The American Interest
http://www.the-american-interest.com/2014/12/10/the-new-industrial-espionage/

*Appeared in:* Volume 10, Number 3
*Published on:* December 10, 2014
OPACITIES

# The New Industrial Espionage

JOEL BRENNER

*The information revolution has rendered obsolete the legacy legal regime on intellectual property rights, enabling spying for commercial purposes to morph into a strategic issue.*

The lawless world of international espionage, until recently the preserve of the most secretive organs of government, has come to affect the everyday commercial affairs of businesses around the world, which are woefully unprepared to deal with it. Economic espionage is not itself a new phenomenon. Chinese silkworms legendarily made their way to India in a clandestine transaction. In 1812, Francis Cabot Lowell traveled to Britain, where he visited and managed to memorize and steal the secret workings of the Cartwright loom.[1] More recently, starting no later than 1980, Hitachi and other Japanese companies repeatedly launched espionage attacks against IBM and other American companies, with the support of the Japanese government. In the early 1990s, the purchasing chief for GM's European operations decamped for Volkswagen, allegedly taking with him GM's cost-cutting secrets. Though he was never convicted, German prosecutors tied him to a trove of secret GM documents, and VW settled with GM for $100 million and a commitment to buy $1 billion in auto parts. American know-how was the target, and by the mid-1990s, tens of billions of dollars' worth of intellectual property had reportedly been stolen from American companies.[2]

This was the background against which Congress passed the Economic Espionage Act of 1986, which criminalized stealing intellectual property.[3] The incidents that led to the act, while notorious, were exceptional. That is no longer true. The ubiquitous digitization of information and pervasive connectivity of electronic networks have facilitated espionage as well as productivity, and they have turned exceptional theft directed against the largest American companies into a daily reality for companies large and small.

Foreign intelligence services and their surrogates have been penetrating the networks of Western corporations on a regular basis and stealing technology electronically since the late 1990s, but for years most businesses preferred to ignore the problem. That was in part because they did not understand it and in part for fear of antagonizing countries in which they wished to do business. That began to change in 2010, when Google admitted that Chinese cyber spies had penetrated its networks, stolen source code, and used Google both to spy on its users and to worm their way into many other companies. About a week later the *Christian Science Monitor* revealed that persistent electronic espionage against Marathon Oil, Exxon-Mobil, and ConocoPhillips had yielded massive amounts of information about the quantity, value, and location of global oil discoveries. The theft was traced to a single site in China.[4] That same year, Chinese spies mounted a sophisticated penetration of RSA, the company known for security tokens. These tokens are the cryptographic keys to other companies' secrets. Their theft led to the compromise of some 760 other organizations, including four major defense contractors and the Massachusetts Institute of Technology.[5]

These incidents represent a small part of the systematic theft of intellectual property (IP), much of it state sponsored, that shows no sign of abating. In 2009, while serving as the national counterintelligence executive, I warned that foreign entities were penetrating U.S. networks to steal technology, trade secrets, and proprietary information.[6] The warning got little traction. In 2011, however, following the Google affair, the undertone of unease became audible when my successor reported that "[f]oreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security."[7]

This is unquestionably true. American and European firms have lost automotive braking and battery technology, high-speed rail technology, aeronautical test data, and valuable chemical and pharmaceutical formulas in this way. The governments of Germany and Britain have complained publicly about the thievery. Networks in Japan and Australia have also been scoured. About 20 percent of European companies have been victim to at least one attempt to steal a trade secret over the past decade.[8] Western companies and governments nevertheless continued to dither.

Then in 2013 the security firm Mandiant disclosed that hundreds of terabytes of data from 141 companies in 20 different industries had been stolen remotely by China, and traced the theft back to a specific office in the People's Liberation Army known as unit 61398.[9] The U.S. government could have made similar disclosures years earlier but regrettably chose silence. After the Mandiant report, however, the thievery had become too brazen, pervasive, and obvious to ignore. This past May, in *United States v. Wang*, a Federal grand jury indicted five Chinese military personnel associated with unit 61398 for economic espionage and related crimes against five

U.S. companies and a U.S. labor union.

State-sponsored espionage directed at company secrets is still growing, however. In its most recent breach report, Verizon reported that state-affiliated actors had increased significantly to account for 21 percent of all breaches. The Chinese intelligence services are the worst but not the only sponsors of this kind of larceny. The Russian intelligence services are quieter and more selective than the Chinese, but they too are in the business of stealing IP for commercial purposes. Indeed, they operate under a public directive from President Putin to "more actively protect the economic interests of our companies abroad."[10] Iran also engages in economic espionage, and unlike other offenders, it is also active in attempting to disrupt American banks.[11] France and Israel are frequently cited as offenders too, though recent examples are hard to find. Taken together, this larceny is an assault on national economies in which jobs and wealth depend on innovation and IP protection. By 2010, IP-intensive businesses accounted for more than a third of U.S. GDP and, directly or indirectly, for nearly 28 percent of all U.S. jobs.[12]

Technology alone cannot prevent this larceny. Attribution of cyber network operations—that is, proving who did it—is difficult, though with enough time and resources it can sometimes be done, as the Mandiant report demonstrates.[13] But even if the internet were fundamentally re-engineered to make attribution more reliable at the device level, the weakest link in the system would remain the human user. Moreover, the operation of national and global enterprises, whether private or governmental, requires sensitive information to be widely shared among people in far-flung locations. Clamping down severely on that dissemination would impair productivity and the quality of decision-making. Some degree of network vulnerabilities will therefore continue, regardless of technological improvements.

Even as the level of theft increases, quantifying its aggregate financial cost is difficult. For reputational and liability reasons, many companies will not disclose that they have been victimized, and companies that do business in China are resolutely silent on the subject (at least in public) for fear of retaliation. In any case, translating an IP loss into lost market share, revenue, and profit is usually speculative. This kind of loss has therefore been impossible to insure against. But regardless of the aggregate figures, the effect of cyber-enabled economic espionage on victim companies can be devastating. Those companies deserve effective remedies.

We are dealing with a trade and economic issue. Theft via networks should not be treated differently than theft by any other means. The question is whether the theft of legally protected IP should be treated differently when undertaken by governments or their surrogates. Answering this question requires an examination of basic ideological differences regarding espionage.

Moses sent spies into Canaan. In the *Rig Veda*, which is at least as old as the oldest text in the Hebrew Bible, spies sit at the table with the god Varuna. To most practitioners of espionage, and indeed to anyone familiar with the hard realities of international relations, the idea of limiting the ancient practice through law is naive. Espionage is *premised* on breaking laws—other countries' laws. Spies will undertake it so long as their masters believe they can get away with it, and it has long been tolerated under international law.

Though espionage is ancient, its modalities have recently shifted in two fundamental ways. First, it has moved from a retail-scale business to a wholesale business. The quantity of purloined information moving over our networks is measured in units too large for most people to comprehend. And if you can extract terabytes of data from an adversary's network from thousands of miles away, you may not require a human spy in the adversary's camp. Or the spy you require may be an underling in the IT department rather than the Defense Minister's principal private secretary.

The second change is the relentless targeting of proprietary, non-military technology. There have been cases in previous centuries of state-sponsored espionage directed against economic targets, but they generally involved military technology, such as European cannon-making technology sought by the Turks in the 15$^{th}$ century, or British and German naval technology before World War I. In contrast, state-sponsored espionage against commercial IP is unrelated, in many cases, to military or defense. This kind of espionage has become pervasive in part because insecure networks make it easy to get away with. The collapse of the Soviet Union also drove home to the Russians, the Chinese, and others that if they could not compete technologically and economically with the West, and with the United States in particular, they could not compete geopolitically in any dimension. This is largely why state-sponsored IP theft is state policy in China, Russia, and certain other countries, and why it has become a plague in the West.

To Chinese and Russian ears, however, the distinction between economic and other kinds of espionage is an ideological construction, convenient only to the West. In their view, all state-sponsored espionage is by definition conducted in the national interest. In these countries, where a distinction between the public and private sectors is either non-existent or blurred, and where public and private actions are expected to support national policy, an attempt to carve out IP theft as qualitatively different from other espionage is merely a self-serving, bourgeois legalism.

The Chinese are in any event ideologically hostile to law as a means of controlling the state. Indeed, the English phrase "rule of law", by which we mean that the law controls the state as well as private actors, can also be translated into Chinese as "rule by law", by which the Chinese mean that the state uses law to achieve the aims

of the state.[14] Last year the Chinese Communist Party explicitly criticized Western notions of rule of law and constitutional government as an "attempt to undermine the current leadership and the socialism with Chinese characteristics system of governance."[15]

This philosophical disposition nevertheless contains a contradiction that will become increasingly apparent. China's policy of a peaceful rise in international affairs is based on the belief that its increasing prominence will promote stability, benefit its neighbors, and increase its comprehensive national power, by which it means cultural and diplomatic influence as well as military power. To achieve those goals, China must stand *for* something, just as the United States, however imperfectly, stands for economic and political liberty at home and abroad. But the Chinese, like the Japanese in the 1980s, are well aware they have been unable either to articulate or exemplify a national ideal that other nations can be expected to recognize, let alone willingly follow. Their growing reputation for international commercial IP banditry is inconsistent with this aspiration.

The level of this banditry, most of it from China, has reached alarming levels. State-sponsored theft of IP is not merely an attack on the victim enterprises. It is also an attack on the basic principles of the multilateral commercial order to which China and many other nations have already agreed and from which they benefit. It is therefore time to consider measures aimed at strengthening the multilateral system of political norms that apply, or should apply, to state-sponsored IP theft.

In 1994 the Marrakesh Agreement among the world's trading nations created the World Trade Organization (WTO), a successor to the General Agreement on Tariffs and Trade (GATT). The WTO structure included the Agreement on Trade-Related Aspects of Intellectual Property Rights, known as TRIPS.[16] Previous multilateral agreements had focused on goods trade and did not protect intellectual property, which by then accounted for a large and growing percentage of the world's wealth, particularly in Europe and North America. TRIPS aimed to protect IP from predation. It was an important element, along with the then-new General Agreements on Trade in Services (GATS), in updating global trade rules to better reflect the modern global economy as it existed twenty years ago.

TRIPS protects not only trademarks, copyrights, and patented goods but also designs and trade secrets. It does so by requiring WTO members to adopt domestic standards for protecting IP and enforcement procedures, and penalties to ensure that IP holders can effectively enforce those rights internally and at their borders, such as by excluding counterfeit goods. These requirements need not meet Western standards, but they must "permit effective action" against infringement and must provide "expeditious remedies." Developing nations were given significant time to comply with this requirement through transitional arrangements. When China and

Russia joined the WTO (in 2001 and 2012, respectively), however, they immediately assumed full TRIPS obligations.

Violations of TRIPS are covered by the WTO's dispute settlement understanding (DSU), through which member states, but not private parties, can bring disputes to the WTO for consultation and, if necessary, resolution by decision. Disputes that cannot be resolved through consultation are heard in the first instance by a dispute panel, and in the second instance by an appellate body. These bodies make findings and recommendations; binding decisions can be made only by representatives of all member governments, acting as the Dispute Settlement Body (DSB). Panel and appellate body reports to the DSB must be accepted, however, unless there is a consensus that they be rejected. This rule virtually ensures acceptance.

From the perspective of 1994, TRIPS and GATS brought the multilateral trading regime up to date, but that was long before the internet had become the backbone of a digitized knowledge economy with little respect for international borders. Consequently, TRIPS did not deal with cross-border enforcement challenges, which are now rife as a result of network-enabled IP theft by both states and criminal organizations. In 2013 Richard Clarke, who was special adviser for cybersecurity in the George W. Bush Administration, and James Lewis, a senior fellow at the Center for Strategic and International Studies, each suggested that this form of industrial espionage be outlawed under TRIPS. Computer network operations by their nature cross borders and trigger both virtual and actual effects at great distances. This characteristic makes them a fit subject for an international remedy. Nevertheless, Clarke and Lewis's suggestion was quickly met with objections. The chief objection was simply to point out that TRIPS merely requires members to enact and enforce at least minimal *national* laws to enforce TRIPS principles; it cannot deal with extra-territorial misbehavior. As David Fidler of the Indiana University School of Law put it, "WTO rules operate on a territorial basis, meaning that only in unusual circumstances do the rules recognize the legitimacy of the extraterritorial application of a WTO member's domestic law in trade contexts."[17]

This is a fair statement of how TRIPS has worked for the past twenty years. As a result, however, we find ourselves with an international trading regime in which members are obligated to prohibit IP theft in their national laws, but are free to engage in it, chiefly but not exclusively through network-enabled espionage in other countries. This is an irrational and probably untenable arrangement. The question, then, is how TRIPS and the WTO's dispute settlement structure might work to inhibit state-sponsored IP theft.

Fortunately, TRIPS already enshrines principles of fair play and honest dealing that are inconsistent with cross-border IP theft "for commercial purposes", and it establishes the right to protect oneself from such theft

(Article 26). On its face, this right applies against all third parties—states as well as non-states—regardless of the means by which it is violated. Another provision enshrines the principle of honest commercial practice: "Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices" (Article 39.2). These same principles should form the foundation of a remedy in the WTO as well as under national law.

The international trade regime in goods and services has long recognized an exceptional remedy known as a "non-violation nullification of benefits", based on the premise that negotiated benefits may be "nullified or impaired" by measures that may be technically consistent with TRIPS provisions (GATT Article 23). This remedy has been rarely invoked, though a provision for it appears in many bilateral U.S. trade agreements, and various WTO decisions make it clear that the remedy is disfavored. The United States and Switzerland proposed to permit such complaints in the case of IP, but widespread objections, especially from the developing world, resulted in a 1994 moratorium on them, which has been extended several times since then.

In theory, the opposition to permitting non-violation complaints under TRIPS is grounded in resistance to a mechanism that could lead to an expansion of specifically negotiated TRIPS obligations. But that argument merely turns inside out the rationale for permitting non-violation complaints in the first place: namely, that countries sometimes engage in measures that do effectively nullify those negotiated obligations. In practice, the opposition stems more narrowly from the belief that non-violation complaints would undermine the Doha Declaration on Public Health. That Declaration recognized that TRIPS "can and should be interpreted and implemented in a manner supportive of WTO members' right to protect public health and, in particular, to promote access to medicines for all." The specific fear is that developed nations with large pharmaceutical industries, like Switzerland and the United States, would use non-violation complaints as "a stealth attack on WTO members' sovereign right to use TRIPS flexibilities such as compulsory licensing to safeguard health and promote access to medicines for all."[18]

The objection to the *general* lifting of the moratorium on non-violation complaints in TRIPS is unlikely to be overcome. But nations asserting this objection do not assert a right to steal IP; they are concerned with health. So a multilateral consensus against state-sponsored IP theft may therefore be possible if a health-related exception can be crisply carved out, and diplomatic efforts to achieve it could proceed based on either of two proposals.

The first proposal would lift the moratorium on non-violation complaints only in cases of non-military IP theft,

even when engaged in by a sovereign. The second proposal, alternatively, would amend TRIPS to make such theft an explicit violation. Neither proposal would affect developing nations' asserted right to ignore or compulsorily take a patent for public health purposes. Amending TRIPS may be harder to achieve, but would be preferable for two reasons: It would give clearer guidance to arbitrators faced with actual disputes, and it could lead to the imposition of obligatory rather than advisory remedies as would apply in cases on non-violations (DSU Article 26).

Pursuing either path would require patience and a significant diplomatic effort. That effort should start with drafting the necessary principles into the Trans-Pacific Partnership (TPP) and the Transatlantic Trade and Investment Partnership (TTIP), which are now being negotiated. Attempts to lift the TRIPS moratorium or amend TRIPS could benefit from this experience. Recognizing that TRIPS covers state-sponsored IP theft would be important not only as a remedy in its own right. It may be even more important as a means of controlling retaliation for actions taken under national laws.

There has been no shortage of excuses for failing to address state-sponsored cyber theft of IP. The first excuse is that "everybody does it." Americans have had this charge thrown at them with force in the wake of Edward Snowden's disclosures, but Snowden is a red herring here. Stealing IP for commercial gain is unlike the surveillance he exposed because it is an assault on property whose right to protection is already recognized in TRIPS. True enough, the Chinese and the Russians do not accept this distinction. But they are members of, and benefit from, a world trade order that rests on precisely such distinctions; they should not be permitted to participate in that order while they simultaneously go about undermining it.

The "everybody does it" rationale is also false. The U.S. government does not employ its intelligence services to steal IP in support of national industries—for two good reasons. First, it is a bedrock principle of American policy to strengthen the legal order that supports IP rights and international trade. To sacrifice that principle for whatever tactical advantage would derive from IP theft would be foolish. Second, to be brutally honest about it, the Russians and Chinese don't have much IP to steal. Russia, for all its cultural depth and brilliant scientific minds, has never produced a commercially viable computer chip. China, for all its engineering prowess and dramatic growth rate, has thus far not produced much innovation.

In an effort to prove that the U.S. government does "it", however, Snowden has asserted that the United States engages in "economic espionage" because it will grab any information it can, economic and otherwise. But "economic espionage" is much too broad a term to be useful. Neither Snowden nor anyone else has shown that U.S. intelligence has stolen IP for commercial purposes, but those who imagine that he is a noble whistleblower

incline to believe everything he says without scrutiny. The only economic espionage that offends existing international norms is the stealing of IP for commercial gain—regardless of whether a state or a private actor undertakes it. This is not a self-serving American distinction; TRIPS recognizes the significance of a "commercial purpose" and "unfair commercial use" in establishing violations.

Hence, penetrating a foreign banking network for the purpose of understanding or disrupting terrorist financing is not commercial use, and no one proposes to prohibit the collection of economic information *per se*, even when it pertains to an individual firm, let alone an economic sector or an entire economy. Nor should a state be prohibited from conducting espionage for the purpose of understanding, say, the condition of another nation's economy or its position in international political or trade negotiations, or for the purpose of interdicting criminal behavior. Every nation able to conduct that kind of espionage does so and will continue to do so. Nor would the development of weaponry or military technology (as defined by the Wassenaar Agreement) be off-limits to espionage merely because it is undertaken by a commercial entity. None of these activities offends TRIPS principles.

Another explanation for failing to address economic espionage through international norms is that it supposedly cannot be stopped and is now simply a condition of doing business. But that is precisely the point to be tested. Equally defeatist is the rationale that we innovate faster than the thieves, so they will never catch up with our latest stuff. This is what chief executive officers tell their boards of directors when they find themselves over a barrel in a lawless and disruptive cyber environment. But the argument ignores the fact that third-world markets are usually happy to buy last year's model or the one before that. They may even prefer it.

We find ourselves at a juncture reminiscent of the early days of the campaign against foreign bribery. Many were scornful of the Foreign Corrupt Practices Act of 1977 and called it unrealistic or worse. The list of objections to that act rings a familiar bell: It would be difficult to distinguish corrupt payments from legitimate payments; business could not be done in some countries without corrupt payments; and, of course, everybody supposedly did it. But entrenched corruption did long-term damage to the political culture of less developed countries, and forbidding it was the right thing to do. The European Union and the United Kingdom eventually implemented their own anti-bribery measures, thus copying the legislation they formerly ridiculed. Foreign commercial bribery has not been wiped out, but it now comes with much higher costs. Transnational IP theft probably cannot be wiped out either, but significant costs can be attached to it that would form a limiting boundary for its practice.

The practical difficulties of implementing even limited espionage protections under the WTO are nevertheless

significant, and they begin with the need to put a boundary on the national security exception to the TRIPS rules. Article 73 states that the agreement cannot be used "to prevent a Member from taking any action which it considers necessary for the protection of its essential security interests." On paper, that exception is limited to disclosure obligations, to rights under the UN Charter, and to matters involving fissionable materials, traffic in arms, and measures taken in wartime or international emergency. In practice, however, these limitations may not apply.

Moreover, as already noted, the Chinese and Russians do not recognize a distinction between national and economic security. This is a deep ideological belief and not merely a position of current convenience. The United States also accepts the linkage between economic and national security; President Obama referred to economics or the economy 130 times in his current National Security Strategy. But a legitimate exception cannot be allowed to swallow the entire TRIPS principle of fair dealing in international trade. A prosperous regime of global trade requires a national security exception *and* a requirement that trading partners obey a common set of norms. If the security requirement could be invoked to permit state-sponsored theft of IP, it could also be invoked to condone the state-sponsored infringement of any patent and any other protected right relating to any subject.

Network intrusions present difficult evidentiary issues, but they are not unique in this regard. Proof of misappropriation would have to be presented, with all the well-known difficulties of attributing cyber operations to a particular device, operator, and organization. And if some or all of that evidence were classified, the complainant's government might have to make a difficult decision about giving up intelligence sources and methods.

Countries already deal with that problem in their own national courts, however. Assuming that misappropriation were shown, would it be sufficient to show an intention to use the misappropriated IP for commercial purposes, or would actual introduction of a product into the flow of commerce be required? Would proof of damage be necessary? These questions raise ordinary issues of judicial proof. Parties and courts deal with them regularly. Remedies would not seem different in kind from those that arise in other WTO cases.

The fundamental obstacles to bringing a measure of international order to rampant IP theft remain political and commercial. Companies and nations must weigh the likelihood of retaliation against complainants by the allegedly offending nation, either under that nation's law or by commercial or political measures. That difficulty will not disappear. Potential claimants would have to deal with it, just as litigants deal with other strategic decisions. Undoubtedly, there would be some potential for unwanted escalation. In the absence of

institutionalized legal means to deal with this problem, however, victim companies and states will be tempted to take unilateral steps, overt and covert, that hold even greater potential for instability and that bear a far greater risk of escalation. If the level of commercial espionage does not abate, we can expect to see retaliatory cyber measures against economic sectors, with significant potential for disruption.

The use of national intelligence means (directly or through proxies) to steal technology and business secrets for commercial purposes must be brought under control by concerted diplomatic efforts as well as enhanced national laws. The thievery is corrupt, and in the already affirmed language of TRIPS, it is "an affront to honest commercial practices in international trade." Thus far most Western companies have felt that the short-term profits have been worth the long-term cost of losing technology and incubating their own competition. But they now stand at a tipping point. Confronting the challenge will require four concerted initiatives.

First, the United States and like-minded states should agree on a definition of state-sponsored, non-military IP theft for commercial purposes. A fundamental issue will be whether to include dual-use technologies. Espionage directed against non-military IP is distinguishable from the politico-military variety precisely because it involves property already protected under TRIPS. State sponsorship should not be a predicate in a TRIPS proceeding that involves IP theft, however, any more than, say, in a patent proceeding. Yet including state-sponsored acts in the definition is critical because it would remove a blanket defense for such espionage in international law.

Second, national laws remain critical and should be strengthened in three important ways: They should permit the sequestration of goods containing stolen IP under procedures that are rapid as well as fair; they should deny access to banking systems by companies that profit from stolen IP; and they should allow a private right of action under national laws by parties victimized by trade-secret theft.[19]

Third, the U.S. government should lead a consensus for including an enforceable proscription against network-enabled IP theft in the TPP and the TTIP.

Fourth, the U.S. government should encourage like-minded states to lead a diplomatic effort to include the same proscription in TRIPS, either through a partial lifting of the current moratorium on non-violation complaints under TRIPS or by amending TRIPS. This effort will require persuading India, Brazil, Indonesia, Egypt, and other nations that the effort to combat network-enabled IP theft will not undermine the Doha Declaration on the TRIPS Agreement and Public Health. It will also require trading nations to give the WTO sufficient resources to deal with an expanding and crowded docket.

The goal in all of this is to devise effective mechanisms to diminish the plague of network-enabled IP predation. Western companies should support this effort because they will benefit from it, but given the potential for retaliation they cannot be expected to lead it. Progress will depend on achieving an international consensus through hard diplomatic work. That work will be difficult and the goal will seem elusive, but it is high time to begin the effort.

[1]Cartwright's effort had been foreseen and encouraged by Treasury Secretary Alexander Hamilton's Report on Manufactures December 5, 1971. Hamilton specifically referred to textile mill technology and said, "To procure all such machines as are known in any part of Europe, can only require a proper provision and due pains." His report was rejected by Congress, however, and so did not become official policy of the United States.

[2]*U.S. v. Kai-lo Hsu*, 155 F.3d 189, ¶23 (3d Cir. 1998), citing Richard J. Heffernan and Dan T. Starwood, *Trends in Intellectual Property Loss* (1996). *Hsu* involved the theft of secrets from Bristol-Myers Squibb.

[3]18 U.S.C. §§ 1831–1832. Section 1831 criminalizes "economic espionage", which requires a showing that the defendant knew that a foreign government, instrumentality, or agent would benefit from the theft. Section 1832 criminalizes "industrial espionage", which is the theft of trade secrets in interstate or foreign commerce. The distinction between industrial and economic espionage is therefore significant for Federal criminal law purposes, but the terms are otherwise often used interchangeably.

[4]Mark Clayton, "US Oil industry hit by cyberattacks: Was China Involved?", *Christian Science Monitor*, January 25, 2010; McAfee, "Global Energy Cyberattacks: 'Night Dragon'", February 10, 2011.

[5]See Brian Krebs, "Who Else Was Hit by the RSA Attackers?", Krebs on Security, October 11.

[6]Office of the National Counterintelligence Executive, "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY 2008" ("ONCIX 2008 Report"), July 23, 2009.

[7]ONCIX, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011" ("ONCIX 2011 Report"), October 2011.

[8]Joel Brenner, *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World* (Penguin, 2013); see also Alex Barker, "Brussels Takes Aim at Economic Espionage", *Financial Times*, November 28, 2013.

[9]Mandiant, "APT 1: Exposing One of China's Cyber Espionage Units", February 2013.

[10] Quoted in the ONCIX 2011 Report, p. 6.

[11]See appendix, ONCIX 2008 Report.

[12]U.S. Department of Commerce, "Intellectual Property and the U.S. Economy: Industries in Focus", March 2012, pp. vi–viii.

[13]There are three levels of attribution. First, from what machine did the attack originate? Second, who controlled the machine? And third, who was that person working for? The first level, and in some cases the second, can sometimes be done reliably through electronic means alone, with time. The third level, if done at all, usually requires additional intelligence means and methods.

[14]For this point and for the point expressed in the following paragraph, I thank Nigel Inkster, CMG, Director of Transnational Threats and Political Risk, International Institute for Strategic Studies, London.

[15]"Document 9: A China File Translation", *China File*, August 8, 2013.

[16]I am grateful to Robert C. Fisher of Hills & Company, formerly of the Office of the U.S. Trade Representative, for his advice on WTO and TRIPS issues. The opinions and any errors in this discussion are mine, however, not his.

[17]Fidler, "Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage", *Arms Control Law*, February 11, 2013.

[18]WTO TRIPS Council, "India's intervention on Non-Violation and Situation Complaints", February 26, 2014; "Intellectual property meeting mulls Irish tobacco plan, drug tariffs, sport, non-violation."

[19]These and other measures were proposed in *The Report of the Commission on the Theft of American Intellectual Property* (2013).

**Joel Brenner** *is a lawyer and security consultant and the Robert Wilhelm Fellow for 2014–15 in the Center for International Studies at the Massachusetts Institute of Technology. He is the former national counterintelligence executive and former inspector general and senior counsel of the National Security Agency.*