

# Trade Secrecy as an Instrument of National Security? Rethinking the Foundations of Economic Espionage

Aaron J. Burstein\*

## Abstract

Economic espionage—the misappropriation of trade secrets to benefit a foreign government—is rightly regarded as a national security problem. The national security dimension of trade secret misappropriation arises through an externality. To maintain their rights under trade secret law, trade secret holders must take reasonable measures to protect their secrets; but these measures may not extend to protecting information from highly sophisticated adversaries who wish to use it in markets that the owner has no interest in entering. To individual trade secret holders, such misappropriations may not register as much of a loss. Repeated over time and in strategically important industries, however, state-coordinated use of misappropriated trade secrets may facilitate the cheap and rapid development of infrastructure to such an extent that it alters U.S. technological advantages and economic security. Unlike traditional espionage, there are effectively no internationally observed legal or normative constraints on economic espionage.

The U.S. response to this problem has been a mixture of law enforcement, based on the economic espionage statute, and counterintelligence. Despite a handful of prosecutions and some evidence of coordination among law enforcement and intelligence agencies, there are few signs that the United States has developed an effective response to protecting the national security interest in trade secrets.

This article argues that this failure is due to policymakers' neglect of the basic, intertwined domestic and international elements of economic espionage. Domestically, a combination of statutory reform and administrative efforts could encourage trade secret holders to invest in more effective information security measures as well as the sharing of threat information between trade secret holders and the government. But these efforts are likely to be futile without international norms that discourage economic espionage. Appealing to parallels between traditional and economic espionage, this article argues that informal diplomatic efforts could be helpful in managing economic espionage risks.

---

\* TRUST and ACCURATE Research Fellow, University of California, Berkeley, School of Information. E-mail: aaron.burstein@gmail.com. I thank John Chuang, Barry Horowitz, Maryanne McCormick, Shari Lawrence Pfleeger, and Fred Schneider for helpful discussions. I am grateful to Will DeVries, Joseph Lorenzo Hall, Corinne Keet, Dave Levine, and Deirdre Mulligan for reviewing drafts of this Article. Augustín Núñez and Chien-Min Yang provided outstanding research assistance. This Article is based in part upon work supported by a grant from the U.S. Department of Homeland Security, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

<b>I. INTRODUCTION.....</b>	<b>3</b>
<b>II. THE EVOLUTION OF ESPIONAGE—ECONOMIC AND OTHERWISE .....</b>	<b>8</b>
A. INFORMATION TRADITIONALLY PROTECTED ON NATIONAL SECURITY GROUNDS.....	8
B. THE POST-COLD WAR EXPANSION OF ESPIONAGE.....	9
1. <i>Geopolitical Change</i> .....	10
2. <i>Technological Change</i> .....	12
C. WHY ECONOMIC ESPIONAGE IS A NATIONAL SECURITY PROBLEM: EXTERNALIZATION OF LOSSES .....	15
<b>III. LEGAL RESPONSES TO ESPIONAGE: THE NATIONAL SECURITY CONTEXT FOR THE ECONOMIC ESPIONAGE STATUTE.....</b>	<b>19</b>
A. DIPLOMACY AND THE INTERNATIONAL LAW OF ESPIONAGE.....	20
B. DOMESTIC REGULATION OF INFORMATION DISCLOSURES BASED ON NATIONAL SECURITY CONCERNS .....	21
1. <i>Classification</i> .....	21
2. <i>Export Controls</i> .....	25
3. <i>Corporate Governance Controls</i> .....	27
4. <i>Legally “Hardening” Government Information</i> .....	29
<b>IV. NOT KNOWING YOUR ENEMY: HOW THE ECONOMIC ESPIONAGE STATUTE FAILS TO ADVANCE NATIONAL SECURITY GOALS .....</b>	<b>31</b>
A. THE INCOMPATIBLE GOALS AND STRUCTURE OF REGULATIONS PROTECTING TRADE SECRETS AND NATIONAL SECURITY INFORMATION .....	32
1. <i>Mechanisms for Trade Secret Protection</i> .....	33
2. <i>Rationales for Trade Secrecy</i> .....	35
B. THE CURIOUSLY NARROW ENFORCEMENT HISTORY .....	41
C. COMPLACENT OVERSIGHT BY CONGRESS .....	46
D. STUNTED UNDERSTANDING OF ECONOMIC ESPIONAGE THREATS .....	47
1. <i>A Hypothetical</i> .....	48
2. <i>Reassessing the Chinese Economic Espionage Threat</i> .....	49
<b>V. TOWARD BETTER MECHANISMS FOR DISCOURAGING ECONOMIC ESPIONAGE .....</b>	<b>52</b>
A. TWO WAYS TO AMEND THE ECONOMIC ESPIONAGE STATUTE.....	54
1. <i>Strengthening the Economic Espionage Statute</i> .....	54
2. <i>Changing Trade Secret Holders’ Incentives to Invest in Information Security</i> .....	56
B. IMPROVING THE UNDERSTANDING OF ECONOMIC ESPIONAGE THREATS THROUGH PUBLIC-PRIVATE COOPERATION .....	58
C. CONSTRAINING CONDUCT THROUGH DIPLOMACY .....	61
<b>VI. CONCLUSION.....</b>	<b>65</b>

## I. Introduction

For a law that is seldom enforced, the federal statute prohibiting economic espionage (18 U.S.C. § 1831) would seem to have a lot of work to do. More than a dozen years after going into effect, the statute has resulted in six indictments and two convictions.

Yet economic espionage widely cited as an urgent problem. For example, President Obama's initial homeland security agenda stated that "[i]nnovations in software, engineering, pharmaceuticals and other fields are being stolen online from U.S. businesses at an alarming rate" and stated that the new administration would "[w]ork with industry to develop the systems necessary to protect our nation's trade secrets and our research and development."<sup>1</sup> Recent intelligence community reports deem economic espionage an "unrelenting threat,"<sup>2</sup> as foreign attackers seek to run a "vacuum" over critical U.S. industries to collect information from them.<sup>3</sup> Other reports link economic espionage not only to economic losses for U.S. companies but also to providing other nations with "the ideas to arm themselves and achieve parity" with the technological capabilities of the United States.<sup>4</sup>

Economic espionage also serves as an exhibit in arguments calling for potentially far-reaching plans to revise authorities and reorganize the government to address the dismal state of U.S. cybersecurity. A review of cybersecurity policy ordered by President Obama states that "a growing array of state and non-state actors are compromising, stealing, changing, or destroying

---

<sup>1</sup> [http://www.whitehouse.gov/agenda/homeland\\_security/](http://www.whitehouse.gov/agenda/homeland_security/) (viewed Jan. 20, 2009).

<sup>2</sup> Office of the National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage FY07 1* (2007). This report is commonly abbreviated as "FECIE." I adopt this convention, and throughout this paper, I refer to a given year's report as "FECIE [year]." Hence, the 2007 report cited here is "FECIE 2007."

<sup>3</sup> FECIE 2005 at v.

<sup>4</sup> Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency* 13 (Dec. 2008), at [http://www.csis.org/component/option,com\\_csis\\_pubs/task,view/id,5157/](http://www.csis.org/component/option,com_csis_pubs/task,view/id,5157/)

information” that is of value to U.S. firms.<sup>5</sup> Pending federal legislation asserts that “industrial espionage that exploits weak cybersecurity dilutes our investment in innovation while subsidizing the research and development of our foreign competitors.”<sup>6</sup>

The dearth of economic espionage prosecutions is therefore a puzzle that warrants solving. This puzzle is actually far older than the recent attention to economic espionage acknowledges; the perceptions that anything goes and no one is accountable on the Internet have been around since it became a popular communications medium. In 1996, for example, Senator Leahy gave a statement in support of the EEA that echoes the current debate:

We all know what to do when we hear about somebody who pulls up in a car, rushes into a bank, guns blazing, robs the bank and takes off. And we think of the 20 to 30 to 40 thousand dollars that they might have gotten in that kind of an episode. I think we have to be far more worried about the 200, 300, 400 million dollars [in damage] that may be done at 3:00 in the morning by tapping computer keys.<sup>7</sup>

The Economic Espionage Act was supposed to address such misappropriations, and not just in the cyber realm. Specifically, the economic espionage statute made it a federal crime to misappropriate a trade secret with the knowledge that the theft will benefit a foreign government,

---

<sup>5</sup> *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* iii (2009).

<sup>6</sup> Cybersecurity Act of 2009, S. 773, 111th Cong., § 2(2) (2009).

<sup>7</sup> Senate Judiciary Committee, Feb. 1996 hearing. The most obvious sign of this statement’s age is in the estimate of losses from economic espionage. More recent figures are approximately 1000 times greater. Later in the Article I provide reasons to regard these numbers with great suspicion.

agent, or instrumentality.<sup>8</sup> Thus, the prohibitions are both technology-neutral and generic, in the sense that they apply to any trade secret, irrespective of whether disclosure would pose an immediate harm to national security interests.<sup>9</sup> Thus, at least as a formal matter, the EEA brought the federal government’s resources and expertise to bear on foreign agents’ misappropriation of trade secrets.<sup>10</sup>

The small number of prosecutions—and their nearly exclusive focus on activities relating to China—as well the continued search for effective law enforcement and regulatory solutions for the economic espionage problem suggest that we need to examine economic espionage at a fundamental level. This examination begins with the recognition that the economic espionage statute has a deeply mixed conceptual and legal heritage, with three principal parts. The first part concerns the incentives of trade secret holders and the goals of national security. The EEA, addresses the infringement of an intellectual property right—trade secrecy—which is designed to encourage innovation by giving private parties a degree of exclusivity in information.<sup>11</sup> Private parties decide how to protect and exploit this information. The real purpose of the economic espionage statute, however, is to address a national security problem. These goals are in tension.

---

<sup>8</sup> 18 U.S.C. § 1831. This was one of two new federal crimes defined as part of the EEA. The other, theft of trade secrets (18 U.S.C. § 1832) lacks the element of intent to benefit a foreign government and carries lighter penalties. Economic Espionage Act of 1996, Pub. L. 104-294 § 1 (1996) (codified at 18 U.S.C. §§ 1831-39). Throughout this article, I refer to 18 U.S.C. § 1831 specifically as “the economic espionage statute” and § 1832 as “the trade secret theft statute.” References to the EEA apply to both of these statutes.

<sup>9</sup> For an argument that Congress should enact legislation that specifically targets cyber attacks, see Jonathan Eric Lewis, *The Economic Espionage Act and the Threat of Chinese Espionage in the United States*, 8 CHI.-KENT J. INTELL. PROP. 189, 232-34 (2009). For reasons developed throughout this Article, I believe a more comprehensive approach is necessary to alter the incentives of trade secret holders, U.S. government officials, and foreign actors.

<sup>10</sup> See James H.A. Pooley, Mark A. Lemley, and Peter J. Toren, *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 178-79 (1997).

<sup>11</sup> See, e.g., Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1649-50 (2002).

Private parties generally do not have the incentives to protect their information at a level commensurate with national security concerns. Also, trade secret holders' discretion as to whether and to whom to disclose a secret is at odds with national security regulation's basic model of centrally controlling access to information. The second element of this landscape is a need for public-private information sharing. Since protecting privately held information carries national security significance, the government and private parties need some way to coordinate what they know. Third, addressing economic espionage requires some mechanism for transmitting constraints that will shape the incentives of foreign governments.

This Article seeks to put these three pieces together. None of them can stand alone. I argue, however, that the U.S. policymakers desperately need to pay attention to this last element in order to give the others a chance to work.

The remainder of this article proceeds in five parts. Part II situates economic espionage in the broader context of traditional espionage, the effort to gain unauthorized access to information that the government designates as confidential in order to prevent harm to its military or diplomatic interests. The shift to *economic* espionage, which targets privately held information such as trade secrets, occurred when political and technological changes in made it worthwhile for other nations to spend intelligence resources collecting a broad array of information. This Part also establishes the characteristics of economic espionage that properly define it as a national security problem.

Part III reviews how U.S. laws and regulations, as well as international law and norms, have responded to the evolution of espionage threats. Drawing on the literature that has examined espionage from an international law perspective, I argue that domestic regulations of

national security information are complementary to international rules and norms that constrain espionage activities. These constraints are mostly absent when it comes to economic espionage.

In Part IV I argue that the U.S. approach to economic espionage is fundamentally misguided and is failing. This is evident in the gap between assessments of levels of economic espionage activity and actual cases. I argue that the economic espionage statute's acceptance of the basic design of trade secret law means that the statute does not align the incentives of trade secret holders with the goals of national security, does not promote necessary communication between trade secret holders and law enforcement agencies, and does nothing to advance shared international understandings of what constitutes acceptable economic information collection.

In Part V, I set forth ways to remedy these defects using the levers of domestic law, government-private sector relations, and international constraints. Strengthening the economic espionage statute by imposing stiffer penalties expanding its prohibitions will be ineffective. Tinkering at the edges of a law that is basically incompatible national security goals is unlikely to reduce economic espionage. Instead, policymakers should consider ways to better align the incentives of trade secret holders with the goals of national security. Creating a disclosure requirement is a plausible way to bring this about. In addition, to allow the private sector and the government—through law enforcement, counterintelligence, or diplomacy— to act proactively, more effective means of information sharing are necessary but also create new needs for Congressional oversight. To reduce losses in the near term and slow the economic espionage arms race in the long term, addressing the absence of internationally accepted constraints on economic espionage is a necessary step. These efforts should build on the existing international framework regulating traditional espionage and could begin with the modest steps I identify here.

Part VI concludes.

## **II. The Evolution of Espionage—Economic and Otherwise**

Though the codification of a national security interest in protecting trade secrets is a relatively recent development, it followed a long evolution of how information relevant to the military, foreign affairs, and national economic strength are produced and managed within the government. This Part reviews that evolution.

### ***A. Information Traditionally Protected on National Security Grounds***

The traditional core of national security information includes military plans and capabilities, instructions to diplomats, and the sources and methods governments use to collect such information about other states are among the most sensitive types of information government officials can possess.<sup>12</sup> Disclosures of such information during wartime can tip off enemies as to plans and capabilities, potentially leading to battlefield defeats.<sup>13</sup> During peacetime, leaks of these kinds of information can allow other nations—allies as well as adversaries—to quietly counter military and technological advances and frustrate diplomatic strategies.<sup>14</sup> Conversely, successful intelligence gathering can forewarn a government about such threats, allowing it to adjust its tactics or disrupt attacks.<sup>15</sup> Collecting and analyzing information about other nations' plans and capabilities through open as well as covert means has

---

<sup>12</sup> See, e.g., Exec. Order 12,958 § 1.5 (defining these categories of information as potentially subject to classification).

<sup>13</sup> For example, during WWII, the U.S. military convinced newspapers not to print reports of successful code breaking efforts.

<sup>14</sup> An example from the early days of U.S. intelligence efforts is the interception and decoding of Japanese diplomatic cables in advance of certain treaty negotiations.

<sup>15</sup> *Id.*, *supra* note \_\_\_, at 1 (stating that “Pearl Harbor taught [the United States] that foreknowledge is a possible guarantor of survival”).

thus been part of relations among states since antiquity, and extensive intelligence organizations are common in modern industrialized nations.<sup>16</sup>

Intelligence also involves a defensive element.<sup>17</sup> To prevent adversaries from gaining an information advantage, governments seek to protect information about their own activities. Finding ways to defeat foreign governments' efforts to maintain secrecy is therefore a key component of intelligence. Espionage, which is the "consciously deceitful collection of information, ordered by a government . . . accomplished by humans unauthorized by the target to do the collection"<sup>18</sup> has always been an element of intelligence.<sup>19</sup> As one Cold War-era history of espionage put it, "[n]ations that did not spy went down into the dust of oblivion because they didn't; other nations, ancient and modern, waxed fat on the fruits of espionage."

## ***B. The Post-Cold War Expansion of Espionage***

Protecting information that might compromise national security is no longer as simple as it once was. Threats have proliferated due to political upheaval, and the role of information and

---

<sup>16</sup> The U.S. intelligence community comprises 16 separate organizations, each with a distinct range of methods and objectives and objectives defined largely by executive order.

<sup>17</sup> Intelligence is defined by the activities of collection and analysis, while counterintelligence means frustrating adversarial intelligence efforts. See Office of the Nat'l Counterintel. Exec., Counterintelligence Mission, <http://www.ncix.gov/about/mission.html> (last visited Jul. 5, 2009) (listing "[p]rotect[ing] vital national assets from adversarial intelligence activities," among other objectives of U.S. counterintelligence agencies).

<sup>18</sup> Dieter Fleck, *Individual and State Responsibility for Intelligence Gathering*, MICH. J. INT'L L. 687, 688-89 (2007) (quoting Lt. Col. Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 325-26 (1996)). Accord COL. ALLISON IND, A SHORT HISTORY OF ESPIONAGE 9 (1963) ("[I]n spying, or espionage, a pivotal point is *prohibited* information. International espionage can, in fact, be defined as the 'attempt to obtain clandestinely or under false pretenses denied information concerning one government for transmission to another government.'" (emphasis in original; internal quotation also in original and apparently used to highlight the definition).

<sup>19</sup> See TERRY CROWDY, THE ENEMY WITHIN: A HISTORY OF ESPIONAGE 15-33 (stating the oldest record espionage dates from the 13th century before the Common Era, and providing other examples from ancient Greek and Chinese histories). See also Ind, *supra* note \_\_\_, at 2 ("Spying is at least the second oldest profession . . .").

intellectual assets in the U.S. economy has dramatically expanded the extent to which the misappropriation of privately controlled information can implicate national security.

## 1. Geopolitical Change

The geopolitical landscape has changed dramatically over the past 20 years. The bipolar “game” of U.S.-Soviet relations<sup>20</sup> has given way to a more fluid era of emerging powers and asymmetric conflict.<sup>21</sup> After the Soviet Union fell, the story went, foreign intelligence services had a sudden abundance of expertise and resources to gather information about U.S. industries.<sup>22</sup> Since 1995, intelligence community assessments of economic espionage have stated that 10-20 nations present the most serious threats.<sup>23</sup> The countries engaged in economic espionage are “both allies and adversaries.”<sup>24</sup> An influential GAO report, made public in 1996, noted that “U.S. allies actively seek to obtain classified and technical information from the United States

---

<sup>20</sup> Chesterman, *supra* note \_\_\_, at 1097 (using the game metaphor to describe U.S.-Soviet relations).

<sup>21</sup> The emerging powers most frequently cited as being of interest are China and India. For reasons that will become obvious later on, I focus on China in this Article.

<sup>22</sup> *See, e.g.*, S. Rep. 104-359, at 7 (1996) (“In a world that increasingly measures national power and national security in economic terms as well as military terms, many foreign intelligence services around the world are shifting the emphasis in targeting. . . . Since the U.S. continues to be on the cutting edge of technological innovation, technology theft will remain a major concern for us.”) (quoting then-CIA Director Robert Gates).

<sup>23</sup> Former FBI Director Louis Freeh testified in a hearing on the EEA that 23 foreign nations were engaged in economic espionage. May 9, 1996, House Judiciary Committee, Crime Subcommittee. That number was repeated in early installments of the FECIE. *See* FECIE 1996; FECIE 1997. Subsequent reports stated that only about one-third of these nations presented serious economic espionage threats FECIE 1998 at 6 & n. 4 (reporting that eight nations represent “the most serious threat”); FECIE 1999 at 1 (reporting that “over half a dozen” nations were “most active collectors of US proprietary information and critical technologies”). In the early years of this decade, the reported number of active collectors spiked to nearly 100. *See* FECIE 2002 (reporting 75 nations); FECIE 2003 (90); FECIE 2004 (100). At first this figure was unqualified, FECIE 2002, but more recent reports have clarified that a “entities from a few key countries accounted for the bulk of attacks.” FECIE 2003. The most recent report is in line with estimates from the mid 1990s. FECIE 2007 (noting that “[w]hile collectors came from a large number of countries, those from fewer than 10 nations, including both allies and adversaries, accounted for the bulk of targeting activity”).

<sup>24</sup> FECIE 2007 at ii.

through unauthorized means.”<sup>25</sup> Though official counterintelligence documents usually refrain from naming specific countries—other than China and Russia—most of their identities are fairly clear from other government documents. Israel, France, Germany, Japan, and India all are frequently identified as sources of economic espionage activities.<sup>26</sup> The objective of many of these collection efforts, which included corporate mergers and acquisitions, recruitment of U.S. citizens, and infiltration of Department of Defense communications networks, was to obtain military technology so that the countries could produce it themselves, and possibly export the knowledge or the finished goods to build alliances or to build a sufficiently large customer base to support a country’s own arms industries.

The set of actors that are motivated to collect intelligence has thus expanded considerably. The record of economic espionage prosecutions in the United States is decidedly more focused. Five of the six indictments filed under the economic espionage statute name Chinese nationals or U.S. citizens of Chinese descent as defendants.<sup>27</sup> U.S. officials also publicly discuss China’s alleged espionage activities in greater detail than those of any other country. I discuss the significance of this pattern in Part \_\_\_. This shift in the structure of the world political order has contributed to the strategic importance of economic development in other nations.

---

<sup>25</sup> U.S. General Accounting Office, *Defense Industrial Security: Weaknesses in U.S. Security Arrangements with Foreign-Owned Defense Contractors* 22-26, Feb. 1996 [hereinafter GAO, *Espionage Report*]. This report discussed in detail the activities of five pseudonymous countries that engaged heavily in economic espionage. Intelligence watchers quickly discerned the identities of these countries: Israel, France, Japan, Russia, and Germany. See John J. Fialka, *Stealing the Spark: Why Economic Espionage Works in America*, 19 WASHINGTON QUARTERLY 173 (1996).

<sup>26</sup> Id.

<sup>27</sup> DOJ press releases.

## 2. Technological Change

Even before the political upheaval that marked the end of the Cold War, rapid changes in information and communications technology were underway. One consequence of these changes was that information technology for which the military was one of the only customers—it was too expensive for anyone else—was eclipsed by technology available on the mass market. To exploit these innovations, as well as their lower costs, the military began to meet some of its information technology needs by acquiring commercially available, “off-the-shelf” components.<sup>28</sup> As former FBI Director Louis Freeh noted:

[The IT and military sectors] produce classified products for the government; 2) they produce dual-use technology used in both the public and private sectors; and 3) they are responsible for R&D and creation of leading-edge technologies critical to maintaining U.S. economic security. Losses at any of these levels could affect U.S. international competitiveness and security.<sup>29</sup>

Beyond this, the U.S. government in general relies heavily upon commercial information and communications technologies to manage its operations, and to provide information to and interact with citizens. In the private sector, of course, these same technologies have spurred countless innovations, increasing opportunities for expression, increasing productivity, and allowing companies to reach new domestic and international markets.

But at the same time, these technological developments have exposed military and civilian government information systems to direct attacks and made it vulnerable to information that leaks from private sector systems. These changes have also made it more difficult to rely on

---

<sup>28</sup> Some of these are “dual-use” technologies, which have military and non-military applications. See *infra* discussion.

<sup>29</sup> Testimony of Louis J. Freeh before the House Judiciary Committee, Crime Subcommittee, May 9, 1996.

national border to keep adversaries at bay.<sup>30</sup> Finally, technological developments have made it much cheaper to collect economic and technological information on a scale that allows large-scale, rapid industrial development without investing in fully independent research and development.<sup>31</sup> This presents the prospect of other nations “leapfrogging” the United States in technological development.

For these reasons, Congress in 1995 ordered the intelligence community to begin systematically studying and reporting on “foreign economic collection and industrial espionage.”<sup>32</sup> Each report has outlined the targets, methods, and harms of economic espionage, and each one states that economic espionage inflicts grave harm on the United States. The 1995 report, for example, states that economic espionage caused U.S. companies to cut jobs and lose market share.<sup>33</sup> The 2000 report points to the “dramatically increased” risk to “sensitive business information and advanced technologies . . . in the post-Cold War era as foreign governments—both former adversaries and allies—have shifted their espionage resources away from military and political targets to commerce.”<sup>34</sup> The ends of this collection are not only to gain access to security-related technology and information but also to gain “a competitive edge in the global

---

<sup>30</sup> Developments in IT and communications technology were not the only technological changes that reshaped thinking about national security. Rapid changes in transportation, beginning with steam powered ships, forced the United States to confront the fact that “our oceans no longer protected us.” Col. Chet Richards, *Shattering Illusions: A National Security Strategy for 2009-2017* 53, in *America’s Defense Meltdown: Pentagon Reform for President Obama and the New Congress* (Winslow T. Wheeler ed.) (2008).

<sup>31</sup> Research and development costs both time and money. Researchers must, of course, be funded. But the course of basic and applied research also involves pursuing directions that may not produce practical solutions to real-world problems. Uncovering the details of successful research can save a competitor—whether it is an individual, a private firm, or a nation-state—considerable amounts of time.

<sup>32</sup> This is one of many instances of variations in terminology. “Industrial espionage” is typically used to refer to simple trade secret misappropriation, i.e., in the absence of intent to benefit a foreign government.

<sup>33</sup> FECIE 1995 at 16.

<sup>34</sup> FECIE 2000 at 6.

economy.”<sup>35</sup> In 2007, the report quoted a National Academies of Science report to link economic espionage to the possibility of an abrupt loss in the “lead in science and technology.”<sup>36</sup> This loss could be broad: FECIE reports over the years have consistently named the information technology, energy, biotechnology, defense, and manufacturing sectors as the most important targets.<sup>37</sup>

The first intelligence reports on economic espionage scarcely mention cyber attacks; uses of the Internet were limited to collections of “open source,” or legally and openly available, information.<sup>38</sup> The next year, the Internet-based collection was mentioned as a method, though one that was more hypothetical than real.<sup>39</sup> The absence of any call to secure these networks is conspicuous. The 2000 report specified Internet collection methods in greater detail, singling out targeted e-mails and “exploiting Internet discussion groups.”<sup>40</sup>

By 2001, however, the Internet had emerged as a decidedly dark force in intelligence community assessments. That year’s report devoted a section to “cyber attack and exploitation,” which described “foreign probes” and gave an example of a system that withstood “several hundred attempts” to defeat its access controls.<sup>41</sup> The report concluded that “intelligence collectors are attempting to use the Internet to gain access to sensitive or proprietary information.” And in 2007, the report gets more specific about both cyber attack methods and perpetrators. In addition to large-scale information collection using open sources as well as brute-force attacks against government and private-sector systems, attackers started “spear-

---

<sup>35</sup> *Id.* at 2.

<sup>36</sup> FECIE 2007 at 1.

<sup>37</sup> *Compare* FECIE 1995 *with* FECIE 2007.

<sup>38</sup> *See* FECIE 1995 at 20.

<sup>39</sup> *See* FECIE 1996 at 10. This report also ran together the problems of attacks on government and private networks.

<sup>40</sup> FECIE 2000 at 8-9.

<sup>41</sup> FECIE 2001 at 2.

phishing”): sending e-mail to targets such as corporate executives that appears to come from a trusted source but in fact carries malicious files or directs the recipient to malicious content.<sup>42</sup>

In contrast to their consistency in identifying targeted economic sectors, intelligence community reports have varied widely in their quantitative assessments of harm. These were initially modest, with the 1995 report stating that U.S. companies lost “millions of dollars” from economic espionage.<sup>43</sup> In 1996, this figure grew to \$24 billion per year.<sup>44</sup> By 2002, annual losses were estimated to be \$300 billion.<sup>45</sup> More recent reports, however, have ceased to make any quantitative estimate of loss, without offering a reason for doing so.<sup>46</sup> This reluctance to quantify losses does not suggest that the intelligence community has changed its assessment that economic espionage is a serious national security concern. The consistency of intelligence community reports, and the absence voices to the contrary—other than official denials from countries accused of sponsoring economic espionage—tend to support this conclusion.

### ***C. Why Economic Espionage Is a National Security Problem: Externalization of Losses***

At the end of the Cold War, U.S. national security strategy shifted from maintaining the military power and foreign relations necessary to contain the Soviet Union and other communist

---

<sup>42</sup> FECIE 2007 at 4.

<sup>43</sup> FECIE 1995 at 16.

<sup>44</sup> FECIE 1996 at 6.

<sup>45</sup> FECIE 2002 at vii. *Cf.* FECIE 2001 (reporting estimate of “\$100-250 billion in lost sales”).

<sup>46</sup> *See* FECIE 2005 at 1 n.3 (stating that the “illegal outflow of technology imposed huge costs on the United States” but noting that [c]alculating a precise dollar figure for these losses would be difficult”). For a dissection of how a questionable estimate of losses due to another kind of intellectual property rights infringement – copyright infringement – see Julian Sanchez, *750,000 Lost Jobs? The Dodgy Digits Behind the War on Piracy*, Ars Technica (last modified Oct. 7, 2008), <http://arstechnica.com/tech-policy/news/2008/10/dodgy-digits-behind-the-war-on-piracy.ars>.

countries<sup>47</sup> to a more expansive set of goals that included maintaining economic security. The 1991 National Security Strategy made this link plain: “National security and economic strength are indivisible.”<sup>48</sup> EEA supporters then used a syllogism to argue that trade secrets have national security significance: economic security is an element of national security. Economic espionage and other threats to intellectual property are threats to economic security. Therefore, economic espionage threatens national security. The House Report on the EEA uses exactly this argument:<sup>49</sup>

There can be no question that the development of proprietary economic information is an integral part of America’s economic well-being. Moreover, the nation’s economic interests are a part of its national security interests. Thus, threats to the nation’s economic interest are threats to the nation’s vital security interests.

This argument proves too much; it does not provide a principle to distinguish economic espionage from other sources of economic loss. After all, others factors—traffic congestion and sick days taken to treat preventable illnesses, for example—cost U.S. businesses significant

---

<sup>47</sup> See Don M. Snider, *The National Security Strategy: Documenting the Strategic Vision 2*, Strategic Studies Institute, Army War College (1995) [http://www.cs.indiana.edu/sudoc/image\\_30000047651504/30000047651504/pdfdocs/jel/research/natlsecy.pdf](http://www.cs.indiana.edu/sudoc/image_30000047651504/30000047651504/pdfdocs/jel/research/natlsecy.pdf) (noting that a broad consensus over containment strategy lasted into the late 1980s).

<sup>48</sup> National Security Strategy (Aug. 1991). See also Snider, *supra* note 56, at 9 (“Even more than the previous reports, the [1991 National Security Strategy] attempted to communicate the idea that American economic well-being was included in the definition of national security, . . .”); Testimony of Secretary of State Warren Christopher before the Senate Foreign Relations Committee, Nov. 4, 1993 (“In the post-Cold War world, our national security is inseparable from our economic security.”) (quoted in Louis Freeh’s 1996 House testimony). The definition of national security also expanded to encompass technological, trade, and even environmental issues at this time. See National Security Strategy (1991) (“We must also be more fully aware of international financial, trade and technology trends that could affect the security of the United States, including its economic well-being.”)

<sup>49</sup> H.R. Rep. 104-788, 1996 U.S.C.C.A.N. 4021, 4022 (1996).

amounts of money each year; but few would suggest that these problems are national security problems. Moreover, the touchstone of economic espionage is trade secrecy. In some cases of economic espionage, the trade secret owner might have had no interest in marketing a product or service in the country that sponsored the espionage.<sup>50</sup>

Trade secret misappropriation from one nation to another, however, may create losses that the targeted firm does not completely internalize; there is an externality in this case. To illustrate, suppose Country *A* and Country *B* are military rivals that engage in little trade. Country *A* sponsors the theft from Country *B* of diagrams for semiconductor chip manufacturing equipment. The target company in Country *B* had no plans to build a plant in Country *A* or even to sell finished chips to it. Still, Country *A*'s industries now have access to a low-cost, highly advanced chip making facility. This access can be used to support any and all of Country *A*'s industries, including, of course, the military sector, which might further work against Country *B*'s national security interests. But, since the targeted company does not bear these losses directly, it has no trade secret-based incentive to reduce the risk of misappropriation by a sophisticated, nation-state-backed adversary. Without communication between the private-sector targets of attacks and the law enforcement, intelligence, and military agencies that monitor these threats, all end up with incomplete information. Private companies might fail to grasp the broader significance of an incident and dismiss it, while government agencies as well as Congress are left with gaps in their knowledge. That is, private firms are likely to spend only as much as they believe is justified by their expected loss from trade secret misappropriation.<sup>51</sup>

---

<sup>50</sup> See the discussion of the *Meng* case, *infra*.

<sup>51</sup> For a variety of reasons that scholars in many disciplines are exploring, firms tend to invest less in securing their information than would be socially efficient.

Supporters of the EEA described precisely this externality. For example, at a February 1996 Senate hearing on economic espionage, Senator Arlen Specter asked FBI Director Louis Freeh for his take on Boris Yeltsin’s instructing Russian intelligence services to use economic espionage to “close the gap” with Western economies.<sup>52</sup> Director Freeh replied that these instructions posed a “very ominous threat to this country, to the infrastructure, to our economy, and on top of these, the American companies, as good and sophisticated as they are, are not prepared, nor should they be, to deal with that kind of an attack.”<sup>53</sup>

Congress sought to address this externality by making it more costly for agents to engage in economic espionage. A conviction for economic espionage can lead to a longer prison sentence than a trade secret theft conviction, other things being equal.<sup>54</sup> The costs imposed on principals—foreign instrumentalities that sponsor economic espionage—are, however, probably more attenuated. They do not serve prison time, pay restitution, or lose property through forfeiture. Nor, as I explain below, does the EEA bring with it any tradition of shared norms that might reduce other nations’ incentives to sponsor economic espionage. Thus, it is unclear that the economic espionage does much to change the overall costs to sponsoring nations.

Congress also chose not to address the externality of economic espionage by creating stricter requirements for protecting trade secrets. The EEA’s definition of trade secrecy, and the range of conduct it prohibits, are arguably broader than they are under state trade secret laws.<sup>55</sup>

The economic espionage also was not formulated with the aim of encouraging trade secret

---

<sup>52</sup> Senate Feb. 1996 hearing.

<sup>53</sup> Senate Feb. 1996 hearing. Such strong rhetoric has persisted but is now focused on China rather than Russia.

<sup>54</sup> The same holds true if an organization charged. *Compare* 18 U.S.C. § 1831(b) (providing a maximum fine of \$10 million for economic espionage) *with* § 1832(b) (providing a maximum fine of \$5 million for trade secret theft).

<sup>55</sup> *See* Michael L. Rustad, *The Negligent Enablement of Trade Secret Misappropriation*, 22 SANTA CLARA COMP. & HIGH TECH. L.J. 455, 468 (2006).

holders to invest in additional information security measures. Indeed, the opposite was true; proponents of the statute argued that the government should pay the costs of reducing economic espionage through law enforcement.<sup>56</sup> Finally, the economic espionage statute does not impose liability on trade secret holders who are the victims of attacks.<sup>57</sup>

### **III. Legal Responses to Espionage: The National Security Context for the Economic Espionage Statute**

The impulse of Congress, law enforcement agencies, and industry groups to address economic espionage by making it a crime is understandable. As I discuss on this Part, the United States has relied on domestic criminal statutes to fill voids in the international legal framework surrounding traditional espionage. These laws, as well as the classification system,<sup>58</sup> also provide individuals who have authorized access to sensitive information with incentives not to disclose the information to unauthorized recipients. In addition to criminal penalties, contracts prohibiting disclosure and the prospect of penalizing companies for engaging in unauthorized transactions serve to align individual actors' incentives with the national security goals defined by the government. This Part describes how these three components—government-established information protection priorities, international law and norms, domestic regulations—are integral parts of a system for regulating espionage.

---

<sup>56</sup> See the statement of former FBI Director Louis Freeh, *supra* note \_\_\_\_.

<sup>57</sup> For a discussion of the merits of this approach, see generally Rustad, *supra* note \_\_; Susan W. Brenner & Anthony C. Crescenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act*, HOUSTON J. INT'L L. 389 (2006).

<sup>58</sup> Classification is governed mostly by executive order. Unauthorized acquisitions or disclosures of classified materials may constitute an offense under one of the espionage statutes, but it is the government officials designated as classification authorities under the order who decide what is classified.

## **A. Diplomacy and the International Law of Espionage**

Despite the importance of intelligence in general, and espionage in particular, in international affairs, few provisions of international law confront these subjects head-on. The Hague Regulations provide that, though spies captured in wartime are not entitled to the same protections as prisoners of war and can be put to death, they are entitled to humane treatment, a trial, and a waiting period before being executed.<sup>59</sup> To grossly simplify matters, different modes of intelligence gathering in peacetime run from clearly acceptable (satellite imaging)<sup>60</sup> to ambiguous (electronic communications interception)<sup>61</sup> to clearly illegal (territorial breaches such as airborne surveillance, surveillance from within territorial waters, and unauthorized use of territory by foreign agents).<sup>62</sup>

Breaches of these rules are sometimes punished with force.<sup>63</sup> More often, however, nations respond through diplomatic channels by reproaching diplomats, expelling spies, or trying spies under the host nation's criminal laws. The United States, for example, has long had

---

<sup>59</sup> Simon Chesterman, *The Spy Who Came in from the Cold: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1079-80 (2006).

<sup>60</sup> Chesterman, *supra* note \_\_, at 1085.

<sup>61</sup> Chesterman, *supra* note \_\_, at 1086 (describing interceptions by Britain and the United States of communications of representatives to the U.N. Security Council prior to the Council's vote on the 2003 resolution authorizing the invasion of Iraq).

<sup>62</sup> Chesterman, *supra* note \_\_, at 1081-84 (citing the alleged abduction of an Egyptian national in Italy by CIA agents in 2003). Still, international law provides some accommodation for intelligence collection within the general prohibitions that flow from notions of national sovereignty. For example, the Vienna Convention on Diplomatic Relations contains provisions that balance the fact of intelligence collection with a host state's interest in regulating collection. *See* Chesterman at 1087-90. Provisions that lend some support to intelligence collection include the acceptance of military attaches and the inviolability of diplomats' persons and communications and of the premises of an embassy. *Id.* at 1088-89. Provisions that allow host state regulation include the right to restrict diplomats' mobility and the duty of diplomats to obey the national laws of the host state. *Id.* at 1088.

<sup>63</sup> The Soviet Union's shooting down of a U-2 surveillance aircraft in 1960 provides one example. As Simon Chesterman notes, this flight was prohibited under international law, and "the United States protested neither the shooting nor the subsequent trial of the pilot." *Id.* at 1083.

criminal espionage statutes to punish the collection and disclosure of “information respecting the national defense.”<sup>64</sup> A full review of these statutes is not germane here.<sup>65</sup> The point I wish to emphasize is that domestic espionage statutes exist in a broader context defined by international legal rules as well as diplomatic norms.

The remainder of this Part details the other principal domestic authorities that regulate the flow of information on national security grounds. The basic paradigm underlying the protection of national security information is to prevent disclosure. The goal is prevent untrustworthy or adversarial parties from obtaining information that could impair national interests. There are three mechanisms for achieving this goal: imposing affirmative obligations on individuals not to disclose information, regulating corporate governance, and creating special legal protection for systems that hold national security information. All three of these mechanisms rely upon a central, governmental authority to assess the sensitivity of information.

## ***B. Domestic Regulation of Information Disclosures Based on National Security Concerns***

### **1. Classification**

Classification is the most important example of disclosure prevention. The classification paradigm imposes affirmative duties on government agencies, private firms, and individuals to prevent the disclosure of classified information.

---

<sup>64</sup> 18 U.S.C. §§ 793-794, 798.

<sup>65</sup> For extensive reviews and forceful critiques of these statutes, see Harold Edgar & Benno C. Schmidt, Jr., *Curtiss-Wright Comes Home: Executive Power and National Security Secrecy*, 21 HARV. C.R.-C.L. L. REV. 349 (1986); Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUMB. L. REV. 929 (1973). For a more recent review, see Mark R. Alson, Note, *Someone Talked! The Necessity of Prohibitions Against Publishing Classified Financial Intelligence Information*, 42 VAL. U. L. REV. 1277 (2008).

The authority for information classification is not statutory but rather constitutional. It arises from the president's authority to conduct matters of national security and foreign affairs.<sup>66</sup> Through executive orders, presidents have given more specific directions to agencies and the private sector as to how to protect information.<sup>67</sup>

The rationale for creating this system is to protect "national security information" in a manner that balances the need to keep information about the military, intelligence, diplomacy, and other sensitive functions of the national government away from adversaries with "democratic principles requir[ing] that the American people be informed of the activities of their Government."<sup>68</sup> More specifically, revealing details of military plans or technologies, or intelligence sources or method, can threaten national defense.<sup>69</sup> Breaches of confidentiality can also reveal government deliberations concerning foreign affairs, potentially leading to diplomatic friction or an unwillingness of foreign governments to engage with the United States.<sup>70</sup> As Professor Nathan Sales points out, government classification authority exists in some tension with private sector prerogatives, such as being able to run a business, not disclosing information

---

<sup>66</sup> U.S. Const. art. 2 § 2. *See also* Christina E. Wells, "National Security" Information and the Freedom of Information Act, 56 ADMIN. L. REV. 1195, 1199 (noting that classification is governed almost entirely by executive order); Edgar & Schmidt, *Executive Power and National Security Secrecy*, *supra* note \_\_, at 368-70 (discussing *United States v. Marchetti*, 466 F.2d 1309 (4th Cir. 1972), in which the Fourth Circuit held that "the process of classification is part of the executive function beyond the scope of judicial review").

<sup>67</sup> For a brief history of information classification in the United States, see Sales, *supra* note 66.

<sup>68</sup> Exec. Order 13,292, 68 Fed. Reg. 15,315 (Mar. 25, 2003). This order modified the prior executive order governing classification, Executive Order 12,958, which was issued on April 24, 1995. The language concerning the democratic values side of the balance is the same, but the secrecy side makes explicit mention of "transnational terrorism" and "homeland security."

<sup>69</sup> Sales, *supra* note 20, at 818-821.

<sup>70</sup> *Id.* at 821.

to the government, and, conversely, not being subject to gag rules imposed by intelligence collectors.<sup>71</sup>

Several institutional features of classification bear emphasis. First, classification authority is highly centralized. Under the Executive Order governing classification, the president, vice president (when performing executive duties), and “agency heads and officials designated by the President” have the authority to classify information.<sup>72</sup> These individuals may, in turn, delegate this “original classification authority” to individuals who have a “demonstrable and continuing need” to exercise classification authority.<sup>73</sup> In addition, a single official—the Director of the Information Security Oversight Office of the National Archives—oversees agencies’ information classifications.<sup>74</sup>

Second, as a general rule, classifications last for a fixed amount of time. Information is declassified either after 10 years or, if the classifying authority determines that the information is sufficiently sensitive, after 25 years.<sup>75</sup> This general rule, however, provides considerable flexibility to depart from these defaults. On one hand, the classification authority may set an earlier date for declassification.<sup>76</sup> On the other hand, the authority may extend the deadline or even mark information for indefinite classification.<sup>77</sup>

Third, only certain categories of subject matter may be classified, though these categories are broad. The categories that are most relevant to economic espionage are “scientific,

---

<sup>71</sup> *Id.* at 813.

<sup>72</sup> Exec. Order 13292 § 1.3(a).

<sup>73</sup> *Id.* § 1.3(c).

<sup>74</sup> See Executive Order 13,292. 68 Federal Register 15,315, Mar. 2003 (requiring agencies to report classification decisions and send notice of impending declassifications to the Director, and granting the Director authority to reverse agencies’ classification decisions).

<sup>75</sup> *Id.* § 1.5(a).

<sup>76</sup> *Id.* § 1.5(b).

<sup>77</sup> *Id.* § 1.5(d).

technological, or economic matters relating to the national security” and military plans and weapons systems.<sup>78</sup> To be sure, these categories are broad and have become broader over time,<sup>79</sup> but they do limit the scope of classification. The other subject matter limitation on classification is the categorical exclusion for “[b]asic scientific research information not clearly related to the national security.”<sup>80</sup>

Finally, though only information that is “owned by, produced by or for, or is under the control of the United States Government” may be classified,<sup>81</sup> the government can regulate how private parties handle classified information. Noting that the private sector plays a crucial role in the national security apparatus, President George H. W. Bush in 1993 ordered the creation of a National Industrial Security Program, which requires private-sector entities to protect classified information “in a manner equivalent to its protection within the executive branch of Government.”<sup>82</sup> The Program put the Secretary of Defense in charge of setting rules for the private sector to follow when handling classified information, including required information security practices, reporting information loss or compromise to the government, submitting lists of cleared facilities and employees, submitting to reviews of corporate ownership to detect “foreign ownership, control, or influence,” and reporting visits by employees to foreign

---

<sup>78</sup> *Id.* §§ 1.4(a), (c). The other categories are: foreign government information, intelligence activities, sources, and methods; foreign relations, programs for safeguarding nuclear materials or facilities, and capabilities or vulnerabilities of infrastructure systems. *Id.*

<sup>79</sup> Wells, *supra* note 100.

<sup>80</sup> Exec. Order 13292 § 1.7(b).

<sup>81</sup> *Id.* § 1.1(2).

<sup>82</sup> Executive Order 12,829. 58 Federal Register 3479. Jan. 1993 (preamble). The program applies only to entities doing business with government—“contractors, grantees, and licensees.” *Id.* § 101(a). It does not apply to the handling of national security information in law enforcement or domestic intelligence investigations, nor does the Program address national security exemptions to the Freedom of Information Act or other laws that obligate the government to disclose information. For a review of the former, see Sales, *supra*. For a review of the latter, see Adam M. Samaha, *Government Secrets, Constitutional Law, and Platforms for Judicial Intervention*, 53 UCLA L. REV. 909 (2006); Wells, *supra* note 100.

countries.<sup>83</sup> Thus, the Program imports the government classification scheme to the private sector and closely regulates private-sector personnel decisions, information security practices, and decisions to disclose incidents concerning classified information.<sup>84</sup>

## 2. Export Controls.

Export controls are the second major part of the disclosure-prevention regime for information holding national security implications. The Commerce Department is in charge of approving exports that fit this description.<sup>85</sup> Specifically, Export Administration Act authorizes the Commerce Department to place “goods or technology”—the latter term includes information<sup>86</sup>—that would “would make a significant contribution to the military potential of any other country or combination of countries which would prove detrimental to the national security of the United States”<sup>87</sup> on an export control list.<sup>88</sup> U.S. individuals and firms are required to

---

<sup>83</sup> See generally United States Dept. of Defense, National Industrial Security Program Operating Manual (2006) [hereinafter “NISPOM”]. See the discussion below of national security-oriented corporate governance regulations for more details about the Program.

<sup>84</sup> Specifically, the NISPOM requires a contractor to “promptly submit a written report to the nearest field office of the FBI regarding information coming to the contractor’s attention concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities at any of its locations.” See NISPOM, *supra* note 117, § 1-301.

<sup>85</sup> See Export Administration Act of 1979, Pub. L. 96-72, 93 Stat. 503 (codified as amended in 50 U.S.C. app. § 2401 *et seq.*).

<sup>86</sup> The Act defines “technology” to mean “information and know-how . . . that can be used to design, produce, manufacture, utilize, or reconstruct goods, including computer software and technical data, but not the goods themselves.” 50 U.S.C. app. § 2415(4). For consistency with the usage in the rest of this article, I will refer simply to “information” that is subject to export controls.

<sup>87</sup> 50 U.S.C. app. § 2402(a).

<sup>88</sup> A similar structure applies to defense articles, defense services, and “related technical data,” as provided under the Arms Export Control Act of 1976, Pub. L. 94-629, 93 Stat. 503 (codified as amended at 22 U.S.C. § 2751 *et seq.*, and the associated International Traffic in Arms Regulations (ITAR), 22 C.F.R. § 121. Similarly, the Treasury Department controls financial transactions with certain foreign nations its Office of Foreign Assets Control. See generally 31 C.F.R. parts 500-598.

obtain export licenses before exporting any such information.<sup>89</sup> An “export,” in turn, may occur not only when information is sent outside the United States but also when it is disclosed—even within the United States—to an “unauthorized person,”<sup>90</sup> such as a citizen of a country to which exports of the relevant information are restricted.<sup>91</sup> A broad array of information falls within the scope of the Export Administration Act, ranging from encryption software to rocket propulsion systems.<sup>92</sup>

Though an explicit purpose of export controls is to protect national security and foreign policy interests,<sup>93</sup> the system of controls balances these interests with encouraging trade.<sup>94</sup> Thus, the Export Administration Regulation (EAR) provides ways to incorporate public comment into decisions about whether to restrict a good or technology.<sup>95</sup> The EAR also allows private entities

---

<sup>89</sup> Export controls have been criticized on a number of grounds, including that they place too a significant compliance burden on U.S. businesses and reduce their access to foreign markets while underestimating the ease with which export-controlled nations can obtain goods and information indirectly. This argument was common during the “crypto wars” of the mid 1990s, when IT companies argued that Congress needed to relax restrictions on the exportation of encryption software. *See, e.g.*, Testimony of Jim Barksdale Before the Senate Committee on Commerce, Science, and Transportation, July 25, 1996 (stating that export controls on encryption “make information-rich businesses vulnerable to costly security breaches and espionage” and “cost America lost sales and lost jobs. Foreign competitors are even using U.S. export control laws as an explicit part of their marketing strategy.”). For general critiques of the export control regime, see Barry P. McDonald, *Government Regulation or Other “Abridgements” of Scientific Research: The Proper Scope of Judicial Review Under the First Amendment*, 54 Emory L.J. 979 (2005); Nathan T.H. Lloyd, Note, *Rebuilding a Broken Regime: Restructuring the Export Administration Act*, 37 VAND. J. TRANSNAT’L L. 299 (2004).

<sup>90</sup> 50 U.S.C. app. § 2415(5)(C). Such disclosures are known as “deemed exports.” See U.S. Dept. of Commerce, *Don’t Let This Happen to You! Actual Investigations of Export Control and Antiboycott Violations* 21, July 2008, <http://www.bis.doc.gov/complianceandenforcement/dontletthishappentoyou-2008.pdf> (using this phrase).

<sup>91</sup> *See id.*

<sup>92</sup> *See* 15 C.F.R. part 774 (Supp. 1).

<sup>93</sup> 50 U.S.C. app. § 2402(4).

<sup>94</sup> *See* 50 U.S.C. app. § 2402(1), (2).

<sup>95</sup> Indeed, the composition of the Commerce Control List is subject to notice and comment rulemaking. *See, e.g.*, U.S. Dept. Commerce, *Interim Final Rule on Encryption Simplification*,

to protest denials of licenses and other administrative actions.<sup>96</sup> The classification regime provides none of these balancing mechanisms.<sup>97</sup>

Still, the EAR replicates the central disclosure-prevention feature of classification: a central authority decides which information is subject to restrictions on disclosure. Private entities that hold information governed by the EAR are subject to civil and criminal penalties for violating it. The list of export-controlled technologies and clearance procedures may be Byzantine, but it is complete; in theory a person can determine from looking at the list whether a given good or piece of information is on the list. Finally, this same authority decides whether to make exceptions to rules that would otherwise prohibit disclosure of information, which is akin to an original classification authority's power to declassify information.

### **3. Corporate Governance Controls**

The second principal element of the national security information protection paradigm is a set of controls on private firm structure. These measures affect both the internal management of firms as well as changes in ownership or control. They complement the EAR and other regulations that govern exchanges of specific pieces of information, on the theory that an adversary could gain access to sensitive information by acquiring the entity that controls the information.

---

73 Fed. Reg. 57495-01, Oct. 3, 2008 (amending the EAR to clarify and simplify export licensing for encryption software).

<sup>96</sup> 15 C.F.R. § 756.

<sup>97</sup> Still, there are constitutional limits on the government's ability to classify information, and a party seeking access to classified information can file Freedom of Information Act requests and challenge denials in court. But, as Professor Adam Samaha has recently pointed out, reconciling the government's interest in secrecy and public norms favoring access to information and governmental transparency usually requires going to court. Samaha, *supra* note \_\_\_. The EAR's built-in administrative mechanisms for ongoing review and public participation are missing from the review of classification.

As a result, the government uses two processes to assess whether certain aspects of corporate governance might create national security threats. The first process focuses on foreign investment in U.S. firms. It is generally applicable, in the sense that a company may be subject to review even if it does not handle classified information. Under amendments to the Defense Production Act, Congress requires the President to review any transaction in which a foreign government seeks to acquire control of a U.S. entity for its effects on national security.<sup>98</sup> In practice, these investigations are handled by the Committee on Foreign Investment in the United States (CFIUS), which was authorized by Congress and formally created by executive order.<sup>99</sup> CFIUS must conduct more extensive national security investigations if it determines, after its initial review, that the transaction would “impair” national security or the acquiring entity is a foreign government or controlled by a foreign government.<sup>100</sup> If CFIUS concludes that the transaction would impair national security, it may enter into a risk mitigation agreement with the parties or recommend that the President prohibit the transaction.<sup>101</sup> CFIUS must submit annual reports detailing the number of transactions it reviewed and investigated, the outcomes of the transactions (whether or not influenced by CFIUS), and trends in covered transactions.<sup>102</sup> In addition, CFIUS must specifically evaluate in its annual report whether it found “credible evidence of a coordinated strategy by 1 or more countries or companies to acquire United States

---

<sup>98</sup> 50 U.S.C. app. § 2170(b)(1). After a series of high-profile controversies surrounding proposed foreign acquisitions of U.S. infrastructure and technology companies, Congress revised the statutory authority for CFIUS. *See* the Foreign Investment and National Security Act of 2007, Pub. L. 11049, 121 Stat. 246 (amending 50 U.S.C. app. § 2170).

<sup>99</sup> *See* Executive Order 13,456, Jan. 23, 2008; Executive Order 11,858, May 7, 1975.

<sup>100</sup> 50 U.S.C. app. § 2170(b)(2).

<sup>101</sup> 50 U.S.C. app. § 7120(d); Executive Order § 7.

<sup>102</sup> 50 U.S.C. app. § 7120(m). For a recent example of a CFIUS report to Congress, see Committee on Foreign Investment in the United States, Annual Report to Congress (Public Version), Dec. 2008, <http://www.treas.gov/offices/international-affairs/cfius/docs/CFIUS-Annual-Rpt-2008.pdf>.

companies involved in research, development, or production of critical technologies for which the United States is a leading producer” or “industrial espionage activities [that are] directed or directly assisted by foreign governments against private United States companies aimed at obtaining commercial secrets related to critical technologies.”<sup>103</sup>

Thus, the executive branch must provide Congress with at least some details about the use of transactions to transfer sensitive information to foreign entities. Moreover, the statute authorizing CFIUS requires its report to Congress to address “critical technologies,” thereby setting a priority on protecting certain types of information.

A second corporate governance mechanism to limit disclosures of information held by U.S. firms is essentially an extension of the classification system, which was briefly discussed above. The National Industrial Security Program (NISP), administered by the Department of Defense,<sup>104</sup> sets minimal standards for contractors that handle classified information. These standards include requirements for clearing employees and visitors; securing information systems; and reporting foreign operation, control, or influence of the contractor. These rules set forth a far-reaching program to regulate contractors’ corporate governance and to allow the Defense Department and other agencies to monitor private entities, though it appears that the DOD has been weak in its oversight.<sup>105</sup>

#### **4. Legally “Hardening” Government Information**

The government also “hardens” its information systems against attack by defining crimes that take government control of a computer, or the presence of classified information on the

---

<sup>103</sup> 50 U.S.C. app. § 2710(m)(3).

<sup>104</sup> See U.S. Dept. of Defense, National Industrial Security Program Operating Manual, Feb. 28, 2006. The NISP was established by Executive Order 12,829.

<sup>105</sup> See U.S. Govt. Accountability Office, *Observations on the National Industrial Security Program*, GAO-08-695T, Apr. 16, 2008.

computer, specifically into account.<sup>106</sup> The most important example of this approach is the Computer Fraud and Abuse Act (CFAA).<sup>107</sup> The CFAA’s approach is the converse of the regulations discussed above; instead of imposing duties on individuals who are authorized to hold information, the CFAA makes it illegal to gain access to information without authorization.

Specifically, the CFAA makes it a crime to obtain classified information by “knowingly access[ing] a computer without authorization.”<sup>108</sup> The CFAA does not stop here; it prohibits breaking in to any “protected computer”—essentially any computer connected to the Internet.<sup>109</sup> In the case of computers holding classified information, however, the act of unauthorized access itself is sufficient to constitute a crime. No showing of monetary loss is necessary, as is the case in most violations defined by the CFAA.<sup>110</sup> Attacking classified systems is also punished more severely than other violations of the CFAA.<sup>111</sup> To my knowledge, however, the United States has not brought a single indictment under this section of the CFAA.

---

<sup>106</sup> See Roland L. Trope, Monique Witt, and William J. Adams, *Hardening the Target*, 6 IEEE SECURITY & PRIVACY MAGAZINE 77, 78 (Sept. 2008) (describing “target-hardening” as measures that “would avert or substantially reduce the targeted enterprise’s vulnerability to risks known—or that should have been known”).

<sup>107</sup> Pub. L. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030).

<sup>108</sup> 18 U.S.C. § 1030(a)(1).

<sup>109</sup> See 18 U.S.C. § 1030(e)(2) (defining “protected computer” to mean not only a computer used by the U.S. government but also a computer “which is used in interstate or foreign commerce or communication”). Still, the CFAA defines violations specifically for U.S. government computers. 18 U.S.C. § 1030(a)(2). For example, the State Department employees who snooped on Barack Obama’s and Hillary Clinton’s passport files were charged under § 1030(a)(2)(B). Plea Agreement, *United States v. Yontz* ¶ 1 (D.D.C. Sept. 10, 2008), [http://blog.wired.com/27bstroke6/files/yontz\\_plea\\_agreement.pdf](http://blog.wired.com/27bstroke6/files/yontz_plea_agreement.pdf); Plea Agreement, *United States v. Cross* ¶ 1 (D.D.C. Jan. 8, 2009), <http://blog.wired.com/27bstroke6/files/crossplea.pdf>.

<sup>110</sup> For example, the most widely used provisions of the CFAA require proof that unauthorized access caused an aggregate loss of \$5000 or more in a one-year period. 18 U.S.C. § 1030(a)(5).

<sup>111</sup> Violations of § 1030(a)(1) carry a maximum prison sentence of 10 years for a first offense, while violations of § 1030(a)(2) carry a maximum of one year.

## IV. Not Knowing Your Enemy: How the Economic Espionage Statute Fails to Advance National Security Goals

Viewed as an addition to classification and the legal provisions intended to prevent disclosures of sensitive information to foreign agents, the EEA is incongruous. The regulations discussed in Part III possess the same basic model of information flow: a central governmental authority sets sensitivity levels and controls disclosures through individual incentives, commercial transactions, or transactions resulting in changes in corporate control.<sup>112</sup> All of this takes place in the context of long-term observation of adversaries who act under a system of established, albeit incomplete, international legal rules and norms.

When members of Congress recognized that “our” trade secrets were under attack by foreign-sponsored adversaries, they did import the other structures that support domestic law. Congress did not propose to alter the basic design of trade secret rights to facilitate government monitoring of disclosures. Instead, Congress created an analogue to the existing espionage statutes, making the intent to benefit a foreign government an element of the new crime and the basis for harsher punishment.<sup>113</sup> As discussed above, however, the threats that led to the

---

<sup>112</sup> Controlling information disclosure in private transactions is in some tension with individual and other nations’ economic prerogatives. *See* GAO, *supra* note 139 (noting that a web of laws and regulations, including those discussed in the main text, “identify and protect technologies critical to maintaining U.S. technological superiority on the battlefield and to provide for the transfer of these technologies to foreign parties in a manner consistent with U.S. economic, foreign policy and national security interests”).

<sup>113</sup> Congress also had a more modest goal in passing the EEA, in which benefiting a foreign government is somewhat peripheral. Before the EEA was enacted, federal law lacked a generally applicable trade secret statute. Supporters of the law saw the lack of federal protection for trade secrets as unfair in two respects. First, it seemed an incongruous neglect of secret information in an increasingly information-dependent economy. Though the Supreme Court had held that trade secrets are a form of property, it also limited the application of pre-EEA criminal statutes to trade secret misappropriation. *See* *United States v. Carpenter*, 484 U.S. 19, 26-27 (1987) (finding a property right in a trade secret on the ground that “[t]he confidential information was generated from the business, and the business had a right to decide how to use it prior to disclosing it to the public); *Dowling v. United States*, 473 U.S. 207 (1985) (holding that

development of the EEA represented a break from past espionage practices and targeted a broader array of information than in the past. Though supporters of the economic espionage statute linked it rhetorically to national security, the statute provides neither the incentives nor the structure to make it effectively support national security goals. Instead, the economic espionage statute was left to stand on its own. This Part argues that this was misguided as a matter of legal policy and has been a failure in practice.

### ***A. The Incompatible Goals and Structure of Regulations Protecting Trade Secrets and National Security Information***

The goals and design of trade secret law are fundamentally different from national security information regulations. Though the purpose(s) of trade secret as a legal doctrine are still widely debated, most commentators agree that helps to order commercial relationships among private parties.<sup>114</sup> Private parties decide whether to treat information under their control as a trade secret. They decide whether and under what circumstances to disclose the secret to others. And finally, private parties decide whether to take action to enforce their trade secret rights. None of this changed when the EEA made it a federal crime to misappropriate a trade secret.

This subpart lays out the major theories of trade secrecy and relates the text, history, and enforcement of the economic espionage statute to those theories. I argue that trade secret law differs fundamentally from the laws that protect national security information. Trade secret law does not provide any of the mechanisms that facilitate the protection of national security

---

copyrighted works do not fall within the “goods, wares, or merchandise” covered by the National Stolen Property Act, 18 U.S.C. § 2314). Other federal statutes—wire fraud and mail fraud, for example—were limited to specific means of transporting information and hence only cover a subset of economic espionage cases.

<sup>114</sup> See generally Robert Bone, *A New Look at Trade Secret Law: A Doctrine in Search of a Justification*, 86 CAL. L. REV. 241 (1998) (arguing that trade secret law has no independent justification and should be based on contract law).

information. This subpart also argues that none of the principal theories of trade secret protection are consonant with what Congress hoped to achieve by passing the economic espionage statute, or what prosecutors hope to achieve by enforcing it. The structure and rationale of trade secret protection simply make it unsuitable to do the work of national security.

## **1. Mechanisms for Trade Secret Protection**

Trade secret law contains nothing remotely comparable to the system of centralized assessment of sensitivity and control over dissemination that characterizes classification. Indeed the absence of any centralized recording of information about trade secrets is part of what distinguishes them from other forms of IP. Unlike patents and trademarks, trade secrets need not be disclosed to, reviewed by, or registered with any agency in order to be enforceable. Also, in contrast to copyright protection, which protects published works with exclusive rights of reproduction and distribution,<sup>115</sup> trade secret protection is lost if the owner fails to take reasonable measures to keep it secret<sup>116</sup> or discloses it to another person without creating at least an implicit duty to keep it confidential.<sup>117</sup>

Any comparable structure—some sort of confidential trade secret registry, for example—would be inimical to the broader scheme of the law. Individual firms decide whether and how to

---

<sup>115</sup> 17 U.S.C. § 106.

<sup>116</sup> This is true under both the Uniform Trade Secrets Act, which most states have adopted in some form, as well as the Economic Espionage Act. *See also* *Rockwell v. DEC* (7th Cir. 1991) (holding that deciding what security measures are reasonable in a given context is a factual question that must balance the costs and benefits of a given level of protection); *United States v. Krumrei* (holding that the EEA’s use of “reasonable measures” to define “trade secrets,” 18 U.S.C. § 1839, is not unconstitutionally vague).

<sup>117</sup> *See* *Smith v. Dravo Corp.*, 203 F.2d 369 (7th Cir. 1953) (holding that disclosure of a trade secret during an acquisition negotiation did not preclude trade secret action); *see also* *Bone*, *supra* note 147, at 301-302 (arguing that courts should find an implied duty of confidentiality only when they would find an implied-in-fact contract).

protect trade secrets.<sup>118</sup> Many companies do not maintain lists of their trade secrets, preferring instead to define broad confidentiality obligations with employees and business partners, and define a trade secret more specifically after they suspect misappropriation.

It would probably be counterproductive to require firms to take these steps. An important policy consideration in courts' efforts to relate trade secrets to patent rights in particular has been that they offer a low-cost way of protecting information that is valuable but not patentable.<sup>119</sup> Imposing greater costs on trade secret holders would likely result in some firms deciding not to protect their trade secrets at all.

An alternative to knowledge management is to induce trade secret holders to be more aggressive in reporting suspected misappropriation to law enforcement agencies, which could then investigate likely instances of economic espionage. Such a voluntary mechanism would at least be consistent with the structure of trade secret law, but it would have to overcome the significant downside that private firms see in reporting trade secret theft to law enforcement agencies. A persistent complaint among private sector representatives is that criminal investigations draw unwanted attention to a company and, even worse, sometimes end up exposing the information that the company sought to protect.<sup>120</sup>

---

<sup>118</sup> Some firms might not have complete discretion to keep quiet about an incident. Under the Sarbanes-Oxley Act, publicly traded companies must report "material" events that may affect shareholder equity. See Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 186 & nn.218-219 (2005) (arguing that Sarbanes-Oxley creates trade secret protection obligations). The Sarbanes-Oxley Act also requires companies to use "internal controls" to prevent compromises of their information systems and to report annually on the effectiveness of these controls. Michael D. Scott, *Tort Liability for the Vendors of Insecure Software: Has the Time Finally Come?*, 67 MARYLAND L. REV. 425, 477-478 (2008).

<sup>119</sup> See generally *Kewanee*.

<sup>120</sup> See Testimony of Scott Charney Before the House International Relations Committee, Sept. 13, 2000 (noting "a reluctance by some industry members to go to law enforcement. . . . [T]he

## 2. Rationales for Trade Secrecy

In addition to providing enforcement mechanisms that are incompatible with protecting national security information, the rationales for trade secret law are also mostly irreconcilable with national security. As a result, trade secret law is not up to the task of channeling the energy of trade secret owners toward the ends of national security; nor is trade secret law successful in changing the incentives of would-be economic spies. Which rationale, if any,<sup>121</sup> best fits trade secret law is a topic of continuing scholarly and jurisprudential debate. The discussion here does not attempt to settle these debates. Instead, the discussion shows that none of the rationales advanced for trade secret protection is commensurate with the goal of preventing the disclosure of information when it would harm national interests.

**Efficiency: Providing Incentives to Create and Disclose Information.** One commonly cited rationale for trade secret law is that it enhances economic efficiency.<sup>122</sup> A world with trade secret law, the argument goes, provides greater incentives to invent and lowers the costs of

---

biggest [reason] I see is that for a private victim, if they go to the government they lose control over the case.”); 2004 WLNR 6247871 (“In the past, corporations feared investigations and bad publicity, or worried that trade secrets might emerge in court. But now more high-tech firms and other companies are starting to work with the FBI, the CIA, the military and other government bodies to choke espionage cases before they worsen.”); 5/15/2006 Nat’l L.J. S1: “The companies ‘have been appalled at the cavalier way [the FBI and federal prosecutors] handled their trade secrets,’ Fink said. ‘They feel they are more at risk for getting trade secrets exposed by coming forward than just sweeping it under the rug.’ ” According to some accounts, the FBI has grown more adept at handling trade secrets during investigations.

<sup>121</sup> Professor Robert Bone has also argued that there is no coherent justification for trade secret law and that trade secret disputes should be governed by contract principles. *See Bone, supra* note 147.

<sup>122</sup> *See, e.g., Rockwell v. DEV*, 925 F.2d 174, 178 (7th Cir. 1991) (discussing trade secret misappropriation as a “sterile wealth-redistributive-not-productive-activit[y]”).

exchanging information, relative to a world without it.<sup>123</sup> Thus, the efficiency rationale holds that trade secrecy encourages both information creation and information disclosure.<sup>124</sup>

The argument from efficiency is that trade secret protection provides some marginal incentive to invent or disclose, compared to a world without trade secrecy. For example, trade secrecy provides some exclusivity for inventions that are not or might not be patentable.<sup>125</sup> In these cases, some inventors might refrain from disclosing their inventions to others in order to wait for the Patent Office to decide whether to issue a patent.<sup>126</sup> Other inventors might simply choose not to disclose information at all, because the risk of unauthorized use or disclosure is too great, and the deterrent provided by a purely contractual substitute for trade secrecy is too small. Still others might resort to costly security measures or a highly restricted employee pool.<sup>127</sup>

---

<sup>123</sup> Mark A. Lemley, *Property, Intellectual Property, and Free Riding*, 83 TEX. L. REV. 1031, 1031 (2005) (“Intellectual property in the United States has always been about generating incentives to create.”).

<sup>124</sup> *Id.*

<sup>125</sup> As Chief Justice Burger wrote for the Supreme Court in *Kewanee Oil Co. v. Bicron Corp.*:  
For those inventors “on the line” as to whether to seek patent protection, the abolition of trade secret protection might encourage some to apply for a patent who otherwise would not have done so. For some of those so encouraged, no patent will be granted and the result will have been an unnecessary postponement in the divulging of the trade secret to persons willing to pay for it. If (the patent does issue), it may well be invalid, yet many will prefer to pay a modest royalty than to contest it, even though *Lear* allows them to accept a license and pursue the contest without paying royalties while the fight goes on. The result in such a case would be unjustified royalty payments from many who would prefer not to pay them rather than agreed fees from one or a few who are entirely willing to do so.  
416 U.S. at 486-87.

<sup>126</sup> *Id.*

<sup>127</sup> *See Kewanee*, 416 U.S. at 485-86 (arguing that, without trade secret protection, firms would have to pay employees with knowledge of secrets “an amount thought sufficient to assure their loyalty” and that “[t]he innovative entrepreneur with limited resources would tend to confine his research efforts to himself and those few he felt he could trust without the ultimate assurance of legal protection against breaches of confidence”).

These restrictions are likely to raise the cost of developing new inventions and thus reduce the level of inventive activity.<sup>128</sup>

Both aspects of the efficiency rationale—promoting invention and promoting disclosure—are in obvious conflict with the national security paradigm. The objective of protecting information under the national security paradigm is to prevent disclosures that would impair national interests. This objective is both negative and binary, and a single decisionmaker—the government—decides which disclosures are permissible. In contrast, the efficiency rationale for trade secrecy holds that private parties are best situated to decide whether disclosing information is to their advantage. To first order, trade secret owners do not care whether a prospective trade secret licensee is a national friend or foe, foreign or domestic. What matters is whether a trade secret licensee will respect the terms of the agreement under which it obtains access to the secret. Conversely, trade secret owners may care little about the identity of a trade secret misappropriator. Indeed, the owner might be harmed more by a competitor’s misappropriation than by misappropriation from a country in which the firm does not compete.

Additionally, the efficiency rationale views legal protection as a substitute for the trade secret owner’s investment in security. All the owner has to do is take “reasonable” measures to maintain secrecy. If trade secret owners were encouraged to add the potential harm to national security to the potential costs of a breach,<sup>129</sup> one would expect them to invest more in security

---

<sup>128</sup> Judge Posner made this point clearly when discussing how to evaluate whether a trade secret holder took “reasonable precautions” to maintain secrecy: “If trade secrets are protected only if their owners take extravagant, productivity-impairing measures to maintain their secrecy, the incentive to invest resources in discovering more efficient methods of production will be reduced, and with it the amount of invention.” *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 180 (7th Cir. 1991).

<sup>129</sup> This is a big “if.” As discussed above, supporters of the economic espionage statute argued that harm to national security is an externality that a trade secret owner does not internalize when its secret is misappropriated.

and, correspondingly, less in invention.<sup>130</sup> In practice, of course, trade secret owners are unlikely to have good information about how the information security threats they face intersect with national security, which might further distort their investments in secrecy.

**Upholding Commercial Morality.** While the mismatch between the efficiency rationale and national security centers on the incentives of inventors, the mismatch between the commercial morality rationale centers on the assumptions about the incentives to which adversaries are likely to respond. The commercial morality justification for trade secrecy holds that the law should protect a party that discloses information to another party as part of a confidential relationship.<sup>131</sup> As the Supreme Court has written, “[t]he necessity of good faith and honest, fair dealing, is the very life and spirit of the commercial world.”<sup>132</sup>

Even within the confines of U.S. trade secret law, defining generally accepted industry norms, and determining whether a firm complies with them, is difficult.<sup>133</sup><sup>166</sup> When globalized industries, multinational firms, and foreign actors enter the picture, the question of where to look for industry norms becomes even more daunting.<sup>134</sup>

---

<sup>130</sup> The same reasoning leads to the conclusion that trade secret owners would be more reluctant to disclose. Raising the expected cost of disclosing a trade secret, by adding harm to national security to the private harm that the trade secret owner might suffer, would discourage owners at the margin from disclosing.

<sup>131</sup> The leading statement of this view comes from *E.I. Du Pont de Nemours Powder Co. v. Masland*, which held that trade secret law ought to punish breaches of confidentiality. 244 U.S. 100, 102 (1917).

<sup>132</sup> *Kewanee*, 416 U.S. at 481-82 (internal quotation and citation omitted).

<sup>133</sup> See Bone, *supra* note 147, at 294-96 (“A court cannot therefore simply condemn conduct as wrongful while nodding in the direction of industry practice; the court must offer convincing evidence that the practice exists. . . . For an industry norm to exist, it must be part of a relatively stable industry-wide equilibrium. Such an equilibrium often will be supported by non-legal sanctions imposed informally within the industry.”) (citations omitted).

<sup>134</sup> *Id.*

In practice, the EEA might obviate some of this inquiry. The offenses are defined under the Act in terms of taking a trade secret “without authorization.”<sup>135</sup> This standard broadens the civil conduct standard of “improper means,”<sup>136</sup> but it does not necessarily clarify which conduct is proscribed.<sup>137</sup>

The few decisions issued in trade secret theft cases do not address this element of the statute. Indictments simply allege that the defendants “stole[], appropriated, and obtained without authorization” the information that was at issue in each case.<sup>138</sup> In most cases, confidentiality agreements appear to provide the basis for determining that the defendants acted “without authorization.” Thus, the course of EEA enforcement has not clarified which norms the Act seeks to protect.

It is doubtful that devoting more prosecutorial resources to using the EEA to define norms for international economic information collection would succeed. The basic problem of economic espionage is that agents act on behalf of principals who stand outside a shared system of formal and informal constraints on their conduct.<sup>139</sup> Though EEA supporters emphasized that

---

<sup>135</sup> 18 U.S.C. §§ 1831-32.

<sup>136</sup> Geraldine Szott Moohr, *The Problematic Role of Criminal Law in Regulating Use of Information: The Case of the Economic Espionage Act*, 80 N.C. L. REV. 853, 883 (2002) (arguing that the “ ‘improper means’ that merits criminal penalties has become unauthorized use—freed from the requirement of a confidential relationship”) under the EEA. Some legislative history, however, suggests that Congress did not intend the language to reach too far. For example, Congress did not intend to criminalize reverse engineering.

<sup>137</sup> As Professor Orin Kerr has discussed at length in the context of computer fraud laws, making unauthorized use or access to information subject to punishment is fraught with ambiguity. *See generally* Orin Kerr, *Cybercrime’s Scope*, 78 N.Y.U. L. Rev. 1596 (2003).

<sup>138</sup> Ye & Zhong Indictment at 4 line 18; *id.* at 6 line 2; Meng Indictment at 14-16; Lee & Ge Indictment at 5-6; Chung Indictment at 18 (alleging that Chung “possessed and concealed without authorization . . . trade secrets belonging to Boeing, knowing them to have been appropriated, obtained, and converted without authorization”).

<sup>139</sup> Trade secret provisions in existing international treaties do not address this problem. TRIPS is the most important example. All that TRIPS requires of signatories is that they provide the “possibility of preventing [trade secret] information lawfully within their control from being

the law was justified to prevent other countries from benefiting from U.S. firms' research and development, they ignored the fact that foreign economic information collection is a game played by different rules. A law passed in the United States does not address these rules.<sup>140</sup>

**Punishing Unfair Competition.** Finally, some scholars and courts argue that trade secret law should punish unfair methods of competition. Allowing business firms to breach duties of "good faith and honest, fair dealing" the Supreme Court has noted,<sup>141173</sup> would exact an "inevitable cost to the basic decency of society when one firm steals from another."<sup>142</sup>

This rationale fails to reconcile trade secret protection with the ends of national security for reasons similar to those discussed in connection with industry norms. Foreign governments seeking know-how from U.S. targets are unlikely to be moved by a domestic policy judgment that this behavior is unfair.<sup>143</sup> These governments simply are not playing the same game as private businesses.<sup>144</sup>

The course of the economic espionage statute's enforcement has built on and enhanced this rhetoric, even when the substance some economic espionage cases appear to have a tenuous connection to national security interests. Finally, in its oversight of economic espionage threats and enforcement of the statute, Congress has relied mainly upon sources whose perspectives are oriented toward national security.

---

disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices." TRIPS art. 39(2)

<sup>140</sup> See Part V for a discussion of how to change this situation.

<sup>141</sup> *Kewanee*, 416 U.S. at 482.

<sup>142</sup> *Id.* at 487.

<sup>143</sup> See, e.g., Richard A. Posner, *THE PROBLEMATICS OF MORAL AND LEGAL THEORY* 75 (1999) ("[N]orms are more effective when people are under the observation of their peers.").

<sup>144</sup> See *supra* Part III.A.

## ***B. The Curiously Narrow Enforcement History***

The record of the economic espionage statute's enforcement also provides evidence that it is doing little to advance U.S. national security interests. Despite some organizational shifts that have established more formal ties between enforcement of the statute and agencies holding national security-related authority,<sup>145</sup> the actual record displays a dearth of evidence that the statute is much help in controlling espionage.

The facts alleged in actual cases also show some movement toward handling misappropriation of information that lies closer to the core national security concerns that the economic espionage statute was intended to address. This movement was almost inevitable, given the facts of the first economic espionage prosecution. In that case, two Japanese scientists were charged with misappropriating and destroying genetic materials owned by a medical research foundation.<sup>146</sup> National security did not get a mention in official statements announcing the indictments.

---

<sup>145</sup> For example, an FBI representative testified in 2000 that efforts to enforce § 1831 catalyzed cooperation between law enforcement and the intelligence communities:

There are a number of ways that we look at and approach economic espionage in the FBI and intelligence community-wide. We're not doing this ourselves, we are enjoined [sic] with the Department of Defense, the Central Intelligence Agency, Commerce, Customs, et cetera. This is not an FBI, unilateral responsibility. But we sort of coordinate it. And one of the main ways we do that is utilizing the Economic Espionage Act of 1996, . . .

Testimony of Sheila Horan Before the House International Relations Committee, Sept. 13, 2000. The other major change occurred in 2006, the National Security Division of the Justice Department took control of economic espionage prosecutions.

<sup>146</sup> U.S. Dept. of Justice, First Foreign Economic Espionage Indictment; Defendants Steal Trade Secrets from Cleveland Clinic Foundation, May 8, 2001, *at* [http://www.usdoj.gov/criminal/cybercrime/Okamoto\\_SerizawaIndict.htm](http://www.usdoj.gov/criminal/cybercrime/Okamoto_SerizawaIndict.htm). The case ended with one defendant pleading guilty to making a false statement to investigators and Japan refusing to extradite the other defendant. Tetsuya Morimoto, First Japanese Denial of U.S. Extradition Request: Economic Espionage Case, *Northwestern Law—In the News*, July 1, 2004, *at* [http://www.law.northwestern.edu/news/article\\_full.cfm?eventid=1395](http://www.law.northwestern.edu/news/article_full.cfm?eventid=1395).

Subsequent cases show three clear trends—to the extent one may infer a trend from so few cases—that pertain to national security impact of the economic espionage statute. The first trend is that all of these cases involve defendants who are Chinese citizens or persons of Chinese descent and stand accused of misappropriating trade secrets to benefit China. This focus is consistent with assessments from the intelligence community and elsewhere that China is engaged in a well-funded and sustained effort to catch up with the technology base of the United States and other highly industrialized nations. But the absence of any espionage benefiting a country other than China is peculiar, given that one or two dozen countries are alleged to be major perpetrators. The fact that a broad array of countries has been implicated in economic espionage’s “neighbor” statutes suggests the same thing.

Second, the prosecutions dealing with China, taken together, show that prosecutors are taking greater pains to highlight the national security implications of the cases they bring. Specifically, two cases have called attention to an alleged link between the defendants and China’s “863 Program.” The 863 Program is a government-sponsored research program that appears to employ a wide range of tactics, legal and illegal, within the United States, to collect scientific and technical information.<sup>147</sup> In a press release announcing the indictment of Fei Ye and Ming Zhong, the Department of Justice presented the defendants’ activities as a threat to

---

<sup>147</sup> FBI, Press Release, Dec. 4, 2002, at <http://www.usdoj.gov/criminal/cybercrime/yeIndict.htm>. Suspicion of the 863 Program began before the first economic espionage prosecutions, with China’s rapid emergence as a military and industrial power. The Program was scrutinized in the House of Representatives Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People’s Republic of China (“Cox Report”), which stated that the Program’s purpose is to “narrow the gap between the PRC and the West by the year 2000 in key science and technology sectors, . . .” Cox Report at 11. The Cox Report also called attention to the fact that military and dual-use technologies were areas of the 863 Program’s focus, as well as the role of military officials in the Program’s administration. *Id.* at 13. Still, the Cox Report did not state expressly that the 863 Program served as a vehicle for economic espionage.

“the integrity of the economy,” which, had it been successful, would have given China “a powerful capability to compete with worldwide leaders’ . . . in the field of integrated circuit design.”<sup>148</sup>

This is probably an overstatement. Ye and Zhong were charged with stealing trade secrets relating to the microprocessor design. There is no indication in the indictment or elsewhere that these designs were classified or export-controlled. The indictment does state that a Chinese government review committee found that the technology Ye and Zhong were found attempting to steal had “important significance for the development of China’s high-level embedded CPU,” would help China’s integrated circuit industry, and recommended further government support.<sup>149</sup> Thus, the concern in this case apparently was not that trade secrets at issue carried national security significance on their own, but rather that they might allow China to develop its own capacity to build certain kinds of computer chips.<sup>150</sup>

Similarly, the U.S. Attorney who signed the indictment of Lan Lee and Yuefei Ge stated, “[t]he vigorous enforcement of intellectual property statutes increases the economic vitality of [northern California], and adds to the security of our nation as a whole.”<sup>151</sup> The DOJ’s statement also tied the defendants to China’s 863 program—a link the defendants later admitted<sup>152</sup>—but

---

<sup>148</sup> *Id.* In Senate testimony given after Ye and Zhong had pleaded guilty to economic espionage, FBI Director Robert Mueller turned up the rhetoric. He cited the convictions as an example of protecting the United States from the theft of its “most sensitive secrets.” Robert S. Mueller, III, Statement Before the Senate Judiciary Committee, Mar. 5, 2008, at <http://www.fbi.gov/congress/congress08/mueller030508.htm>.

<sup>149</sup> Ye & Zhong indictment, at 3-4.

<sup>150</sup> This echoes the “leapfrog” argument made in support of the economic espionage statute in Congress. See Part III.A.2.

<sup>151</sup> U.S. Dept. of Justice, Two Bay Area Men Indicted On Charges Of Economic Espionage, Sept. 26, 2007, at <http://www.usdoj.gov/criminal/cybercrime/liIndict.htm>.

<sup>152</sup> Dan Levine, *DOJ’s Economic-Spy Strategy Emerges*, The Recorder, May 5, 2008, at <http://www.law.com/jsp/article.jsp?id=1202421126406>.

added a gratuitous paragraph about the Chinese military's support for and use of the 863 program.<sup>153</sup>

Other prosecutions, though they do not refer to the 863 Program, make it clear that prosecutors sought to emphasize the national security significance of the cases they brought. For example, in a statement announcing the sentencing of Xiaodong Sheldon Meng, who was accused of stealing trade secrets relating to military flight simulation and night-vision goggles,<sup>154</sup> the Assistant Attorney General for National Security stated that the “case demonstrates the importance of safeguarding sensitive U.S. military technology as well as trade secrets. It should also serve as a warning to others who would compromise our national security for profit.”<sup>155</sup> Finally, in the announcement of the indictment of Dongfan Chung, who was charged with misappropriating trade secrets relating to the Space Shuttle, a military transport plane, and a satellite launch rocket,<sup>156</sup> a U.S. Attorney involved in the case stated that “[d]isclosure of this information to outside entities like the PRC would compromise our national security.”<sup>157</sup>

---

<sup>153</sup> DOJ Press Release, *supra* note 83.

<sup>154</sup> U.S. Dept. of Justice, Former Chinese National Charged with Stealing Military Application Trade Secrets from Silicon Valley Firm to Benefit Governments of Thailand, Malaysia, and China, Dec. 14, 2006, at <http://www.usdoj.gov/criminal/cybercrime/mengCharge.htm> [Meng Announcement]. Note that the products with exclusively military applications were classified as “defense articles” that cannot be exported without a license. This kind of classification represents a different information protection paradigm and an alternative to the trade secret-based paradigm of the economic espionage statute.

<sup>155</sup> DOJ Press Release, June 18, 2008. *See also* Meng Announcement, *supra* note \_\_ (stating that Meng’s activities jeopardize[d] our country’s military advantages in the world”).

<sup>156</sup> *See* U.S. Dept. of Justice, Former Boeing Engineer Charged with Economic Espionage in Theft of Space Shuttle Secrets for China, Feb. 11, 2008, at [http://www.usdoj.gov/opa/pr/2008/February/08\\_nsd\\_106.html](http://www.usdoj.gov/opa/pr/2008/February/08_nsd_106.html). This statement identifies the rocket in question as Boeing’s Delta IV, *id.*, which appears to be used to launch military satellites, Boeing Co., Integrated Defense Systems Delta IV Overview, at <http://www.boeing.com/defense-space/space/delta/delta4/delta4.htm> (last visited Jan. 21, 2009).

<sup>157</sup> *Id.* The Assistant Attorney General for National Security also stated that economic espionage threatens “our economic and national security.” *Id.*

The third pattern is that method of cyber-based economic espionage is conspicuously absent from these cases. Given that intelligence and law enforcement officials continue to emphasize both the severity of the economic espionage threat and the growing role of cyber attacks as a method of espionage, one would expect to see increasing numbers of criminal prosecutions in which these methods play a role. Specifically, intelligence community assessments strongly hint that China is responsible for at least some cyber-based espionage, though they note that it is difficult to attribute these attacks to state actors or to infer state sponsorship for them.<sup>158</sup> The U.S.-China Economic and Security Review Commission has been more direct. In its most recent report to Congress, the Commission states that there may be 250 or more “hacker groups” active in China and, though it did not present any direct evidence that these groups are state-sponsored,<sup>159</sup> it argued that the Chinese government’s pervasive monitoring of Internet communications means that the government is aware of the groups’ activities and tolerates or even encourages them.<sup>160</sup>

Perhaps the overall absence of cyber methods in these cases is due to the sufficiency of evidence obtained from other sources. Perhaps investigators are unwilling to reveal their own sources and methods for collecting information about cyber attacks. And, as discussed earlier, evidence about Internet-based attacks can be particularly difficult to obtain and, even if available, nearly impossible to use to attribute actions to a particular individual or may lead to an individual who is effectively impossible to extradite.<sup>161</sup> Economic espionage prosecutions also

---

<sup>158</sup> *Id.*

<sup>159</sup> USCC 2008 Report at 164.

<sup>160</sup> USCC 2008 Report at 164 (“[T]he Chinese government closely monitors Internet activities and is likely aware of the hackers’ activities.”).

<sup>161</sup> Extraterritorial jurisdiction is something that the FBI asked for and received in the EEA. To wield this power, the government must be able to extradite suspects from other countries. It has made only one such attempt and was unsuccessful.

take a long time to assemble. In some cases, the conduct at the heart of a case has transpired over years or decades, and investigations may take a few additional years. Thus, there may be a lag between the methods that have appeared in indicted cases and those that are currently under investigation. Finally, detecting cyber-based access to and misappropriation of information is difficult.<sup>162</sup> An incident might not become evident unless a trade secret holder knows what to look for, and actually looks for it. Even then, firms are generally under no obligation to report intrusions to law enforcement or intelligence agencies.<sup>163</sup> Thus, cyber-espionage might be both under-detected and under-reported.<sup>164</sup> Still, despite (or perhaps because of) the lack of data concerning the use of cyber-espionage, this method plays a large role in the discourse surrounding both economic espionage and cybersecurity.

### **C. Complacent Oversight by Congress**

Members of Congress have not pressed either law enforcement or intelligence officials to explain the narrow focus of economic espionage enforcement. Nor has Congress used its oversight capacity seriously to address whether the statute is playing a constructive role in addressing the problem of economic espionage. Instead, Congress has relied on sources that tend to confirm the national security narrative that promoted the economic espionage statute and to blur the fundamental differences between protecting trade secrets and national security

---

<sup>162</sup> See FECIE 2005 at 10 (“Detection of intrusions is difficult.”).

<sup>163</sup> *Contra* the requirements of state security breach notification (SBN) laws, which generally require disclosure following a leak of personally identifiable information. See generally Security Breach Notification Laws: Views from Chief Security Officers. Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law, Dec. 2007, at [http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso\\_study.pdf](http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso_study.pdf).

<sup>164</sup> See General Accounting Office, Economic Espionage: The Threat to U.S. Industry (GAO/T-OSI92-6, Apr. 29, 1992):

[S]ophisticated methods are used in espionage against U.S. companies.

Unfortunately, the companies targeted by foreign intelligence agencies may not know—and may never know—that they have been targeted or compromised.

Quoted in GAO/NSIAD-96-64 Defense Industrial Security at 20.

information. For example, a member of the U.S.-China Economic and Security Review Commission testified in 2008 that there is little difference between economic espionage and espionage traditionally defined: “[M]y own view is that today it is often difficult to distinguish between what we define as espionage related to the national defense under the Espionage Act . . . and economic espionage or the theft of proprietary information and trade secrets covered by the Economic Espionage Act . . . .”<sup>165</sup>

Intelligence community assessments point in the same direction. The community’s annual reports to Congress, for example, identify joint ventures and simple purchases of technology as “methods” of economic espionage. But those methods are not theft of trade secrets at all. Instead, foreign investment in and transactions for either specific information or for entire companies represent ways that the interests of private parties and the government can diverge in the protection of trade secrets.<sup>166</sup> There may be national security reasons to block or modify these transactions, but they are not rooted in trade secret misappropriation.

#### ***D. Stunted Understanding of Economic Espionage Threats***

The information vacuum left by the current legal structure for dealing with economic espionage that creates a dual hazard. First, it may lead policymakers to focus undue attention on a single threat, namely, China. But, second, the same information vacuum may lead policymakers to overreact, prescribing policy solutions that are not justified by the actual threats. I address these problems in turn in the rest of this Part.

---

<sup>165</sup> Testimony of Larry Wortzel Before House Judiciary Committee, Jan. 29, 2008. This witness went on to disparage practices that trade secret law recognizes as legitimate; he lumps together “shameless[] stealing” with reverse engineering. *Id.*

<sup>166</sup> See *infra* Part IV.

## 1. A Hypothetical

Taking a step back from the indictments and the statements of the U.S.-China Commission, one can find room to doubt that the main purpose of the 863 Program—the funding program at the center of two indictments—is to develop an economic espionage force. More generally, some reflection suggests that the overall picture of highly disciplined Chinese agents posing as scientists to carry out the mission of a well funded, sustained, centrally controlled attack on the technological know-how of U.S. firms is a bit distorted.

To change the facts from economic espionage indictments slightly, suppose that a U.S. scientist was arrested in Beijing with disks full of software source code obtained from a Chinese company. Suppose further that the scientist possessed a grant proposal for the Defense Advanced Research Projects Agency (DARPA), as well as an email from a Department of Defense program manager assuring him that engaging in classified research would not ruin his life by precluding him from publishing results from other work in academic journals. This hypothetical scientist also has documents showing evidence of venture capital funding to start a company to commercialize his research and state and local tax credits to locate the company in the same town as the university at which he teaches.

To an observer familiar with collaborations in the United States among academia, government, and private industry, these might seem like desirable but not extraordinary assets. But the pieces do not add up to show that the scientist was acting to benefit the government. Someone unfamiliar with the institutional structure of U.S. scientific research, however, might take note of the DARPA funding application and the tax credits, and conclude that the scientist was being induced by government officials at all levels to try to take trade secrets out of China.

The purpose of this hypothetical is not to suggest that it was wrong to use the economic espionage statute against any of the individuals who have so far been charged. Instead, I want to suggest that a lack of familiarity with a country's institutions can make certain conduct appear far more integrated into a national plan than it actually is. The image of China as a sponsor of economic espionage is that it uses a well-disciplined, military-controlled hierarchy to provide scientific and technological funding to individual scientists. The body of public evidence that supports this image is composed of instances illicit activities that are not balanced by reference to other ways of gaining knowledge, such as developing indigenous talent and learning from published sources. Criminal prosecutions, of course, do not provide a forum for taking all of these considerations into account. The effect in the United States is to leave policymakers without context for assessing how serious threats are; the effect on China is to create an antagonistic atmosphere in official relations.

In any event, evidence from outside economic espionage cases and government reports suggests a more subtle picture of Chinese government sponsorship of espionage. The 863 Program and other funding avenues might involve both Chinese government complicity with economic espionage activity, with a unified vision of technological objectives, with an unwieldy bureaucracy that makes it hard to oversee all activities that are carried out—officially or unofficially—to fulfill those objectives.

## **2. Reassessing the Chinese Economic Espionage Threat**

And indeed, the official purpose of the 863 Program is to provide government funding for basic and applied scientific research and development by industry and academia.<sup>167</sup> It is jointly administered by the State Commission of Science, Technology, and Industry for National

---

<sup>167</sup> Official 863 Program Web site, *supra* (memo on file with author).

Defense, and the Ministry of Science and Technology.<sup>168</sup> Initially, the 863 Program established 15 “themes of interest” (later increased to 20), including information technology, aerospace, and pharmaceuticals; and the program set development goals on a 15-year timeframe. The original, stated goal of the 863 Program was to bring China’s scientific and technological capabilities even to the United States and other Western powers.<sup>169</sup> According to the official government website, the 863 Program seeks to promote international collaboration.<sup>170</sup> Recipients of 863 funding enter into a contract with the government to allocate IP rights for work done with the funding.<sup>171</sup> The standard contract grants IP rights to the person or firm who received the funding, provided that the rights are exploited primarily through the production of goods or services within China.<sup>172</sup> When an 863-funded project concerns national security, researchers must sign non-disclosure agreements and keep information relating to the project confidential.<sup>173</sup> Chinese officials have repeatedly denied that the 863 Program supports trade secret theft.<sup>174</sup>

A story that further illustrates this point, but has not made it into official U.S. sources, is that of the Arca-3 project. ARCA, a chip design firm in Zhongguanchun Science Park, “Beijing’s Silicon Valley,”<sup>175</sup> had developed two generations of computer chips with millions of dollars of

---

<sup>168</sup> Report of the U.S. House of Representatives Select Committee on U.S. National Security and Military/Commercial Concerns with the People’s Republic of China 13, Jan. 1999, <http://www.house.gov/coxreport/>.

<sup>169</sup> USCC 2007 Report at 127.

<sup>170</sup> Private companies may apply for 863 funding, provided that the applicant company is controlled by Chinese persons.

<sup>171</sup> Notice of Managing Intellectual Property Rights of Projects from National High Technology Research and Development Program [hereinafter “863 Contract”] (on file with author).

<sup>172</sup> 863 Contract.

<sup>173</sup> Official 863 Program Web site, *supra* (memo on file with author).

<sup>174</sup> Liu et al., *supra* note 176.

<sup>175</sup> Wu Zhong, *Two chip scandals set back China’s IT industry*, ASIA TIMES ONLINE, July 4 2006, [http://www.atimes.com/atimes/China\\_Business/HG04Cb06.html](http://www.atimes.com/atimes/China_Business/HG04Cb06.html).

financial support from the Chinese government.<sup>176</sup> The government’s interest was in making China into a leader in processor technology, rather than remaining “the world’s low-cost manufacturing workshop.”<sup>177</sup> ARCA then secured funding from the 863 Program to produce a third generation chip. After ARCA failed to meet deadlines, it was audited by government officials, who found that ARCA had spent much of its funding constructing a building and paying its employees salaries that violated ARCA’s contract with the government.<sup>178</sup> This scandal followed the revelation that a top academic scientist in China had not developed a home-grown computer chip with his government funding, but had simply replaced the trademarks on U.S.-produced chips.<sup>179</sup> Though these are isolated anecdotes, they provide some counterweight to the official narrative about China in the United States: that it funds and centrally directs the activities of a vast team of scientist-spies. This narrative, after all, is also based on anecdotes. The ARCA example illustrates that there may be mechanisms in China and other countries that can enforce norms of fair competition. Appealing to other nations to use these mechanisms could go a long way toward protecting the interests that motivated the economic espionage statute. I return to this idea in Part V.

Another hazard of focusing on China is that the United States might be neglecting to address espionage by other actors. The cases do not very closely track the diversity of countries that are engaged in economic espionage. France, Israel, Russia, and India have all been cited for a long time as economic espionage threats. Nothing suggests that these threats have abated; yet, aside from Russia, these countries are rarely mentioned in official discussions of economic espionage. As discussed above, one or two dozen countries have been major threats over the

---

<sup>176</sup> Wu, *supra* note 202.

<sup>177</sup> *Id.*

<sup>178</sup> *Id.*

<sup>179</sup> *Id.*

past decade; but all prosecutions except one have targeted individuals alleged to be working for the benefit of Chinese instrumentalities.

Several explanations are consistent with this observation, and it is difficult to accept or reject any of them based on publicly available evidence. Perhaps the defendants in these cases revealed themselves by being uncommonly bold or foolish. Evaluating this explanation would require knowing more about the methods of economic spies acting on behalf of other countries. Another explanation is that the information at stake in these cases was so sensitive that the government decided to pursue the harsh penalties provided by the economic espionage statute, despite the difficulty of proving the defendant's intent to benefit a foreign instrumentality. That is, prosecutors might have given these cases priority because of their deterrence value. A third explanation for the pattern of economic espionage prosecutions is that the government used alternative statutes to address threats from other countries. Official counterintelligence documents lend some support for this explanation. Citizens from ten countries, including China, have been prosecuted under for violations of export controls and related crimes.<sup>180</sup>

## **V. Toward Better Mechanisms for Discouraging Economic Espionage**

The basic flaw in the current economic espionage legal regime is that depends heavily on enforcement of § 1831. This is a contrast with the more general problem of espionage, which depends on government control of information, incentives to protect information using measures that are commensurate with its national security significance, and formal and informal

---

<sup>180</sup> The other countries are Cuba, India, Indonesia, Iran, Iraq, Pakistan, Suriname, and the United Arab Emirates. FECIE 2007 at 9-14. The related crimes include money laundering and “process crimes,” such as making false statements to investigators. See Erin Murphy *The Crime Factory: Process, Pretext, and Criminal Justice*, 97 GEO. L.J. (forthcoming 2009) (discussing process crimes); FECIE 2007 at 9-14 (listing espionage-related convictions).

international rules to constrain behavior. The economic espionage statute did not create any of this structure.<sup>181</sup> Though enforcement of the statute has a role to play in regulating economic espionage, this alone is not sufficient. The basic conditions that made economic espionage an appealing enterprise when the EEA was passed—trade secret holders with insufficient resources and incentives to protect their information against sophisticated threats, law enforcement and intelligence agencies that depend on the voluntary cooperation of the private sector, and the absence even of nascent norms concerning proper modes of gathering information via networks—prevail today. A strategy that builds on the same structure is unlikely to change these conditions.

This Part considers how the available legal and institutional mechanisms might be used to better regulate economic espionage. In Part V.A I consider potential amendments to the economic espionage statute. These fall into two categories: enhancing the law's current penalties, and altering the incentives of trade secret holders to protect their information. There is a trade-off between these two types of proposals. Making the economic espionage statute stronger would build on the basic design of trade secret rights, but it would do little to affect owners' incentives to invest in protecting information. Mechanisms designed to induce trade secret holders to invest more in protection, by contrast, would require modifying some of the basic features of trade secret rights.<sup>182</sup>

---

<sup>181</sup> When information considered a trade secret is also classified or subject to export controls, some or all of these mechanisms come into play. Indeed, in those cases, trade secrecy is somewhat of a secondary consideration. But, as the prosecutions discussed in Part \_\_\_, *supra*, demonstrate, there may be a national security interest in preventing the disclosure of information that is not subject to these regimes, as well as the general interest in protecting trade secrecy as part of a program to maintain national economic security.

<sup>182</sup> See *supra* Part IV.A.

Using the policy mechanisms that are currently in place to deal with economic espionage holds some promise for reducing the harm from economic espionage. Extending these approaches, however, would also entail some potentially significant costs for a questionable benefit. Part VI.A explores these trade-offs. Ultimately, more effectively preventing economic espionage depends on changing the incentives of the nations that sponsor it, and the current law enforcement and counterintelligence provides little hope of doing so. I therefore propose in Part VI.B a diplomatic approach that would explicitly recognize the problem of economic espionage. Finally, Part VI.C emphasizes the importance of taking the right approach to economic espionage, especially in light of its current role in illustrating the national security implications of cybersecurity.

## ***A. Two Ways to Amend the Economic Espionage Statute***

### **1. Strengthening the Economic Espionage Statute**

Though there is little evidence that narrow scope is an obstacle to bringing economic espionage prosecutions, this possibility is worth considering, especially in light of Congress' tendency to address perceived failures of intellectual property laws by expanding their scope. Congress could strengthen the economic espionage statute either by amending § 1831 to prohibit more conduct or expanding the definition of a trade secret under the EEA.

To bring more conduct within the statute's prohibitions, could either by relax the mens rea elements of the economic espionage statute or by broad the current definition of the bad act – taking information “without authorization” – that it targets. Prohibiting additional conduct under the economic espionage statute, however, would create additional uncertainty as to how the EEA maps onto state-based trade secret law. Already – perhaps out of a concern to avoid chilling

conduct that the EEA does not explicitly protect<sup>183</sup> – prosecutors have brought EEA cases in which the alleged conduct would clearly violate civil trade secret law.<sup>184</sup> Prohibiting more conduct, only to have prosecutors refrain from using a more expansive statute to avoid these chilling effects, would be pointless. Similarly, Congress could relax the mens rea standard that distinguishes economic espionage from trade secret theft, namely “intending or knowing that the offense will benefit any foreign government.”<sup>185</sup> Dropping below a standard of intentionality, however, would erase much of the distinction between economic espionage and trade secret theft.

Nor would expanding the EEA’s definition of trade secrecy be likely to do much to make economic espionage easier to prosecute. As the law currently stands, the EEA already gives trade secret holders a broad right against the world.<sup>186</sup> Moreover, as discussed above, the fundamental difficulty of economic espionage enforcement is that most trade secret holders do not have the incentives or resources to protect information at the level required by national security, while the government has limited access to information that would help it to address espionage through law enforcement or counterintelligence. Somehow expanding the definition

---

<sup>183</sup> For example, there is no exemption for reverse engineering.

<sup>184</sup> [CITE] Rustad. This statement applies to both the economic espionage and trade secret theft sections of the EEA. Pooley et al. predicted this outcome. See *supra* note \_\_, at 192-93 (noting that the EEA “makes it a crime to ‘appropriate’ or ‘take’ a secret without authorization from the trade secret owner. These terms might encompass the sort of lawful business espionage that has long been permitted by civil trade secrets law – conduct such as observing a competitor’s property from across the street” but also noting that it is “extremely unlikely that a United States Attorney will prosecute a defendant for activities that are permitted under civil trade secrets law”).

<sup>185</sup> 18 U.S.C. § 1831(a).

<sup>186</sup> See Moohr, *supra* note \_\_, at 898-903; Pooley *et al.*’s caveat has largely been borne out so far.

of trade secrecy without better aligning trade secret holders' incentives with national security interests would do little to address this fundamental problem.<sup>187</sup>

## 2. Changing Trade Secret Holders' Incentives to Invest in Information Security

To address this problem of incentives, Congress could use two other approaches. The first is to make trade secret holders criminally liable for losing information through economic espionage. The original proponent of this idea admits that it “may seem like blaming the victim”<sup>188</sup> but also makes a thoughtful case that creating criminal liability for losing a trade secret to a foreign agent is analogous to regulatory offenses.<sup>189</sup> Both types of offenses are meant to induce actors to internalize some of the costs of the public harms that are associated with their acts or omissions.<sup>190</sup> Blaming the victim, under this proposal, is a last resort that recognizes not only the national-level harm that can result from economic espionage as well as the fact that the principals sponsoring the activity—foreign governments—are effectively beyond the reach of the law.<sup>191</sup>

Fortunately, a less severe approach might be feasible. Drawing on the recent development of state laws requiring businesses to report breaches resulting in the loss of

---

<sup>187</sup> For these same reasons, to the extent that addressing economic espionage is a rationale for creating new state or federal civil causes of action for trade secret misappropriation, I am skeptical of such proposals. *See* Rustad, *supra* note \_\_, at 515-25 (proposing creating a federal civil right of action for trade secret theft as well as a cause of action for negligent enablement). Such changes would not alter any of the three conditions that make economic espionage an especially difficult problem. I limit this assessment to economic espionage and offer no assessment of these proposals' merits with respect to generic trade secret misappropriation.

<sup>188</sup> Brenner, *supra* note \_\_, at \_\_.

<sup>189</sup> *Id.*

<sup>190</sup> *Id.* (noting that “More than a century ago, American criminal law began to use regulatory offenses to create ‘forward-looking incentives yielding socially optimal outcomes’”) (quoting Louis Michael Seidman, *Points of Intersection: Discontinuities at the Junction Of Criminal Law and the Regulatory State*, 7 J. CONTEMP. LEGAL ISSUES 97, 142 (1996)).

<sup>191</sup> *Id.* (main text following n. 322).

personally identifying information (PII),<sup>192</sup> Congress could require trade secret holders to report suspected trade secret misappropriation. The rationale for breach reporting in the case of PII is that the expected costs of a breach—the immediate costs of notifying and offering some protection to affected customers, as well as the less certain but potentially profound costs exacted through harm of the firm’s reputation—give firms incentives to make additional investments in protecting information.<sup>193</sup> This rationale roughly maps to trade secret protection: some of the harms are widely distributed, and silence often pays because it allows firms to escape reputational harm.<sup>194</sup>

Publicly disclosing instances of trade secret misappropriation, of course, might reveal details of foreign intelligence operations that the intelligence community would prefer to keep confidential. A parallel concern arises in the PII breach-reporting context with respect to harming ongoing criminal investigations; the solution in such cases is to delay reporting until it would no longer affect the investigations. These and many other details would need to be worked out to arrive at a practical proposal. For example, policymakers would need to decide upon triggers for breach reporting, the appropriate recipient(s) of reports, penalties for failing to comply with reporting requirements, and an agenda for using breach reports. Discussing these details is beyond the scope of this Article.

---

<sup>192</sup> For a thorough account of the development of these laws and an assessment of their effectiveness, see generally Deirdre K. Mulligan, *Assessing Security Breach Notification Laws* (draft paper on file with author).

<sup>193</sup> *See id.*

<sup>194</sup> Professor Andrea Matwyshyn argues that another harm that results from a reluctance to disclose information about security breaches: it indicates that firms “are not discussing the security risks they face and, therefore, tend not to create a feedback loop for external assessment of their data security processes and risks through disclosure.” Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 Berkeley Bus. L.J. 129, 180-81 (2005).

## ***B. Improving the Understanding of Economic Espionage Threats Through Public-Private Cooperation***

A shortcoming of a mandatory trade secret misappropriation reporting regime is that it is largely a reactive strategy. Though firms subject to a reporting requirement should have incentives to invest in additional information security measures, the government—which has the expertise necessary to evaluate threats involving state actors—remains in the dark until a breach occurs. This not only limits the government to information relating to breaches that are successful and detected but also deprives the government and firms of the opportunity to take coordinated, preventive measures. Put simply, private organizations and government agencies both hold information that could be used to prevent economic espionage; but they lack the structure and incentives to share this information.<sup>195</sup>

This dilemma has led to a series of calls for improving public-private information sharing. The general premise of these arrangements is that collecting information from many disparate sources – private firms facing economic espionage threats – allows a centralized analyst to detect patterns that would not be apparent to individual firms. In principle, the payoff to firms for investing the time and effort to select information to share is that they will receive timely, actionable information to allow them to better detect and mitigate the kinds of sophisticated attacks that law enforcement and counterintelligence officials and Congress would like to address. The problem is that firms do not want sensitive information to leak to

---

<sup>195</sup> An important exception is the compulsory, ex post required under the arms export control restrictions and CFIUS regulations discussed in Part III.B. These regulations provide mechanisms to allow some government supervision of disclosures of trade secrets and other information to potential adversaries. This structure has the virtue of working on a disclosure-prevention model and allowing a broad set of considerations to enter into decisions about whether disclosures would raise national security issues. Its limitations are that it is cumbersome for businesses and addresses only a subset of the information that is at risk through economic espionage.

competitors and so are unwilling to share it directly or even through a third party. Though using a government agency as the collector and analyst of information alleviates the concern of sharing information directly with competitors, it leaves open the risk that information will be exposed by accident or in response to FOIA requests.<sup>196</sup>

Historically, however, the government has failed to close the loop.<sup>197</sup> One apparent exception is an effort by the Departments of Defense and Homeland Security to gather, analyze, and disseminate threat information to defense contractors.<sup>198</sup> According to the information available about the program, the government is thus far avoiding its tendency to keep threat information bottled up.<sup>199</sup>

It is unclear whether this model is appropriate for sectors other than defense. The DoD's information sharing program appears to have been born of a sense of crisis based both on the scale of cyber-based economic espionage and the sensitivity of information being targeted.<sup>200</sup> Thus, private firms bought into the program, and the government recognized that those firms

---

<sup>196</sup> To address FOIA risks, recent statutes that seek to promote information sharing provide broad FOIA exemptions for information shared with the government. See, e.g., Homeland Security Act § 214 (exempting voluntarily disclosed critical infrastructure information from disclosure under FOIA). These exemptions have, in turn, provoked the criticism that they inhibit government transparency.

<sup>197</sup> See CSIS report, *supra* note \_\_, at 44 (“The government seems to believe that it must share information with everyone or no one, and because sharing with everyone poses risks for both companies and the government, the exchange of information is constrained and awkward.”).

<sup>198</sup> See Ellen Nakashima, Defense Dept., Industry Join to Protect Data, Wash. Post, May 25, 2009, at [http://www.washingtonpost.com/wp-dyn/content/article/2009/05/24/AR2009052402140\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2009/05/24/AR2009052402140_pf.html). As this article states, “The goal is a swifter, more coordinated response to threats facing the defense industry. But intelligence and law enforcement agencies have been reluctant to release threat data they consider classified. And the companies have been reluctant to share intrusion data, for fear of losing control over personal or proprietary information.” *Id.*

<sup>199</sup> *Id.*

<sup>200</sup> *Id.*

were in the best position to implement defenses.<sup>201</sup> Firms in other sectors of the economy would probably reach different conclusions about the costs and benefits of engaging in this kind of information sharing partnership. Moreover, the government has substantially less financial leverage over firms in non-defense sectors.<sup>202</sup>

A necessary companion to increased public-private information sharing is vigorous oversight by Congress to ensure fulfillment of statutory objectives<sup>203</sup> and provide a check on the strategic direction of—and possible abuses by—executive agencies. Congress should use its authority to build a more comprehensive picture of the current scope and severity of economic espionage threats. This is especially important in light of the importance of economic espionage as a harm that cybersecurity advocates use to illustrate the harm that can result from cyber attacks.<sup>204</sup> As President Obama and Congress consider reorganizing parts of the federal

---

<sup>201</sup> The centrality of private firms has been a foundation of infrastructure protection policy since the first major studies of the subject in the mid 1990s. *See* President’s Commission on Critical Infrastructure Protection, *CRITICAL FOUNDATIONS: PROTECTING AMERICA’S INFRASTRUCTURE* 19 (1997) (“The government and private sector share substantially the same national information infrastructure. Both have been victims of unauthorized computer intrusions, theft, and disruption. In our view, the line separating threats that apply only to the private sector from those associated with traditional national security concerns must give way to a concept of shared threats . . .”).

<sup>202</sup> For example, no agency in the energy sector comes close to the influence the Defense Department obtains through requirements imposed through regulations and, perhaps more importantly, through contracts.

<sup>203</sup> *See generally* GAO, *Federal Efforts Are Helping to Address Some Challenges Faced by State and Local Fusion Centers*, Apr. 17, 2008.

<sup>204</sup> *See, e.g.*, Amit Yoran, Testimony Before the House Permanent Select Committee on Intelligence, Sept. 18, 2008 (“Given the pervasive evidence that cyber operations are increasingly the preferred asymmetric method for foreign intelligence services collection against the U.S., the counterintelligence functions need significant prioritization and resources. In a context of cyberspace, these activities often target the economic and industrial bases of the U.S.”); Paul Kurtz, Testimony Before the House Permanent Select Committee on Intelligence, Sept. 18, 2008 (“Government networks are being targeted to steal sensitive information and gain understanding of mission-critical dependencies and vulnerabilities. Corporate intellectual property across all sectors is being stolen (information technology, bio-technology, defense industrial base, financial, transportation, and energy). The NCIX has estimated that the loss of intellectual property totals in excess of 200 billion per year.”).

government and revising statutory authorities to address cybersecurity,<sup>205</sup> Congress could provide a valuable service by pressing all sides to justify their policy prescriptions by explaining threats in terms of the underlying legal harms and identifying which actors are best situated to avoid those harms.

### ***C. Constraining Conduct Through Diplomacy***

Even if policymakers succeed in better aligning private firms' incentives with national security and encouraging effective information sharing, economic espionage threats will not only persist but also adapt to improved technological and procedural defenses. If cyber attacks become a more significant method of committing economic espionage, these adaptations can be quick, and they afford economic espionage sponsors even greater insulation from sanctions than they enjoy by sending human agents to the United States. Finding a way to end, or at least slow down, this arms race would address economic espionage at a fundamental level.

To do so, the United States must gain a better understanding of foreign nations' investments in their industrial infrastructures. I argue in this subpart that engaging directly with other countries in order to gain this understanding is the best approach. While this does not require abandoning law enforcement efforts—as I discussed earlier in the Article, law enforcement is most useful as a complement to international norms surrounding espionage—it does require a shift in focus. The point is to ask, “What are the issues?” and “What are our interests?” rather than “Where is the threat?” and “Who is the enemy?”<sup>206</sup> This shift in perspective is appropriate given the multitude of economic espionage sponsors,<sup>207</sup> an observation

---

<sup>205</sup> See generally *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009.

<sup>206</sup> See DOUGLAS T. STUART, *CREATING THE NATIONAL SECURITY STATE* 296 (2008) (suggesting this reframing in connection with national security institutions generally).

<sup>207</sup> See *supra* notes \_\_.

that motivated much of the support for the EEA in the first place. I recognize that this proposal goes against a strong current in the present state of espionage in international relations.<sup>208</sup> But, in addition to providing policymakers with more information about, such engagement could provide an avenue for establishing internationally observed norms to constrain economic espionage.

The basic idea is to use an international agreement, or a series of bilateral agreements between the United States and other nations of interest, under which the signatories would exchange information about their funding for scientific and technological research and development.<sup>209</sup> In effect, nations that agree to this framework would be able to audit the others' books on scientific research and development, allowing a better identification of who is working on what, and how much they are spending on it. Ideally, participating nations would provide the names of organizations that receive funding, the amount of funding, and contracts between the government and funding recipients.

This more cooperative approach could help in two ways. First, it would remove some of the cover of deniability that surrounds most economic espionage. Audits would allow

---

<sup>208</sup> “No general norm exists in international law expressly prohibiting or limiting acts of intelligence gathering. . . . The fact that no explicit treaty norms address peacetime espionage is paradoxical in light of the enormous amount of intelligence activities and their relevance for international relations between states.” Dieter Fleck, *Individual and State Responsibility for Intelligence Gathering*, 28 MICH. J. INT’L L. 687, 688, 690 (2007).

<sup>209</sup> Existing trade agreements would not do the trick. Most free trade agreements (FTAs) the United States has entered into address trade secrecy through Article 39 of the Trade-Related Aspects of Intellectual Property Agreement (TRIPS), and none address economic espionage at all. See the text of FTAs listed by the U.S. Trade Representative, at <http://www.ustr.gov/trade-agreements/free-trade-agreements>; TRIPS art. 39 (establishing signatories’ obligations to provide legal protection for “undisclosed information”), at [http://www.wto.org/english/tratop\\_e/trips\\_e/t\\_agm3d\\_e.htm#7](http://www.wto.org/english/tratop_e/trips_e/t_agm3d_e.htm#7). These agreements, which include NAFTA among the FTAs, provide procedures for resolving conflicts over trade secret protection through adjudication and alternative dispute resolution procedures that are probably too high profile to be useful for confronting economic espionage. As I explain in the main text, a less formal, lower-profile process is warranted for discussing economic espionage.

governments to present evidence that they are not funding groups to take an economic interest in economic espionage, which could be helpful in assessing currently observed attacks. The United States should have a strong normative position to say that its intelligence community does not pass information to U.S. companies and also that it does not sponsor U.S. companies or individuals to engage in information collection for industrial benefit.<sup>210</sup>

Second, by creating a forum for routine, non-public interactions between governments, audits would provide the basis for gradual shaping of norms. This measure of transparency would allow governments to tout good practices while deterring them from funding efforts that other nations find objectionable.

This approach would face some challenges, but none of them is fatal to the basic idea. One challenge is that neither the United States nor any other nation is likely to want to reveal much about how it funds efforts to develop military and other sensitive technologies. The U.S. government, for example, would not be willing to disclose information about classified R&D contracts. But for other kinds of government funding, information is already publicly available and even electronically searchable.<sup>211</sup> This actually points to a strength my proposal: if the United States could convince other nations to make a similar level of information available, it would gain a lot.

A second challenge is that nations with the most to lose—those that depend most heavily upon economic espionage—would simply refuse to participate in the proposed agreement. This type of hurdle presents itself with any international agreement. Explaining how and why

---

<sup>210</sup> [CITE] CIA statements; need to reconcile with Echelon though.

<sup>211</sup> See, e.g., National Science Foundation, Award Search, <http://www.nsf.gov/awardsearch/> (last visited Mar. 25, 2009) (providing Web interface to search records of current and expired NSF grants).

international agreements develop is a vast undertaking that I do not explore here, except to note that scholars have offered explanations using numerous theoretical frameworks.<sup>212</sup> Instead, I note that the United States already exchanges information with other nations—including China—on such sensitive topics as military training, military technologies, and overall security priorities.<sup>213</sup> These arrangements are not perfect, and they do not override efforts to hide information or gather it clandestinely.<sup>214</sup> Still, they demonstrate that some cooperation is possible in practice and might provide a vehicle for starting discussions about funding scientific and technological development. If an initial set of agreements established that the system was manageable, informative, and did not expose sensitive information, this gradual process might encourage more recalcitrant nations to participate.

A final objection is that this proposal is too incremental. By likely exempting funding for military and at least some dual-use technologies, the information that is exchanged might not help the United States or other countries detect espionage directed toward information that would do the most harm if disclosed. This objection misunderstands the overall structure of economic espionage. The misappropriation of information relating to defense-related industries is not the only way that economic espionage harms a nation's economic interests. Rather, it is the collection of information from a diverse and diffuse group of firms, and the transfer of this information to other nations, that creates the kind of broad, public harm that elevates economic

---

<sup>212</sup> See generally Harlan Grant Cohen, *Can International Law Work? A Constructivist Expansion*, BERKELEY J. INTL. L. (forthcoming 2009) (reviewing rational choice, liberal, and constructivist theories of international law).

<sup>213</sup> See Congressional Research Service, U.S.-China Military Contacts: Issues for Congress, May 10, 2005, at <http://fpc.state.gov/documents/organization/48835.pdf> (reviewing arrangements for information exchanges between U.S. and Chinese military and diplomatic officials).

<sup>214</sup> See *id.*; see also Sara Moore, *Lack of Information About China's Military Spending Concerns Gates*, DEFENSELINK, Mar. 5, 2008, <http://www.defenselink.mil/news/newsarticle.aspx?id=49190> (discussing large disparities between China's reported military spending and its actual spending).

espionage into an issue of national economic security. If misappropriated information leads one nation's industries to lose out to competitors who have benefited from being able to skip the time and expense of research and development, that is a national economic loss, irrespective of whether a military industry was involved. Even if stolen trade secrets allow a nation to cheaply build infrastructure that does not compete directly with the espionage target, the nation committing espionage still benefits from infrastructure that is developed more cheaply and quickly than it otherwise would have been. Of course, a different harm—one more closely tied to traditional conceptions of national security—occurs when information is taken from military-related industries. As discussed above, however, these industries tend to be regulated by more specialized disclosure-prevention regimes. To the extent that a nation is concerned about information leaking from these industries, it would likely do better to improve these sector-specific regulations and their implementation and oversight, rather than attempting to use the more general law of trade secrecy.

## **VI. Conclusion**

Business firms continue to regard trade secrets as a form of intellectual that they are best situated to decide how to protect, and the Economic Espionage Act has done little to change that. These firms decide whether and how to protect information that they find valuable. They also decide whether to report instances of misappropriation to law enforcement agencies. Law enforcement and intelligence agencies, though they may have information about how economic espionage plays a role in other nations' efforts to gain technological and economic advantage, generally do not have access to information about the threats that individual firms face. These agencies depend on and react to information supplied by the private sector. This structure lends itself to the enforcement of an IP right, but not to the protection of national security interests.

The economic espionage statute also has not helped to advance the purposes that underlie trade secret protection. Private firms have little reason to view foreign-sponsored threats to their trade secrets differently than they view domestic threats; the economic espionage statute does not advance the cause of innovation more strongly than basic trade secret protection. Nor does the statute or its history of enforcement provide a mechanism for advancing norms that discourage illicit information collection.

Finding a way to define these norms is vitally important but becoming increasingly difficult, given the apparent advances in Internet-based espionage. The general lack of transparency for science and technology funding worldwide not only prevents positive norms from being defined but also provides cover for individuals and governments to carry out activities that are contrary to notion of fairness, both as between firms and as between nations. The United States provides an admirable level of openness regarding its funding for non-classified science and technology. It should tout this example and encourage other nations to follow it.