HARVARD INTERNATIONAL LAW JOURNAL

SYMPOSIUM: Online
DECEMBER 2012 Volume 54

Offensive Economic Espionage?

An article from the symposium, "State Ethics: Controlling the Behavior of Governments and Their Partners"

Susan Brenner*

I. INTRODUCTION

[T]he defensive form of war is not a simple shield, but a shield made up of well-directed blows.[1]

Six years ago, a former Defense Investigative Service officer and I analyzed economic espionage and found that the United States' reliance on a law enforcement approach to this activity becomes increasingly ineffective as espionage moves online.[2]

We based that conclusion on articles in which I analyzed why this approach is ill-equipped to deal with online crime.[3] I later refined that analysis,[4] and have revised my

* NCR Distinguished Professor of Law & Technology, University of Dayton School of Law

[1] CARL VON CLAUSEWITZ, ON WAR 159 (2007).

[2] *See* Susan W. Brenner & Anthony C. Crescenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act,* 28 Hous. J. Int'l L. 389 (2006).

assessment of the strategies we suggested could improve our approach to controlling economic espionage.[5]

Since I no longer believe that those strategies and/or the approach on which the United States continues to rely can control online espionage, I decided to propose a more radical solution. I do so with some ambivalence. On the one hand, I think offensive economic espionage is a practical response to the current state of affairs; on the other, I realize it would create a number of difficult issues, both doctrinal and practical.

II. ECONOMIC ESPIONAGE

The sections below will define foreign economic espionage and explain why the law enforcement strategy is ineffective in dealing with it.

A. The Crime

The Espionage and Sabotage Act of 1954[6] makes it a federal crime for one who, acting "with intent or reason to believe" it will be "used to the injury of the United States", transmits any information pertaining to "the national defense" to a foreign government.[7]

In 1996, Congress created a commercial espionage crime:[8] 18 U.S. Code § 1831(a) criminalizes stealing trade secrets to benefit a foreign government. A trade secret is "financial, business, scientific, technical, economic, or engineering information" that derives economic value from "not being generally known to" the public.[9]

Since 1995, the Office of the National Counterintelligence Executive has issued annual reports that summarize the threat "to the United States from foreign" economic espionage.[10] The 2011 report says it is a "significant and growing" threat to

---

[3] *See id.* at 442–52.

[4] *See, e.g.,* Susan W. Brenner, Cyberthreats: The Emerging Fault Lines of the Nation-State 25–70 (2009).

[5] *See* Brenner & Crescenzi, *State-Sponsored Crime, supra* note 2, at 453–64.

[6] Espionage and Sabotage Act, Pub. L. No. 83-777, 68 Stat. 1216 (1954) (codified as 18 U.S.C. § 794(2006)).

[7] *See* 18 U.S.C. § 794(a).

[8] *See* Economic Espionage Act, Pub. L. 104-294, tit. 1, § 101(a), 110 Stat. 3488 (1996).

[9] 18 U.S.C. § 1839(3).

[10] *See, e.g., ONCIX Reports to Congress: Foreign Economic and Industrial Espionage* OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, http://www.ncix.gov/publications/reports/fecie_all/index.php (last visited Sept. 30, 2012).

"the nation's prosperity and security."[11] It notes that cyberspace "amplifies" the threat by making it possible for "malicious actors" to "quickly steal and transfer massive quantities of data while remaining anonymous and difficult to detect."[12]

Companies report "an onslaught" of online intrusions from China and "extensive, sophisticated" attacks from Russia.[13] And in "the next three to five years," several factors will expand opportunities for harvesting "US economic and technology information."[14]

B. The Crime Control Strategy

For over a century and a half, societies have relied on a crime control strategy in which law enforcement officers create disincentives to commit crimes by apprehending enough offenders to create the perception that violators will be caught and punished.[15] The model has evolved around real-world crime to incorporate four assumptions about crime: proximity; scale; physical constraints; and patterns.[16]

In real-space crime, perpetrator and victim are physically proximate; in real-space, I cannot rob or otherwise victimize you if we are in different countries. This also means crime tends to be one-to-one, i.e., a perpetrator victimizes one person at a time.

Physical constraints also shape real-space crime; if John decides to rob Bank A, he will have to investigate its structure and routine to carry out a successful robbery and escape. He will disguise himself and try to minimize the trace evidence he leaves behind to avoid being apprehended. Since it is extraordinarily difficult to do all this, officers have a reasonable chance of apprehending John (who will probably still be in the locality).

Finally, analysts can identify patterns in real-space crimes. Since many crimes, especially minor crimes, occur in economically-deprived areas, the routine crime officers deal with tends to occur in those areas. High-value crime, such as murder and rape, occurs less often, which means officers can devote more resources to these offenses.

---

[11] Foreign Spies Stealing US Economic Secrets in Cyberspace, OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, i (Oct. 2011), http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[12] *Id.*

[13] *Id.* at 5–6.

[14] *Id.* at 6.

[15] For a detailed treatment of this strategy, *see* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security,* 18 B.U. J. Sci. & Tech. L. 1, 8–64 (2004).

[16] *See id.*

Cybercrime does not require victim-offender proximity, does not fall into identifiable patterns and does not involve one-to-one victimization or the physical constraints associated with real-space crime. Perpetrator and victims can be in different countries, crimes may not be discovered until long after they were committed and may involve evidence in various jurisdictions. These and other factors erode the efficacy of law enforcement response to cybercrime, including online economic espionage, which erodes the disincentive for committing such crimes.

III. OFFENSIVE ECONOMIC ESPIONAGE

I define "offensive economic espionage" as economic espionage Nation-State A directs at Nation-State B in response to economic espionage activity that Nation-State B has directed at Nation-State A. Logically, one could instead characterize this as "defensive economic espionage" since it is a reaction to an attack by the other state.

I prefer offensive economic espionage because the activity I hypothesize lacks the temporal immediacy we associate with the defensive responses criminal law allows. Since traditional crimes are committed in real-time and real-space, law requires that defensive responses be immediate reactions to the threatened harm.[17] This requirement also implicitly derives from the fact that the attacker is readily identifiable and vulnerable to such a response, neither of which is true with regard to online economic espionage.[18] In the latter context, the victim may not realize it has been attacked until days, weeks or even months after the attack has ended.

What I propose is a modified strategy that elongates and expands the process of responding to online economic espionage. Instead of having to respond while the attack is in progress, the victim could respond later, after it had analyzed the attack and determined with the necessary level of confidence that it came from a particular nation-state and, if this is possible, originated from a particular source. If the victim could, at a minimum, determine the location from which the attack originated, offensive economic espionage would allow it to launch a responsive act of economic espionage against an appropriate entity in the host state.

What would such a responsive act consist of? Logically, there seem to be three possibilities: the victim steals proprietary information from the attacker for its own use; the victim destroys or corrupts proprietary information belonging to the attacker; or the victim steals proprietary information from the attacker and broadcasts it online, thereby decreasing or destroying its value to the attacker.

---

[17] *See* WAYNE R. LaFave, SUBSTANTIVE CRIMINAL LAW §§ 10.4(d) & 10.6(a) (2d ed. 2003).

[18] *See* Brenner & Crescenzi, *supra* note 2, at 396–97.

The first possibility is to some extent analogous to the doctrine that allows one whose property has been stolen to recapture it. [19] Here, instead of recapturing its own property, the victim essentially replaces it with property belonging to the entity that attacked it. The argument for allowing this lies in the fact that the victim's property lost all or most of its value once it was misappropriated by the attacker; given that, the premise is that it would be reasonable to allow the victim to replace what was lost with a more or less equivalent substitute.

The second possibility reduces concerns that companies could exploit offensive economic espionage predicated on the first possibility to enrich themselves at another's expense. They might claim to have been victimized when they actually were not, using their ostensible victimization to raid another entity's proprietary information for their own ends. Of course, a company could further its own interests by corrupting or destroying a rival's proprietary information.

The third possibility further reduces the concerns noted above, since the victim would not be able to appropriate the attacker's proprietary information solely for its own use or prevent the attacker from exploiting it. In this scenario, the victim benefits from obtaining the information, but the benefit is diluted by the fact that the victim must share the information with the public.

The constant in each of these scenarios is that the attacker becomes the target of a response that is relatively immediate and more or less proportional to the damage it inflicted on the victim. Like the law enforcement model, this is a reactive strategy that is predicated on creating disincentives for committing future crimes. Unlike that model, in which the reaction is restricted to law enforcement officers, this approach is based on a distributed strategy, i.e., is implemented by civilians.

The law enforcement model's reactive strategy is (only) effective in a world in which states can maintain the integrity of their borders against attackers.[20] Until recently, nation-states used their militaries to protect their borders from attacks by other nation-states (external threats) and used their law enforcement officers to protect their citizens from crimes committed by fellow citizens (internal threats). Cyberspace erodes, even eradicates borders, at least for certain types of attacks, including online economic espionage. Attacks can come from anywhere, surreptitiously. It is simply not possible for law enforcement to be able to respond effectively to transnational attacks, especially given the complexity and the scale on which they can be committed.

---

[19] *See* LAFAVE, *supra* note 18, at § 10.6(d).

[20] *See* BRENNER, supra note 4.

It therefore becomes necessary to move to distributed response strategies that involve civilians in the response. As I explain elsewhere,[21] societies relied on such a model until relatively recently; involving civilians in an offensive economic espionage strategy is therefore not unprecedented. The challenges lie in (i) specifying when a response of the type outlined above is appropriate and when it is not, (ii) defining which civilian entities are authorized to deliver such a response and (iii) articulating the consequences for entities who deliver such a response when it is not appropriate and/or they are not authorized to do so.The first challenge would involve attribution requirements,[22] e.g., requiring that an entity trace an attack to a specific entity with the requisite level of certainty and requiring that the response be as limited in scope as possible (to avoid unnecessary damage). The second might involve a licensing process, in which entities would have to show they were able to trace attacks with the required accuracy and specificity and that they were capable of delivering appropriately limited responses. The third issue would presumably involve the imposition of a type of criminal liability, just as liability is imposed on one who improperly uses force to repel a physical assault on one's property.[23]

An obvious objection that could be raised to implementing offensive economic espionage is that it represents state-sanctioned crime, in that one state authorizes its citizens to attack citizens of another state.[24] The attacked state could therefore ask the state whose citizen engaged in offensive economic espionage to extradite the person for trial and punishment. The objection and the extradition request would both be valid if offensive economic espionage is conceptualized as "mere" crime.[25]

But if one accepts the premise that the entities authorized to initiate offensive economic espionage attacks are, in effect, recruits in a twenty-first century virtual militia, the task of which is to protect the country from attacks that threaten its economic viability, the objection is not so valid—and perhaps is not valid at all. For years some commentators, including former CIA Director Stansfield Turner, have been warning that economic espionage is a serious threat to the United States' national security.[26] In 1999, two officers from the People's Liberation Army noted the efficacy of using economic warfare against other nation-states, a strategy China has

---

[21] *See* Brenner, *supra* note **Error! Bookmark not defined.**.

[22] *See* Brenner, *supra* note 5 at 71–162.

[23] *See, e.g.*, Spradlin v. State, 951 N.E.2d 311 (Ind. App. 2011).

[24] This is true of all state-sponsored economic espionage. *See supra* note 3 at 434–35, 459–64.

[25] Extradition becomes meaningless in this context, since in state-sponsored economic espionage, the state is in effect an accomplice to the crime and is therefore not inclined to surrender its citizen. *See id.* at 450–52.

[26] *See* Jeff Augustini, *From Goldfinger to Butterfinger: The Legal and Policy Issues Surrounding Proposals to Use the CIA for Economic Espionage*, 26 Law & Pol'y Int'l Bus. 459, 484 (1995).

been pursuing for at least a decade.[27] And some security experts are arguing that "striking-back" against online attackers is the best way for companies to defend themselves in cyberspace.[28]

Years ago, some suggested having the CIA conduct offensive economic espionage, on the premise that it is conceptually analogous to and empirically at least as serious as traditional espionage.[29] My disagreement with that proposal lies in the fact that I do not believe that the CIA, or any other government organization, could implement an effective offensive economic espionage effort. Assigning this task to the CIA (or any other government entity) would yield an effort that suffers from the limitations of the law enforcement reactive model, noted above, i.e., it would necessarily be too limited in scope and too sporadic to constitute an effective deterrent.

IV. CONCLUSION

"We're not winning."[30]

Shawn Henry, who recently retired as the Federal Bureau of Investigation's Executive Assistant Director after spending more than two decades with the agency,[31] made the comment noted above. He offered this and other observations in assessing the success of U.S. companies' efforts to prevent online attackers from stealing data from their systems.[32] Henry says defensive measures are not effective against online economic espionage and other cybercrimes, which requires a shift to "'the offense.'"[33]

---

[27] *See* Qiao Liang and Wang Xiangsui, UNRESTRICTED WARFARE 51–53 (1999), http://www.terrorism.com/documents/unrestricted.pdf. *See also* supra notes 12–16 and accompanying text.

[28] *See, e.g.*, Taylor Amerding, Should Best Cybercrime Defense Include Some Offense?, CSO (June 20, 2012), http://www.cso.com.au/article/428187/should_best_cybercrime_defense_include_some_offense/.

[29] *See, e.g.*, Brandon J. Witkow, A New "Spook" Immunity: How the CIA and American Business Are Shielded from Liability for the Misappropriation of Trade Secrets, 14 Emory Int'l L. Rev. 451, 453–68 (2000).

[30] Devlin Barrett, U.S. Outgunned in Hacker War, WALL ST. J. (March 28, 2012), http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html (quoting Shawn Henry).

[31] *Id.*

[32] *See id.*

33 *See id.* ("'You can only build a fence so high, and what we've found is that the offense outpaces the defense, and the offense is better than the defense'").

Henry left the FBI to become President of CrowdStrike Services,[34] a cybersecurity company that, among other things, provides "offensive techniques and procedures" for "combating an adversary on your network."[35] The "techniques and procedures" include "counter-espionage techniques" and "hostile target dismantling".[36]

Henry's comments, and his company's services, are not an aberration. Over the last six months or so, other cybersecurity experts have made similar comments and noted that their companies employ similar techniques to repel the cyberattackers who are pursuing "Western firms' trade secrets and intellectual property."[37]

This interest in moving from defensive to offensive measures is, I think, the product of at least two circumstances. One is that companies are, and have long been, reluctant to report that they were attacked by cybercriminals because their revealed vulnerability can result in a loss of business.[38] The other circumstance, I believe, is that they know law enforcement will be unable to identify and apprehend the perpetrator, so that he/she/they can be tried and punished for the crime(s).

I believe the private sector's increasing interest in using offensive measures to react to online economic espionage and other cyberattacks reflects an implicit realization that, as Henry noted, law enforcement is not effective in this context. I believe this is a predictable response: As one author notes, "[w]herever law enforcement was perceived as non-existent or inadequate . . . vigilantism flowered."[39]

I am not saying that CrowdStrike or the other companies that offer offensive response services are vigilantes. I am saying that the interest in these techniques is a clear sign that our current crime control strategy is not working online, which creates a vacuum. If this continues unabated, and if history is any guide, prospective victims are likely to turn to self-help, or online vigilantism. While I am ambivalent about offensive economic espionage, I believe it is prudent to investigate the

---

[34] *See, e.g.*, Stephanie Lambidakis, FBI Expert Joins Private Firm CrowdStrike, CBS NEWS (April 18, 2012), http://www.cbsnews.com/8301-201_162-57416122/fbi-cyber-expert-joins-private-firm-crowdstrike/. *See also* CROWDSTRIKE, http://press.crowdstrike.com/team (last visited Oct. 10, 2012).

[35] *See* CROWDSTRIKE, http://www.crowdstrike.com/services.html (last visited Oct.10, 2012).

[36] *Id.*

[37] Tom Gjelten, Cybersecurity Firms Ditch Defense, Learn to "Hunt", NPR (May 10, 2012), http://www.npr.org/2012/05/10/152374358/cybersecurity-firms-ditch-defense-learn-to-hunt.

[38] *See, e.g.*, Ian C. Ballon, *Alternative Corporate Responses to Internet Data Theft*, 471 PLI/PAT. 737, 739 (1997).

[39] Richard M. Brown, Review, *Strain of Violence: Historical Studies of American Violence and Vigilantism*, 76 COLUM. L. REV. 361, 363 (1976).

possibility of incorporating private sector entities into a state-sponsored and state-regulated initiative that will create disincentives for engaging in such activity and thereby control its incidence. As I noted earlier, such an effort essentially requires replicating the common law militia and posse comitatus in cyberspace.[40]

[40] *See* Brenner, *supra* note 5 at 165–77.