steal your car, you know because it is gone, but if I steal your customer list or a design plan . . . you will not know that I have it, and you will remain comfortable.” Such an untraditional threat will not be defeated using traditional measures.

The current federal criminal law that prohibits trade secret theft, The Economic Espionage Act of 1996 ("EEA"), is incapable of combating the new and developing tactic of trade secret theft through cyber-espionage. As explained in detail below, the EEA was passed to prevent corporate insiders from stealing trade secrets and selling them to foreign governments and foreign or


12 See Siobhan Gorman, Broad New Hacking Attack Detected, WALL ST. J., Feb. 18, 2010, at A3 (providing an example of recent difficulties with detection and noting that the “damage from the latest cyber attack is still being assessed, and affected companies are still being notified.”).


14 Cf. NAT’L ACAD. OF SCI., NAT’L RESEARCH COUNCIL, LETTER REPORT FROM THE COMMITTEE ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY (2010) (comparing nuclear deterrence with deterrence in the cybersecurity context, and arguing that traditional deterrence strategies formed during the Cold War will be ineffective for deterring cyberattacks).

domestic companies. At the time it passed the EEA, Congress could not have anticipated that trade secret theft through cyberspace would become such an efficient and widely-employed way of stealing proprietary information from domestic companies. The increasing availability of technology and the Internet has led to innovative and ever-evolving cyberattacks. The current law is inadequate to deal with the cybertheft of corporate trade secrets. Thus, Congress must develop new, comprehensive protections to account for the growing threat of cyber-espionage.

Any domestic measures to deter cyber attacks targeted at corporate trade secrets must be combined with diplomatic action that discourages foreign countries from enabling or tolerating cyber-espionage. A comprehensive approach must include updating international treaties that address intellectual property protection, such as the World Trade Organization’s Agreement on Trade-Related Aspects of Intellectual Property Rights (“TRIPS Agreement”). However, the TRIPS Agreement, while attempting to set a minimum standard of copyright, patent, and trademark protection across borders, does not adequately address the protection of trade secrets from economic or industrial espionage. Nevertheless, the United States, through its prominent position in the World Trade Organization, should advocate for increased scrutiny of foreign sponsorship of economic espionage, using the forum of multinational trade negotiations to help foster agreement.

Part II of this comment describes the evolution of trade secret law from its roots in the common law, to the enactment of the Uniform Trade Secrets Act in most of the states, and the passage of the Economic Espionage Act, which makes foreign and domestic trade secret theft a federal crime. Part III provides an overview of the international landscape of trade secret protection and the TRIPS Agreement. Part IV presents the recent real-world attacks on Google’s proprietary source code as a case study. This analysis explains the particular dangers of cyber-espionage, the severity of the problem, and potential practical

16 Economic Espionage: Joint Hearing Before the S. Select Comm. on Intelligence and the Subcomm. on Terrorism, Technology and Governmental Information of the S. Comm. on the Judiciary, 104th Cong. 359 (1996) (statement of FBI Director Louis Freeh) (focusing on theft of proprietary economic information by company insiders, who then might transmit those secrets to other companies or foreign nations.) [hereinafter Senate Hearing].

17 See id. at 63 (statement of FBI Director Louis Freeh) (noting that, at the time, “a lot of proprietary information [was] not transmitted either through computers, nor [did] it reside necessarily on computers”).

18 See INFO. WAREFARE MONITOR \ SHADOWSERVER FOUND., SHADOWS IN THE CLOUD: INVESTIGATING CYBER-ESPIONAGE 2.0 i (2010) (stating that “[a]ttackers employ complex, adaptive attack techniques that demonstrate high-level ingenuity and opportunism.”).


20 See discussion infra Part III.
responses. Part V offers recommendations on how the United States can more effectively prevent and react to cyber-espionage and concludes with a brief outlook of how the combination of domestic and diplomatic actions taken by the United States can improve the economic future for American companies doing business in a digital age.

II. THE STATE LAW SCHEME OF TRADE SECRET PROTECTION AND PASSAGE OF THE ECONOMIC ESPIONAGE ACT

A trade secret "includes generally all types of information, regardless of the method of storage or maintenance, that the owner has taken reasonable measures to keep secret and that itself has independent economic value. . . ." This definition captures a much broader group of proprietary information than is protected under long-standing copyright, trademark, or patent laws. A copyright "protects the physical expression of an idea, but not the idea itself." A trademark "protects a commercial identity or brand used to identify a product or service to consumers." A patent "generally protect[s] products and processes, not pure ideas." All three of these long-recognized legal protections provide their owners with a high degree of certainty about how their proprietary information is protected, and also makes it clear to those who would steal any of these kinds of protected information just exactly how they will be punished. No such certainty exists for the owners or thieves of trade secret information.

Trade secret protection has evolved from the common law, where trade secret misappropriation was initially treated as a tort. As the law evolved and became more specialized, it became necessary to classify it on its own, and the Uniform Trade Secrets Act was developed and adopted by many states. It was only relatively recently that Congress responded to lobbying attempts from

---

22 JAMES POOLEY, TRADE SECRETS § 3.1 (2d ed. 2009).
23 U.S. DEPT. OF JUSTICE, supra note 21, at 3.
24 Id. at 4.
25 Id.
26 Indeed, the Federal Government has made protecting intellectual property a top priority. See, e.g., id. at 309 ("Because of the importance of intellectual property to the national economy and the scale of intellectual property theft, intellectual property crime continues to be a law enforcement priority."); see also id. at 3-5 (introducing the intellectual property protections given to copyrights, trademarks, and patents).
industry leaders, who claimed that existing criminal laws were insufficient to prosecute the growing problem of trade secret theft, and made economic and industrial espionage a federal crime.  

A. Civil Law Tradition of Trade Secret Protection

Prior to passage of the Federal Economic Espionage Act, trade secret theft developed through the common law of the states. The federal patent and copyright laws provided domestic protection for tangible goods, but intangible proprietary information such as "production processes, bid estimates, production schedules, computer software, and technology schematics," did not fall under the protection of the federal patent or copyright laws. The Restatement of Torts (1939) included trade secret misappropriation for the first time.

In the context of industrial espionage, misappropriation is simply "the deliberate taking of information one knows to belong to someone else, whether or not the misappropriator proceeds to use or disclose it." By 1979, the drafters of the Restatement (Second) of Torts declined to include trade secret law in the updated Restatement, recognizing that it had become overly specialized and "that [trade secret law] was no longer properly classified as a species of tort law."
In an effort to develop a uniform set of rules to protect proprietary trade secret information, a majority of states gradually adopted versions of the Uniform Trade Secrets Act ("UTSA"), a uniform code promulgated by the National Conference of Commissioners on Uniform State Laws in 1979. The UTSA provides civil remedies for the theft of trade secrets and allows victims of the theft to recover damages that may "include both the actual loss caused by the misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss." However, because the states passed their own versions of the UTSA, little consistency existed from state to state. Furthermore, companies often were hesitant to engage in expensive litigation in order to prosecute trade secret theft as it often required large outlays for investigatory work.

B. Federal Criminal Law prior to passage of the EEA

As FBI Director Louis Freeh pointed out in his testimony before a Joint Committee hearing of the Senate Select Intelligence Committee and the Subcommittee on Terrorism, Technology, and Government Information of the Senate Judiciary Committee, the protection of proprietary intellectual property emanates from the Constitution. Article I, Section 8 of the United States Constitution states that "Congress shall have the Power . . . [t]o promote the [p]rogress of [s]cience and useful [a]rts, by securing for limited [t]imes to [a]uthors and [i]nventors the exclusive [r]ight to their respective writings and discoveries." The federal patent and trademark acts, which provided owners with statutory remedies to pursue against willful violators, followed from this constitutional recognition that intellectual property required protection. How-

36 UNIFORM TRADE SECRETS ACT (1985).
38 POOLEY, supra note 22, § 2.03[7][b] at 2-30.3 (noting a lack of uniformity as a major drawback of the USTA).
39 H.R. REP. No. 104-788, at 7 (1996) ("Many companies choose to forego civil litigation because of the difficulties in enforcing a monetary judgment against some defendants which may have few assets or foreign governments with few assets in the United States or because companies do not have the resources or time to bring the civil action."); Senate Hearing, supra note 16, at 65 (statement of FBI Director Louis Freeh) ("The amount of discovery, the jurisdiction that is involved, as well as the uncertainty of the litigation . . . make this a problem which we can't simply relegate to the civil system where trade secrets have really been enforced—at least for the last 200 years.").
40 Senate Hearing, supra note 16, at 62 (statement of FBI Director Louis Freeh) ("Unlike many of the statutes that the FBI enforces, the authority for the protection of intellectual property and proprietary economic information really comes from the Constitution itself.").
41 U.S. CONST. art. 1, § 8, cl. 8.
ever, intellectual property falling outside of one these very specific categories generally was left to the less certain protection of the common law.\footnote{POOLEY, supra note 22, § 2.01[1] at 2-2 (noting that “judicial opinions are the well-spring of trade secret law.”). For background on how the common law has developed with respect to the United States Supreme Court, see id. § 2.01[2] at 2-3.}

1. Intellectual Property as Physical Property

Although federal prosecutors had difficulty prosecuting trade secret theft under federal statutes prior to the passage of the EEA, they were able to prosecute some instances of trade secret theft using certain federal statutes. The Interstate Transportation of Stolen Property Act\footnote{18 U.S.C. § 2314 (2006).} ("ISTP") was passed to combat the problem of stolen goods being transported from state to state with a then-novel technology—the automobile.\footnote{Senate Hearing, supra note 16, at 62-63 (statement of FBI Director Louis Freeh).} Federal prosecutors became increasingly reluctant to rely on the ITSP in trade secret theft cases after the Court’s ruling in Dowling v. U.S.\footnote{Dowling v. U.S. 473 U.S. 207, 216 (1985). Id. at 216.} In that case, the Court noted that the ITSP applied only to the theft of “goods, wares, [or] merchandise,”\footnote{Id. at 221.} and therefore the federal criminal statute could not apply to theft of a copyrighted work.\footnote{Id. at 217-18.} Dowling essentially held that a copyright cannot be stolen (which triggers criminal punishment); it can only be infringed upon (subjecting the infringer to civil liability).\footnote{Cf. David D. Mouery, Trademark Law and the Bottom Line—Coke Is It!, 2 BARRY L. REV. 107, 124 (2001) (categorizing trade secrets as a type of intellectual property which are, among other things, “intangible business asset[s]”); Garret Power, Regulatory Takings: A Chronicle of the Construction of a Constitutional Concept, 23 BYU J. PUB. L. 221, 229 (2009) (“Blackstone’s view [of property] failed to account for intangible assets such as business goodwill, trademarks, trade secrets and copyrights.”).} Because a trade secret is an idea and not a physical asset, federal prosecutors have found it difficult to prosecute individuals for trade secret theft under the ITSP.\footnote{See Peter J.G. Toren, The Prosecution of Trade Secret Thefts Under Federal Law, 22 PEPP. L. REV. 59, 81 (1994); Jonathan Eric Lewis, The Economic Espionage Act and the Threat of Chinese Espionage in the United States, 8 CHI.-KENT J. INTELL. PROP. 189, 198-99 (2009).}

2. Federal Wire and Mail Fraud Statutes

The other statutes that federal prosecutors came to rely on in the wake of Dowling were the federal Wire and Mail Fraud statutes.\footnote{Spencer Simon, The Economic Espionage Act of 1996, 13 BERKELEY TECH. L. J. 305,} These statutes re-
quire use of mail or wire communications during the course of the act for federal jurisdiction to apply, and prosecutors often found that the particular facts of a given case rarely fit neatly into the elements of these statutes. Then Director of the Federal Bureau of Investigation Louis Freeh summed up the problem in his testimony during consideration of the EEA: "we are really left with a hodgepodge of statutes, which can from time to time be effectively applied. But what’s lacking is one systematic federal law which addresses the scope of the problem and doesn’t depend on individual circumstances to assert jurisdiction."

C. The Economic Espionage Act

Congress finally addressed the fragmentation and general ineffectiveness of the existing trade secret protection scheme in 1996 with the passage of the EEA. In passing the EEA, Congress recognized the need for uniformity and the inability of the UTSA to effectively deter trade secret theft. The Senate Judiciary Committee noted that "[a] federal criminal law is needed because of the international and interstate nature of this activity, because of the sophisticated techniques used to steal proprietary economic information, and because of the national implications of the theft."

The EEA broadly defines "trade secret" to include all "forms and types of financial, business, scientific, technical, economic or engineering information . . .". In order for the information to be considered a trade secret, its owner must "take[] reasonable measures to keep such information secret." Additionally, proprietary information contained in the trade secret must "derive[] independent economic value . . . from not being generally known to, and not being readily ascertainable through proper means by, the public." The EEA’s definition slightly broadened the scope of information considered to be a "trade secret" from the more limited definition provided by the UTSA, and was met


54 See Senate Hearing, supra note 16, at 63 (statement of FBI Director Louis Freeh).
55 Id.
57 See H.R. REP. NO. 104-788, at 7-9 (1996)(noting the importance of developing a systematic approach to deterring the theft of trade secrets).
60 Id.
61 Id.
62 Spencer Simon, The Economic Espionage Act of 1996, 13 BERKELEY TECH. L.J. 305, 311 (1998) ("The definition of trade secrets under the EEA is broader than that contained in the UTSA because it includes the new technological methods by which trade secrets can
There is a strong indication that foreign economic espionage was a primary concern of Congress at the time of the EEA’s passage. Section 1831 of the EEA prohibits economic espionage, which is defined as the theft of a trade secret that “will benefit any foreign government, foreign instrumentality, or foreign agent.”64 During a joint hearing on the EEA in 1996, Senator Arlen Specter noted that “the White House Office of Science & Technology estimate[d] losses to U.S. business from foreign economic espionage in the $100 billion range. And ABC News . . . has estimated that some 6 million job losses are attributed during this decade to economic espionage.”65 At the same hearing, FBI Director Louis Freeh put forth three reasons to justify a federal law that criminalized economic espionage, noting a recent uptick performed on behalf of foreign countries:

[First], in the wake of the [C]old [W]ar many of the foreign intelligence agencies have diverted some of their objectives from the military targets to the industrial, economic, and proprietary targets. Second, after the [C]old [W]ar many of our traditional allies are now fierce economic competitors. So there is great incentive to obtain U.S. proprietary secrets and information. Third, there is a huge global market which can respond very quickly to early access and early production of items which require [millions of] dollars of research and development.66

Section 1832 prohibits theft of a trade secret by any person, even if it will not benefit a foreign entity.67 Essentially, § 1832 criminalizes domestic trade secret theft.68 Some critics pointed out that it was unusual for an offense to be criminalized without first having been developed through civil penalties.69

now be created and stored.”).
Nevertheless, § 1832 made it a federal crime to undertake action that up to that point was only punishable under state civil laws.\textsuperscript{70} The penalties are more severe under § 1831 for committing economic espionage than for committing domestic trade secret theft under § 1832.\textsuperscript{71} An individual who commits economic espionage under § 1831 may be imprisoned up to 15 years and fined up to $500,000.\textsuperscript{72} An organization may be punished under § 1831 with a fine of up to $10 million.\textsuperscript{73} An individual who commits trade secret theft in violation of § 1832 may serve up to 10 years in prison and also be fined up to $250,000.\textsuperscript{74} An organization found in violation of § 1832 may face a fine of up to $5 million.\textsuperscript{75}

The EEA also contains an extraterritoriality provision that makes it applicable to conduct that takes place outside the United States.\textsuperscript{76} Section 1837 applies to acts of espionage that initiate outside of the United States "if (1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States . . . or (2) an act in furtherance of the offense was committed in the United States."\textsuperscript{77} This section is included to "rebuff the general presumption against the extraterritoriality of U.S. criminal laws [and] makes it clear that the Act is meant to apply to the specified conduct occurring beyond U.S. borders."\textsuperscript{78} This extraterritoriality feature of the EEA was touted as a key component of prosecuting economic espionage that benefits foreign actors under § 1831.\textsuperscript{79} However, as discussed below, technological advances have enabled those who commit economic espionage to completely avoid prosecution under the EEA.

### D. The EEA Has Been Toothless

Despite its aspirations to impose harsh criminal penalties, the EEA fails to provide a robust enforcement mechanism against foreign cybercriminals who initiate attacks on American corporations.\textsuperscript{80} Furthermore, enforcement under

\textsuperscript{71} Compare 18 U.S.C. § 1831 (providing that an individual who commits economic espionage may be imprisoned for up to 15 years) with 18 U.S.C. § 1832 (affording punishment for theft of a trade secret by an individual of not more than 10 years imprisonment).
\textsuperscript{72} 18 U.S.C. § 1831.
\textsuperscript{73} 18 U.S.C. § 1831(b).
\textsuperscript{74} 18 U.S.C. § 1832.
\textsuperscript{75} 18 U.S.C. § 1832(b).
\textsuperscript{76} 18 U.S.C. § 1837.
\textsuperscript{77} \textit{Id.}
\textsuperscript{80} Michael L. Rustad, The Negligent Enablement of Trade Secret Misappropriation, 22
the EEA has mainly targeted domestic trade secret theft. Professor Rustad reported the results of an empirical study of prosecutions under the EEA in the first decade of its enactment, noting that through August 1, 2005, there were "fewer than fifty economic espionage prosecutions filed in federal courts; nearly every prosecution was for domestic rather than foreign economic espionage." Unsurprisingly, given the rapid pace of technological advancement since the EEA’s passage in 1996, it has become increasingly easy for individuals and corporations to perpetrate economic and industrial espionage without leaving the confines of their home or office, and from outside of the United States. The extraterritoriality provision of § 1837 has therefore become ineffective at capturing foreign actors that initiate cyber attacks against corporations in the United States. The FBI, the agency tasked with investigating charges of economic espionage, nearly concedes as much on its economic espionage website with a warning to domestic firms to be on the lookout for spies to go "dumpster diving" in search of discarded trade secrets.

---

82 Id.
83 See, e.g., Ellen Nakashima, More Than 75,000 Computer Systems Hacked in One of Largest Cyber Attacks, Security Firm Says, WASH. POST, Feb. 18, 2010, at A3 (noting one attack that "targeted proprietary corporate data, e-mails, credit-card transaction data and login credentials at companies in the health and technology industries" in "196 countries").
84 See 18 U.S.C. § 1837 (2006) (defining narrow circumstances by which the statute covers conduct occurring outside the United States). However, the statute remains effective for instances of actual, physical infiltrations by foreign agents. See, e.g., United States v. Chung, 633 F. Supp. 2d 1134, 1148 (C.D. Cal. 2009) (describing a six-count conviction of a foreign based on the agent’s physical possession of trade secret documents obtained illicitly from employer within the United States). See also Chad Bray & Jacob Bunge, Former Programmer at Goldman Indicted, WALL ST. J., Feb. 12, 2010, at C6 ("A former Goldman Sachs Group computer programmer . . . was charged in a three-count indictment with theft of trade secrets, transportation of stolen property in interstate and foreign commerce and unauthorized computer access.").
increase in cyber attacks, the EEA, or any federal criminal statute standing alone, will be incapable of effectively deterring such attacks or prosecuting the perpetrators of the attacks. Therefore, Congress and the Administration must take swift action to protect the proprietary information of domestic companies—not only by passing new legislation to address cyber-espionage, but also by engaging with the international community to normalize expectations of trade secret protection across borders. The absence of a diplomatic solution will only make any domestic efforts fruitless.

III. INTERNATIONAL PROTECTION OF TRADE SECRETS AND THE TRIPS AGREEMENT

Prior to the TRIPS Agreement, intellectual property rights were recognized at the international level by two main multilateral agreements: (1) the Paris Convention for the Protection of Industrial Property, and (2) the Berne Convention for the Protection of Literary and Artistic Works. Both conventions are administered by the World Intellectual Property Organization ("WIPO"), though neither has been substantively updated since 1967. As technology evolved, the international community was largely unable to agree on harmonizing intellectual property protection across borders when negotiating in the singular context of intellectual property through WIPO. It required the aegis of international trade to provide nations with incentives to come to an agreement on a minimum standard of intellectual property protection. Negotiations finally began to take place within the General Agreement on Tariffs and Trade

---

87 Nakashima, supra note 83, at A3.
88 See, e.g., David Goldstone, Prosecuting Intellectual Property Crimes 214 (William Hein & Co. 2001) (noting that an EEA case requires a "sufficient nexus to U.S. interests, applying] to conduct occurring outside the United States if: (1) the offender is a citizen or permanent resident alien of the United States ...; or (2) an act in furtherance of the offense was committed in the United States."); see also 18 U.S.C. § 1837 (requiring, as extraterritorial provision of economic espionage statute, an offender be a U.S. citizen or resident alien and for an offense or act relating to the offense be committed inside of the U.S.).
91 Daniel Gervais, The TRIPS Agreement: Drafting History and Analysis 9 (Sweet & Maxwell 1998). Both of these conventions were almost entirely incorporated by reference into the TRIPS Agreement. Id. at 26.
92 Id. at 10.
93 Id. at 10 (describing member countries desiring new intellectual property standards as "using] the Ministerial Conference which launched the Uruguay Round of Multilateral Trade Negotiations at Punta del Este (Uruguay) in September 1986 to inscribe this subject matter on the agenda of the new Uruguay Round.").
("GATT") framework during the mid-1980's, and resulted in the TRIPS Agreement.94

A. Achieving Intellectual Property Protection Through International Trade Negotiations

The World Trade Organization ("WTO"), an international forum of 153 member-countries that regularly meets and negotiates international norms on trade relations,95 adopted the TRIPS Agreement on April 15, 1994.96 The Agreement's ratification was heralded as "the most significant milestone in the development of intellectual property" in the 20th century.97 The international community had relied up to that point on WIPO for normalizing intellectual property rights across national borders.98 However, WIPO was unable to successfully update its governing conventions since its inception in 1967, and also did not promulgate any additional international agreements on patent, trade, or copyright laws.99 WIPO thus proved itself ineffective at fostering agreement on international intellectual property norms.100 Without clear incentives to create new laws or update existing ones, countries with extremely disparate levels of intellectual property development were unwilling to agree to binding, multilateral agreements to standardize protection of intellectual property rights across

94 Id. at 10-25 (chronicling the GATT framework and negotiations that brought about TRIPS).
95 About the WTO—A Statement from the Director General, WORLD TRADE ORGANIZATION, http://www.wto.org/english/thewto_e/whatis_e/wto_dg_stat_e.htm (last visited Jan. 1, 2011). Providing:

The WTO provides a forum for negotiating agreements aimed at reducing obstacles to international trade and ensuring a level playing field for all, thus contributing to economic growth and development. The WTO also provides a legal and institutional framework for the implementation and monitoring of these agreements, as well as for settling disputes arising from their interpretation and application. The current body of trade agreements comprising the WTO consists of 16 different multilateral agreements (to which all WTO members are parties) and two different plurilateral agreements (to which only some WTO members are parties).

Id.
96 GERVAIS, supra note 91, at 25.
97 Id. at 3.
99 See GERVAIS, supra note 91, at 9-10 ("The last revision on substance of both conventions took place at Stockholm in 1967.").
100 Cf. id. at 10.
borders. This dynamic changed when industrialized countries injected a dialogue on intellectual property rights protection into multilateral trade negotiations of GATT, the WTO’s predecessor, in 1986.

B. The TRIPS Agreement

The TRIPS Agreement set minimum standards of intellectual property protection in all member nations. Its purpose, as set out in the preamble, was “to reduce distortions and impediments to international trade . . . to promote effective and adequate protection of intellectual property rights, and to ensure that measures and procedures to enforce intellectual property rights do not themselves become barriers to legitimate trade.” The Agreement achieves this through substantive protections for intellectual property in §§ 1-7, but also through a most-favored nation clause in Article 3, which requires members to “accord to nationals of other [m]embers treatment no less favourable [sic] than that it accords to its own national with regard to the protection of intellectual property.” Members are able to impose more strict intellectual property protection within their own countries, so long as the minimum standards of the Agreement are met. Signatories are also free to meet the provisions of the Agreement in any way that is consistent with the laws of the implementing country. The Agreement’s real contribution to international intellectual property protection was its enforcement provisions, which provided dispute resolution through a body at the WTO, as well as provisions that allow harmed nationals of member nations to recover remedies for violations of the Agreement.

101 Id.
102 Id. at 10 (describing submission of intellectual property proposals prior to the beginning of the new Round by the United States and Japan).
103 TRIPS Agreement, supra note 19, art. 1.
104 Id. pmbl.
105 TRIPS Agreement, supra note 19, art. 3.
106 Id. art. 1.
107 Id.
108 J.H. Reichman, Enforcing the Enforcement Procedures of the TRIPS Agreement, 37 VA. J. INT’L L. 335, 338-39 (1997) (discussing that the minimum standards of intellectual property protection prior to the TRIPS agreement, and the lack of enforcement procedures that existed for these standards, further pointing out that the minimum standards under TRIPS are “only the starting point” and that the enforcement provisions of TRIPS “put teeth into the pre-existing intellectual property conventions”).
109 GERVAIS, supra note 91, at 27 (“Negotiators . . . then added an entirely new set of rules on enforcement (Part III). There was no precedent for this in the field of intellectual property at the multilateral level . . . The final pieces of the puzzle could then be added, including more precise rules on acquisition (Part IV), and more importantly, provisions bringing TRIPS under the general WTO dispute settlement umbrella, known as the integrated dispute settlement system.”).
While TRIPS does apply to intellectual property rights in general, it does not explicitly mention trade secrets, but rather refers to "Protection of Undisclosed Information." The definition of "undisclosed information" in the Agreement, however, is consistent with the traditional trade secret definition. Article 39, § 2 of the Agreement protects undisclosed information so long as "(1) such information . . . is not generally known; (2) has commercial value because it is secret; and (3) has been subject to reasonable steps . . . by the person lawfully in control of the information to keep it secret." There is also a knowledge requirement in Article 39, § 2 that requires those in possession of undisclosed information to show that the acquirer was in contravention of "honest commercial practices," which is defined in a footnote to "include[] the acquisition of information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition." Because trade secret misappropriation in the United States does not require actual knowledge of the possessor's right to the information for liability to attach, "the . . . concern exists that this may afford a lower level of protection (by raising the degree of culpability required to constitute a violation) than that which is generally provided under U.S. law."

C. International Trade Secret Protection is Lacking

The TRIPS Agreement was an important first step at setting a minimum standard of intellectual property protection for the international community. International recognition of a company's patents, copyrights, and trademarks is necessary for a company that relies on these assets to make investments abroad. While these three categories of intellectual property are adequately addressed and protected in the TRIPS Agreement, protection of trade secrets is highly lacking. "Undisclosed information" is protected under the TRIPS

---

111 TRIPS Agreement, supra note 19, art. 39.
112 Id.
113 Id. art. 39 ¶ 2 n.10.
116 See, e.g., CORREA, supra note 110, at 3 ("Moreover, it was argued that shortcomings in availability and enforcement of IPRs may constitute a barrier to trade, as potential exports by inventors or creators may be prevented or diminished by infringing copies of their products in foreign markets.").
118 See generally CORREA, supra note 110, at 31, 368 (stating that the covered rights under the TRIPS Agreement are sections 1-7, Part II; copyright, trademarks, geographical indications, industrial designs, patents, layout-designs of integrated circuits, and undisclosed
Agreement as an element of protection against unfair competition,\textsuperscript{119} which means that misappropriation of such information is largely demoted from the ranks of "intellectual property."\textsuperscript{120} Therefore, trade secrets "do not give rise to exclusive rights, as in the case of patents or trademarks, but possessors of trade secrets can only act against those who have acquired or used the secret information in a manner contrary to dishonest commercial practices."\textsuperscript{121}

While the TRIPS Agreement does not set an ideal minimum standard of trade secret protection for the international community, the process by which it was ratified does provide a strategic roadmap for implementing international trade secret protection norms.

\textit{1. Enhancing International Trade Secret Protection Norms}

The TRIPS agreement was adopted by WTO member-countries following negotiations of the Uruguay Round of the Multilateral Trade Negotiations in 1994.\textsuperscript{122} It was during that negotiating round, over an eight-year span, that the TRIPS Agreement was hammered out.\textsuperscript{123} Developed countries introduced the first drafts of an intellectual property agenda,\textsuperscript{124} and as it became apparent that some form of intellectual property protection was going to advance, developing countries introduced a proposal to address concerns with the direction of the industrialized countries’ initial draft.\textsuperscript{125} In describing the final version of the TRIPS Agreement, Professor Gervais stated that, “the so-called ‘North’ [had] imposed its then most-advanced set of norms on the ‘South.’ In fact, major

\begin{itemize}
  \item \textsuperscript{119} Id. at 32.
  \item \textsuperscript{120} NUNO PIRES DE CARVALHO, THE TRIPS REGIME OF PATENT RIGHTS 25 (2002) ("Protection of undisclosed information, however, is not designated by the Agreement as an intellectual property field \textit{per se}, but merely as an aspect of protection against unfair competition \ldots").
  \item \textsuperscript{121} CORREA, supra note 110, at 32.
  \item \textsuperscript{122} See generally GERVAIS, supra note 91, at 10-25 (describing the negotiating process of the TRIPS Agreement during the Uruguay Round between 1986 and 1994).
  \item \textsuperscript{123} Id.
  \item \textsuperscript{124} Id. at 10 ("The United States and Japan submitted proposals to the Round’s Preparatory Committee to cover all intellectual property rights and their enforcement, not just trademark goods. Long negotiating sessions co-chaired by Colombia and Switzerland tried to reconcile all proposals but failed to produce consensus.").
  \item \textsuperscript{125} Daniel J. Gervais, \textit{The TRIPS Agreement and the Changing Landscape of International Intellectual Property, in INTELLECTUAL PROPERTY AND TRIPS COMPLIANCE IN CHINA: CHINESE AND EUROPEAN PERSPECTIVES} 65, 67-68 (Paul Torremans, Hailing Shan, Johan Erauw, eds., 2007) [hereinafter \textit{Changing Landscape 2007 ed.}] ("In the first few months of [negotiations], a number of industrialized countries tabled, with little advance notice, draft legal texts of what they saw as the future TRIPS Agreement. \ldots As a reaction, more than a dozen developing countries proposed another ‘legal’ text, much more limited in scope, with few specific normative aspects.").
\end{itemize}
industrialized countries made relatively few concessions."\textsuperscript{126}

Developed countries clearly set the policy agenda put forth by the WTO, with the United States usually leading from the front.\textsuperscript{127} Much like crafting legislation in the United States House or Senate, the more developed member-countries set out an ambitious plan, which then had to be scaled back amid compromise to meet the concerns of developing countries.\textsuperscript{128} While this interaction is often the source of much criticism of the WTO and its policies,\textsuperscript{129} the reality is that the United States can and should utilize the WTO to reach international norms that eliminate cyber attacks targeted at trade secret information.

As noted above, however, while the TRIPS Agreement attempts to harmonize protection for patents, copyrights, and trademarks across national borders, it only provides for a minimal protection of trade secrets.\textsuperscript{130} Furthermore, the TRIPS Agreement is already becoming outdated.\textsuperscript{131} Both developed and less developed countries alike "consider the TRIPS Agreement outdated and ineffective in meeting the new challenges created by the advent of the Internet and new communications technologies."\textsuperscript{132} Forcing developing countries to accept amendments to the TRIPS Agreement that are favorable to developed countries' intellectual property agenda will not come without compromise.\textsuperscript{133} Less developed countries have come to realize the importance of intellectual property protection; a change from the time the TRIPS Agreement was introduced and ratified.\textsuperscript{134} "The bargaining advantage developed countries have over their less developed counterparts is no longer as dominant as it was during the

\textsuperscript{126} Id. at 68.

To protect themselves and to reclaim autonomy over their intellectual property policies, both countries blocs have recently pushed for measures that frustrate the harmonization project. While less developed countries push for the establishment of the development agenda, in the hope of rolling back some of the protection required by the TRIPS Agreement and other international treaties, developed countries use bilateral and plurilateral free trade agreements to pressure their less powerful counterparts to ratchet up intellectual property protection and enforcement.

\textsuperscript{129} Id. at 79 (calling the TRIPS Agreement "coercive" and "imperialistic").
\textsuperscript{130} See supra Part III.C.
\textsuperscript{131} Yu, supra note 128, at 73 ("Notwithstanding these harmonization efforts, countries—both developed and less developed—have become increasingly dissatisfied with the international intellectual property regime.").
\textsuperscript{132} Id. at 73-74.
\textsuperscript{133} Id. at 79-81 ("These days . . . less developed countries have begun to understand the importance of intellectual property protection . . . . It is therefore no surprise that they are now taking a more aggressive collective stance on their demands for more group diversification in the international intellectual property regime.").
\textsuperscript{134} Id. at 81.
TRIPS negotiations.\textsuperscript{135}

In addition, attempts to overhaul TRIPS has met much resistance. Critics have argued that under-developed countries would benefit most by ending harmonization of international intellectual property laws altogether, and instead allowing certain countries or groups of countries to remain “diversified.”\textsuperscript{136} One main argument for ending harmonization of international intellectual property laws is that “an inequitable system that is biased in the intellectual property area forces [less developed countries] to utilize an outdated competition model that frustrates their efforts to catch up with their developed counterparts.”\textsuperscript{137}

Critics believe that by harmonizing intellectual property laws, the WTO is actually freezing out a less developed country’s ability to develop its own intellectual property and laws for its protection.\textsuperscript{138} One prominent academic argues that “[b]ecause [developing countries’] obligation[s] to protect intellectual property arise[] solely out of WTO membership, and not from intrinsic economic conditions, the impact on these countries has been especially severe, raising the cost of end products . . . without providing significant compensatory benefits in the form of new sources of revenue.”\textsuperscript{139}

2. WTO Resolution on Trade Secret Theft Perpetrated through Cyber Attack

For these reasons, the United States and other developed countries should avoid an attempt to extract broad intellectual property concessions. However, no grand, ambitious overhaul of the TRIPS Agreement is necessary to reach consensus on the problem cyber attacks pose for owners of targeted proprietary information.\textsuperscript{140} The WTO can be used as a forum to bring more attention to the growing problem of cyber attacks that target trade secrets across national borders. Agreeing to outlaw such predatory behavior will not act as a burden on

\textsuperscript{135} Id. Yu comments:
These days, however, less developed countries have begun to understand the importance of intellectual property protection, the need to develop a knowledge-based economy, and the adverse spillover effects intellectual property can have on such sectors as agriculture, health, environment, education, culture, free speech, and democracy. Led by such heavyweights as Brazil and India and supported by an emerging player in China, these countries have become more vigilant, organized and sophisticated; they now have a better sense of what they want, and, more importantly, what they do not want.

\textsuperscript{136} Id. at 78.

\textsuperscript{137} Yu, supra note 128, at 80.

\textsuperscript{138} Id.


\textsuperscript{140} Id. at 27.
less developed countries, which will still be able to innovate in a legal way. The United State should take steps to educate less developed countries on why it is in their best interest to bring awareness to the problem of cyber-espionage, and at the same time make clear to all WTO member-countries that trade secret misappropriation via cyber attack will not be tolerated.

To this end, President Obama should instruct the United States Trade Representative to draft language that outlines the scope of the problem of trade secret theft as a result of cyber attacks. The trade representative should then approach other strategically important Member-countries, from both the developed and developing blocs, and form an alliance in support of the measure. After reaching a compromise on the language, the alliance should then introduce a resolution strongly decrying the use of cyber-espionage to target proprietary economic information at the next WTO Ministerial Conference.

IV. THE RISKS OF DOING BUSINESS IN THE DIGITAL AGE: GOOGLE AS A CASE STUDY

The recently perpetrated cyber attack on Google is the most publicized and most brazen attack on a domestic corporation to date. This attack demonstrates the ever evolving threat that cyber-espionage poses to domestic corporations. The seriousness of the threat only becomes more apparent as we learn more about the methods of the foreign hackers. Google took the unusual step of widely publicizing the attack because of its belief that the Chinese government was involved. After uncovering the attack and tracing its origin to China, Google threatened to remove its search engine from the Chinese market.

\[\text{See discussion infra Part IV.}\]

\[\text{See, e.g., James T. Areddy,} \text{ People's Republic of Hacking,} \text{ WALL ST. J.,} \text{ Feb. 20, 2010, at A1 ("In China's hacking community, each person does a specific job and, rather than working for a big score, gets paid piecemeal by selling his work, cybersecurity experts say.").}\]

\[\text{The Official Google Blog,} \text{ A New Approach to China,} \text{ http://googleblog.blogspot.com (Jan. 12, 2010, 15:00 EST) ("We have taken the unusual step of sharing information about these attacks with a broad audience not just because of the security and human rights implications of what we have unearthed, but also because this information goes to the heart of a much bigger global debate about freedom of speech."); see also, Chris Carr & Larry Gorman,} \text{ The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act,} \text{ 57 BUS. LAW. 25, 30 (2001) (describing reasons why companies are reluctant to publicize cyber attacks).}\]

\[\text{Andrew Jacobs, Miguel Helft & John Markoff,} \text{ Google May End Venture in China}\]
After months of negotiations with the Chinese government, \(^{146}\) Google had “closed its Internet search service [in China] and began directing users in that country to its uncensored search engine in Hong Kong.” \(^{147}\) Recently, China and Google reached a compromise to renew Google’s license in China. \(^{148}\) The renewal was a result of Google’s decision to stop redirecting users to its Hong Kong-based site. \(^{149}\)

The saga is not over. Just two weeks after Google’s license was renewed, it reported that its search engine had been blocked in China, though it turned out to be a false alarm. \(^{150}\) No matter the end result of the Google-China conflict, Congress and the Administration must act quickly to prevent future stand-offs between domestic corporations and foreign countries.

A. An Alarming Pattern

As details emerge about the attack on Google, the strategy of foreign hackers is becoming more apparent. \(^{151}\) Those committing cyber-espionage are generally not individuals working for their own benefit, or even groups of rogue hackers combining their efforts. \(^{152}\) Cyber-espionage is being heavily coordinated and carried out by and on behalf of foreign countries. \(^{153}\) These attacks

---

\(^{146}\) DiColo, supra note 142 (“Google said two months ago it would stop self-censoring its Chinese search engine and may shutter its offices in China following a major cyber-attack the company said it traced back to the country. The U.S. based search giant has offered few details on the progress of talks between it and Chinese officials.”).


\(^{149}\) Id. (“But last week, with its license to operate in China set to expire, Google announced that it was no longer automatically sending its Chinese users to the Hong Kong site. In what was seen by industry experts as a compromise to appease China, users going to Google.cn instead received a page that allowed them to go to the Hong Kong site by clicking on a link if they wished.”).


\(^{151}\) Eunjung Cha & Nakashima, supra note 142 (“This is a big espionage program aimed at getting high-tech information and politically sensitive information—the high-tech information to jump-start China’s economy and the political information to ensure the survival of the regime,’ said James A. Lewis, a cyber and national security expert at the Center for Strategic and International Studies. ‘This is what China’s leadership is after. This reflects China’s national priorities.’”).

\(^{152}\) Id.

\(^{153}\) Id. See also John Markoff & David Barboza, Researchers Trace Data Theft to Intrud-
narrowly target some of the most well respected corporations in the United States in an attempt to gain proprietary information to be used for the economic benefit of foreign governments.\textsuperscript{154}

Google first described the attack in a post on its official blog: "In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property."\textsuperscript{155} The attacks also "may have succeeded in penetrating elaborate computer security systems and obtaining crucial corporate data and software source codes."\textsuperscript{156}

In the wake of the attack on Google, at least 34 other American companies had discovered they were the victims of a similar cyber attack.\textsuperscript{157} Revealing China’s motive for such attacks, security experts described how the "[t]he recent attacks seem to have targeted companies in strategic industries in which China is lagging."\textsuperscript{158} Another expert described the specific industries being targeted: "[t]he attacks on defense companies were aimed at gaining information on weapons systems . . . while those on tech firms sought valuable source code that powers software applications—the firms’ bread and butter."\textsuperscript{159} These attacks provide a very real-time example of the dangers of cyber-espionage.

Prior to the attack, Google maintained just a 30 percent market share of the Chinese market for Internet searches.\textsuperscript{160} The market leader in China is a Chi-
nese company called Baidu.\textsuperscript{161} However, Google has only been doing business in China since 2006.\textsuperscript{162} There are approximately 400 million Chinese citizens who use the Internet,\textsuperscript{163} with more than sixty percent of Internet users under the age of 30.\textsuperscript{164} Google's business in China accounted for more than $300 million, which made up only a very small fraction of its annual revenue.\textsuperscript{165} Prior to this incident, Google's potential for growth in China, was virtually exponential.\textsuperscript{166} One venture capitalist expressed his surprise at Google's decision, explaining that "Google has Microsoft on the ropes, and China is arguably the world's most important market outside of the U.S. You don't walk away from that on principle."\textsuperscript{167} Google's decision to pull out of China will have influential effects on other American companies that conduct business in China and in other foreign countries.\textsuperscript{168}

B. A Public-Private Solution

In the aftermath of the cyber attack on Google, U.S. government officials investigating the attack have traced its origin to servers located at a prestigious technical school in China, known for its students' prowess in computer science.\textsuperscript{169} This school also has close ties to Baidu, Google's rival in China, and was founded in part through funds from the Chinese government.\textsuperscript{170} China appears to be closely linked to the origins of this attack.\textsuperscript{171} However, if the Chi-

\textsuperscript{161} Jacobs, Helft & Markoff, supra note 156.
\textsuperscript{162} Id.
\textsuperscript{163} Id.
\textsuperscript{164} David Barboza, China's Booming Internet Giants May Be Stuck There, N.Y. Times, Mar. 24, 2010, at B1.
\textsuperscript{165} Jacobs, Helft & Markoff, supra note 156; see also Google, Inc., Annual Report (Form 10-K) 35 (Feb. 12, 2010) (describing 2009 annual revenue as $23,650,563,000).
\textsuperscript{168} James G. Lakely, China's Cyberattack on Google Rattles Techs, Info Tech & Telecom News, Apr. 2010, at 1 ("Google's experience in China raises questions about what a Western company's expectations should be when it decides to do business in a closed and controlling society . . . . Even agreeing to play by a host country's rules, Google learned, doesn't guarantee the government will hold up its side of the bargain.").
\textsuperscript{170} Id. (One of the schools involved "is a huge vocational school that was established with military support and trains some computer scientists for the military. The school's computer network is operated by a company with close ties to Baidu, the dominant search engine in China and a rival of Google.").
\textsuperscript{171} See, e.g., Ellen Nakashima, Diverse Group of Chinese Hackers wrote code in Attacks
nese government does not allow more information to be released from the technical schools, the government’s role in the attacks may never be verified. This lack of access is undoubtedly one of the inherent difficulties of effectively responding to acts of cyber-espionage. Unlike traditional acts of warfare, the perpetrators of cyber attacks are not readily identifiable. Advanced cyber-criminals are able to mask the identity of their attack so that it appears to launch from an Internet connection or server that is many thousands of miles away from the actual launch site.

The National Security Agency (NSA) is currently working with Google to investigate these cyber attacks. Though this relationship is a controversial one because of NSA’s past domestic surveillance activities, the agency’s expertise in this area can be extremely helpful in detecting the source of the attacks and advising Google on prudent next steps. One expert noted that “[t]here are clear benefits to both Google and to NSA of this kind of cooperation. Google can use information from NSA to bolster its computer security, and NSA can use Google’s information to fill out their understanding of the evolving threat to computer security.”

In many cases, it is imperative that federal officials and private stakeholders get an accurate picture of exactly where these attacks originate from. Though there is a rough idea as to which countries are currently undertaking the most voluminous and highly technical attacks, more granular data will help Con-

---


174 Vacellaro & Worthen, *supra* note 172 (“Even if computers at the schools were involved, security professionals point out, they may have been used as intermediaries for attacks that began elsewhere.”); see also, Nakashima, *supra* note 171 (quoting a cyber-forensics expert that “hackers in China routinely direct their attacks through a series of constantly changing Internet protocol addresses [in order to] ‘maintain a foothold on targets’ networks but also to try to bury where they’re coming from.’”).


178 Gorman & Vacellaro, *supra* note 175.

gress and the Administration understand the threats of cyber-espionage and which offenders are repeatedly targeting trade secrets from domestic companies. Private firms will also be empowered to focus on protecting certain kinds of information more intensely depending on the frequency of attack and the propensity of a country to target a certain category of information or that of a specific industry. Patterns only emerge between attacks if there are other recorded instances and characteristics of hacking incidents with which to compare.

The partnership between Google and NSA is one that must be replicated as new and more advanced attacks are launched against U.S. firms. In this instance of a very targeted attack on one of the most blue chip companies in the country, however, NSA officials “had only heard rumors about the Google attack before the company announced it publicly.” Once Google did contact NSA officials, they “had to draft a legal agreement to begin sharing information with Google.”

The NSA recently acknowledged an extensive partnership between federal agencies and the private sector nicknamed “Private Citizen.” While information on this secret program is scarce, it appears to be a formal replication of the Google partnership. Initially, only networks that power critical infrastructure will benefit from the NSA’s capabilities and resources.

As former Director of National Intelligence Mike McConnell recently noted, [t]he NSA is the only agency in the United States with the legal authority, oversight

---


184 Gorman & Vascellaro, *supra* note 175.

185 Id.


187 Id. (“An NSA spokeswoman said the agency had no information to provide on the program. A Raytheon spokesman declined to comment.”).

188 Id. (“The surveillance by the National Security Agency, the government’s chief eavesdropping agency, would rely on a set of sensors deployed in computer networks for critical infrastructure that would be triggered by unusual activity suggesting an impending cyber attack, though it wouldn’t persistently monitor the whole system . . . .”).
and budget dedicated to breaking the codes and understanding the capabilities and intentions of political enemies. The challenge is to shape an effective partnership with the private sector so information can move quickly back and forth from public to private — and classified to unclassified — to protect the nation’s critical infrastructure.\(^{189}\)

The nation’s economic future, however, relies on a much broader range of companies, going beyond the likes of Google and public utilities. Moving forward, American companies must have more concrete information about the role of the federal government and what to expect from its officials when they have become the victim of cyber attacks that target proprietary information.\(^{190}\) Such certainty should extend to each American company no matter its size or sector.

V. LEGISLATIVE AND ADMINISTRATIVE SOLUTIONS

This section proposes a strategy Congress and the President should employ that will help stem the flow of misappropriated proprietary information from domestic corporations to foreign countries and individuals through the use of cyber-espionage.

Congress must pass new legislation that accomplishes what the EEA has proved incapable of doing. The problem of cyber-espionage, whether economic or industrial, is too complex a problem at this time to be individually prosecuted through a single federal criminal statute. The aims of criminal law, such as deterrence and retribution,\(^ {191}\) are unattainable when it is nearly impossible to investigate and assign blame to an actor using traditional criminal law formulas.\(^ {192}\) Congress must take action to empower the Administration to develop policies that will better protect trade secret information of private firms. Congress should also require the federal government to formulate a framework for working with domestic victims of cyber-espionage. Private companies require assurance that the government will respond rapidly and uniformly to cy-

---


\(^{192}\) See, e.g., *NATIONAL ACADEMY OF SCIENCES, LETTER REPORT FROM THE COMMITTEE ON DESECRETING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY* 5 (2010). The Report notes:

Traditionally, law enforcement action serve two purposes. First, when successful, they remove such perpetrators from conducting further hostile action, at least for a period of time. Second, the punishment imposed on perpetrators is intended to dissuade other possible perpetrators from conducting similar actions. However, neither of these purposes can be served if the cyberattacks in question cannot be attributed to specific perpetrators.

*Id.*
ber attacks while keeping all proprietary company information confidential. Once a framework is in place, companies eventually must be more forcefully encouraged to report instances of cyber attacks that target proprietary economic information.

A. Federal Legislation

The EEA is simply out of date. When drafted, the technological capabilities of those wishing to misappropriate trade secrets were minimal. Trade secret theft resembled traditional crime, which required physical proximity to the targeted firm. The proliferation of Internet networks no longer makes trade secret theft so labor intensive. While the intentions of the EEA are noble, the means to carry out its mission must be updated to take into account the exponential expansion of technology that has taken place over the past decade. A criminal statute is not the answer at this time. Congress must first orient the federal government to the problem by passing legislation that emphasizes the issue, and enables the Executive branch to take a lead role in developing the general framework. Simply put, the new legislation must provide the private sector some certainty as to the government's role and response to cyber-espionage.

In the wake of the very public Google attack, Congress has produced several pieces of legislation aimed at protecting and preventing the nation's cyber systems. Senators Rockefeller and Snowe have introduced the Cybersecurity Act of 2009, and the National Cybersecurity Advisor Act, which comprise the Rockefeller-Snowe cybersecurity legislation. Additionally, the Protecting Cyberspace as National Asset, the International Cybercrime Reporting and Cooperation Act, and the Fostering a Global Response to Cyber Attacks Act have all been introduced in either the House or Senate, or have had similar versions introduced in both chambers. Collectively, these proposals con-

195 See discussion supra Part II.
196 Rustad, supra note 193, at 479, 490.
198 Id.
201 S. 1438, 111th Cong. (2010).
tribute to the dialogue necessary for meaningful change to take place. Senator Lieberman's Protecting Cyberspace as a National Asset Act ("PCNAA"), however, is the most comprehensive and was recently approved by the Senate Committee on Homeland Security and Governmental Affairs.\footnote{New Protecting Cyberspace as a National Asset Act (PCNAA) Bill Could Give President Obama Kill Switch to Shut Down the Internet, IT PROFESSIONAL SERVICES (Mar. 18, 2010), http://www.itprofessionalservices.net/PCNAA.shtml.} It provides the Administration with a roadmap of necessary changes, even if the bill is too ambitious for some in Congress.\footnote{Declan McCullagh, Senators propose granting president emergency Internet power, CNET.com, June 10, 2010, http://news.cnet.com/8301-13578_3-20007418-38.html. McCullagh writes: Because there are few limits on the president's emergency power, which can be renewed indefinitely, the densely worded 197-page bill is likely to encounter stiff opposition. TechAmerica, probably the largest U.S. technology lobby group, said it was concerned about 'unintended consequences that would result from the legislation's regulatory approach' and the 'potential for absolute power.'\footnote{Id.}}

B. High Level Advisor

In his presidential campaign, Senator Barack Obama took the unusual step of dedicating nearly an entire campaign speech to the topic of cyber security.\footnote{Senator Barack Obama, Remarks at Purdue University's Summit on Confronting New Threats (July 16, 2008) (transcript available at http://www.barackobama.com/2008/07/16/remarks_of_senator_barack_obam_95.php).} On July 16, 2008, then-Senator Obama said that, as president, he would "make cybersecurity the top priority that it should be in the 21st century."\footnote{Id.} He went on to promise that he would "declare cyber-infrastructure a strategic asset, and appoint a National Cyber Advisor who will report directly to me."\footnote{Id.} Presently, President Obama has only fulfilled one of these promises, by declaring the nation's cyber infrastructure "a strategic national asset."\footnote{Id.} However, while he has created the position of National Cyber Security Coordinator, that individual does not report directly to the president, but to both heads of two separate presidential advisory committees, the National Economic Council and National Security Council.\footnote{Id. This bifurcation is redundant and confusing.}

Cyber-Espionage: Threat to the American Economy

Senator Lieberman’s PCNAA aims to remedy this problem “by establishing an Office of Cyberspace Policy within the Executive Office of the President.”\(^{209}\) The Director of this office requires Senate confirmation and would report directly to the president.\(^{210}\) A review of President Obama’s actions as president, not as candidate, makes clear why a separate advisory office within the Executive Office of the President is necessary to carry out any serious policy initiatives with respect to cybersecurity.

After President Obama’s initial focus on the broad issue of cybersecurity in January 2008, his focus moved to other topics.\(^{211}\) The president initiated a 60-day review of the nation’s cybersecurity policies by soliciting formal recommendations from a panel of experts led by a member of the National Security Council, Melissa Hathaway.\(^{212}\) After the panel’s report was released in May 2009,\(^{213}\) Obama retained Hathaway to be the acting National Cyber Security Coordinator.\(^{214}\) However, after only about six months in office, Hathaway abruptly resigned, signaling her displeasure and lack of influence.\(^{215}\) Instead of moving quickly to replace her in an effort to appear committed to the nation’s cybersecurity agenda, President Obama failed to permanently fill the cyber czar position until December 2009.\(^{216}\) Over the ten-month period from the president’s announcement of the National Cyber Security Coordinator position in a major policy speech, the position was filled on an interim basis for five months and left vacant for another five months.\(^{217}\)

---

\(^{209}\) S. 3480, 111th Cong. § 101 (2010).

\(^{210}\) Id. § 102.

\(^{211}\) See Address to Joint Session of Congress, 2009 DAILY COMP. PRES. DOC. 1 (Feb. 24, 2009) (“I know that for many Americans watching right now, the state of our economy is a concern that rises above all others, and rightly so.”).


\(^{213}\) Remarks on Securing the Nation’s Information and Communications Infrastructure, 2009 DAILY COMP. PRES. DOC. 3 (May 29, 2009).

\(^{214}\) Siobhan Gorman, Security Cyber Czar Steps Down, WALL ST. J., Aug. 4, 2009 at A4 (“Ms. Hathaway had initially been considered a leading contender to fill the cyber post permanently.”).


\(^{216}\) See Greenberg, supra note 208 (reporting how “after 10 months of delays, President Obama has finally chosen a cybersecurity coordinator, filling the so-called ‘cyber czar’ position he had long promised to create to shore up the nation’s defenses against hackers and cyberspies.”).

\(^{217}\) Id.; Siobhan Gorman, Cybersecurity Chief Quits, WALL ST. J., Aug. 4, 2009, at A4; Congress Pressures Obama to Pick Cybersecurity Coordinator, DIGITAL TRENDS (Nov. 3,
tion’s lack of influence on the president’s agenda, a number of top candidates had turned down the job. Finally, Howard Schmidt, a former security official at e-Bay and in George W. Bush’s Administration, accepted the White House’s offer in December 2009.

Mr. Schmidt’s made his first major policy speech on March 2, 2010 at a conference on cybersecurity issues held in San Francisco. In that speech, he announced the public release of the Comprehensive National Cybersecurity Initiative’s (CNCI) 12 initiatives to protect the federal government from cyber attacks. The rapid pace of technological innovation makes time of critical importance, and this period of delay for the Administration’s top cybersecurity official to take substantive public action is simply unacceptable.

Though President Obama initially set forth on a cybersecurity agenda, 2009 was a lost year in terms of making any real progress, with key Administration officials unable to interact with industry leaders because the Administration lacked key officials. The Administration needs to regain a laser focus on cyber security, especially in these dark economic times. The issue of cyber-espionage is too critical and has only added to the uncertainty confronting the country during this economic downturn. The Lieberman requirement that the nation’s top cybersecurity official be made a part of the president’s Cabinet with the advice and consent of the Senate gives the official the authority needed to

218 Andy Greenberg, Obama’s Unwilling Cyber Czars, FORBES.COM (Jul. 20, 2009), http://www.forbes.com/2009/07/20/cybersecurity-obama-economy-technology-security-cybersecurity.html (“One reason that the czarship has remained unfilled for the six months since Obama has taken office . . . may be that the position has taken a back seat to another issue: the economy.”); Lolita C. Baldor, Howard A. Schmidt Tapped to Be Obama’s Cybersecurity Czar, HUFFINGTON POST (Dec. 21, 2009 11:35PM), http://www.huffingtonpost.com/2009/12/21/howard-a-schmidt-tapped-t n 400112.html (“Rather than being a cyber czar, the person will be more of a ‘cyber peasant’ . . . it’s not a top tier position, not someone who reports directly to the president.”).

219 Id. ("The declassified version [of the CNCI] posted Tuesday contains slightly more descriptive material [than the unclassified version], such as acknowledging officially for the first time the role of the National Security Agency in one monitoring program.")

220 Id. ("The declassified version [of the CNCI] posted Tuesday contains slightly more descriptive material [than the unclassified version], such as acknowledging officially for the first time the role of the National Security Agency in one monitoring program.")
make a real impact on the Administration’s treatment of this critical issue.

C. Encouraging Increased Reporting

The Lieberman legislation calls for much-needed improvement on the part of the federal government when it comes to protecting the nation’s cyber security. In addition to the Office of Cyberspace Policy, it introduces a National Center for Cybersecurity and Communications (“NCCO”), housed within the Department of Homeland Security.223 An owner of “covered” private infrastructure is required to report “any incident affecting the information infrastructure of covered critical infrastructure to the extent the incident might indicate an actual or potential cyber vulnerability, or exploitation of a cyber vulnerability.”224

Application of this very general standard to only “covered” infrastructure, which is merely a list of worthy networks chosen by the Secretary of Homeland Security,225 will not prevent the continuous flow of information from this country into the hands of cyber attackers. The proposal falls short in failing to encourage private firms of all shapes and sizes to report cyber attacks that appear to target their proprietary economic information.

There are various other disincentives for firms to report security breaches, which only exacerabtes the problem. Generally, companies are reluctant to make public announcements regarding breaches of security that result in proprietary information being compromised. Testifying at a hearing on the effects of economic and industrial espionage and a review of the EEA in 2000, the then-Deputy Assistant Director of the FBI’s Counter Intelligence Division relayed to Congress the Bureau’s experience working with private firms by saying “that industry and business are somewhat loathe and reticent in engaging with us...”226

When asked how the FBI initiated investigations of EEA violations, she explained that companies were often “reluctant to come to the Federal Government and the Federal Bureau of Investigation” because “they do not want their trade secrets to be aired.”227 They do not want their shareholders to know there are problems in the company. These kinds of bottom line issues are very difficult to overcome when a company comes and finds out information [about a security breach targeting proprietary information].”228

---

223 S. 3480, tit. II.
224 S. 3480, 111th Cong. § 246(c)(1)(A) (2010).
225 See id. § 241(4).
226 House Hearing, supra note 13, at 7 (testimony of Shiela Horan, Deputy Assistant Dir. on Counter Intelligence, Fed. Bureau of Investigation).
227 Id. at 9.
228 Id.
There are various disincentives for firms to report breaches to the government or the public. Studies have revealed the negative impact on reports of cybersecurity breaches on a company's stock price. Larger companies that are able to detect breaches in their network and conduct their own investigations often fear losing control of the matter. An expert described how private companies desire to "control the investigation, decide how many resources to put toward it... whereas when you report it to law enforcement then the subpoenas come and other kinds of compulsory process, and you have to go forward." Though private firms should be encouraged to devote resources to detect and investigate instances of electronic breaches from cyber attack, once confirmed, there must be a formal mechanism for reporting a breach to the government so that the processes put in place to respond to and contain such an attack can be effectively coordinated.

Currently, most studies that report losses attributable to cyber attacks are framed as estimates, especially when converting these losses to a dollar value. Such estimates do not provide an exact picture of the problem. Additionally, firms are reluctant to provide such information, which can be critical to convincing Congress to direct more resources to its cause, even when the study is undertaken anonymously.

Reporting instances of cyber attacks will also provide the government with data streams that it can use to more effectively analyze and respond to such attacks. By having a more complete picture of the problem, the government's top cybersecurity officials will be better able to formulate a uniform process dependent on the size and type of attack, the information targeted, and other relevant factors. Much like an automobile crash site investigator is able to more accurately reconstruct a crash sequence as his experience at varying scenes grows, so too will federal officials be better able to identify the nature and scope of cyber attacks and how they can be best contained.

In its recommendations on Securing Cyberspace for the 44th Presidency, the Center for Strategic and International Studies Commission on Cybersecurity

---

229 See Carr & Gorman, supra, note 145 at 52; see also id. at 26-27 (discussing studies conducted by the American Society for Industrial Security, PriceWaterhouseCoopers, and the Federal Bureau of Investigation).

230 House Hearing, supra note 13, at 14 (statement of Scott Charney, Partner, PriceWaterhouseCoopers).

231 Id.

232 AMERICAN SOCIETY FOR INDUSTRIAL SECURITY, TRENDS IN PROPRIETARY INFORMATION LOSS 25 (2007) ("Because of an insufficient number of responses to this question, the survey team was unable to estimate losses... Among the possible reasons contributing to the low number of responses are:... Respondent is reluctant to provide this data.").

233 AMERICAN SOCIETY FOR INDUSTRIAL SECURITY, TRENDS IN PROPRIETARY INFORMATION LOSS 6 (2007).

234 See supra Part IV.B.
for the 44th Presidency proposed the creation of a Center for Cybersecurity Operations (CCSO). This proposed non-profit organization comprised of public and private sector representatives was envisioned as a forum where "public and private sector entities can collaborate and share information on critical cybersecurity matters in a trusted environment." This type of independent organization could provide private companies with a secure place to report cyber attacks without fear of losing control of the investigation and without the risk of revealing trade secrets. At the same time, it would provide government with vital information on cyber attacks. Companies could have some discretion in whether to report the matter to the FBI for investigation, but regardless of the law enforcement outcome, the organization would facilitate awareness of the critical characteristics of the attack. As more companies realized the benefits of the information gleaned through reporting and also spread more specific information, the CCSO could formulate best practices and make recommendations to Congress on the dangers cyber attacks pose to private industry.

In addition, as the CCSO became more adept at classifying attacks, it could refer extremely serious cases directly to the NSA and the NCCO. A more nimble CCSO would nicely complement the more macro-focused NCCO. This would allow NSA resources to be devoted only to the most egregious attacks, or attacks on companies in strategically important industries, such as defense, where the origin of the attacks is of great concern.

VI. CONCLUSION

Private firms in the United States thrive on making large initial investments of time and capital to develop information, formulas, designs, and products that enable them to subsequently recover the outlays in the marketplace. Firms will only be willing to take the risks associated with developing such proprietary information if they know that none of their competitors will be able to easily duplicate their efforts with a few strokes of the key.

---

236 Id. at 47.
237 Id. at 47-48.
238 See id. at 48.
239 Id.; see McConnell, supra note 177. See generally S. 3480, 111th Cong. tit. II.
240 House Hearing, supra note 13, at 185 (“The United States produces the majority of the world’s intellectual property capital, including patented inventions, copyrighted material and proprietary economic information factor in the incredible ingenuity and inventiveness of the American worker, and one can easily see why [economic and industrial espionage] is so pronounced in the American workplace”).
241 House Hearing, supra note 13, at 33; see McConnell, supra note 177.
While policy makers and industry executives have acknowledged the need for public-private cooperation in various cyber security proposals,\textsuperscript{242} the need for such coordination is especially present where proprietary information and intellectual property of private companies are uniquely at risk,\textsuperscript{243} yet such companies do not possess the information or technical tools to adequately combat the problem. The problem is much too critical to allow individual firms to continue to unknowingly contribute to the growing drain on the nation’s proprietary information by simply ignoring the threat of cyber-espionage. The federal government must take on a crucial leadership role in protecting the trade secrets of the nation’s private companies.

This role can be distilled into three action items. First, Congress must pass legislation that specifically details the scope of the cyber-espionage problem, and creates a framework for private companies to safely report information breaches to the government. Once the reporting framework is in place, federal officials will then be better positioned to determine which threats require a strategic partnership with government experts, as well as the amount of resources that need to be devoted to combating cyber-espionage.

Concurrently, the President should not wait for Congress to promote his National Cyber Security Advisor to a cabinet level position. President Obama should stand behind his commitment to treat the national cyber-infrastructure as a national asset, and give his advisor the stature necessary to make serious recommendations and decisions without having to answer to two separate advisory councils. Howard Schmidt possesses the necessary experience and innovative thinking to perform the job well. However, he should no longer be limited by the confines of his relegated position within the Obama Administration.

Finally, the President should instruct the United States Trade Representative to engage strategic allies to coauthor a resolution decrying the use of cyber attacks to misappropriate proprietary economic information. There are many countries in both the developed and developing blocs that have much to lose through cyber-espionage attacks, and using the WTO as a vehicle to navigate change on intellectual property protection has been successful in the past.

These three actions will serve to realign the American view of the ongoing threat of cyber-espionage, helping to match the intensity with which this country’s enemies seek to undermine the American economy. They will also ensure that the American ideal, which encourages its citizens to achieve success


through hard work and innovation, not deception and fraud, can once again be an attainable goal.