ECONOMIC ESPIONAGE

Deterring Financially Motivated Cybercrime

Zachary K. Goldman* & Damon McCoy**

INTRODUCTION

Deterrence is one of the most venerable concepts in the national security lexicon. It refers to the process of manipulating an adversary's cost/benefit calculations to prevent him from doing something you do not want him to do. The concept is as old as warfare itself, reaching its apotheosis during the Cold War, when it was the central principle governing the security relationship between the United States and the Soviet Union.

But despite the pedigree of deterrence as a theory and a strategy, the community of scholars and practitioners focused on cybersecurity and cybercrime has struggled to adapt it to the burgeoning world of cyber threats. Admiral Michael Rogers, Director of the NSA, has said that the "fundamental concepts of deterrence" in cyberspace are "immature."[1] Senator John McCain has decried the "failure to develop a meaningful cyber deterrence strategy."[2] And some of the most prominent cybersecurity practitioners have noted that "deterrence is an undeveloped theoretical space in cyber war today."[3]

The cyber deterrence discussion has foundered thus far in part because of challenges that are unique to cyber space. This includes problems publicly attributing cyberattacks with confidence, the difficulty that inheres in determining whether a technological system has failed because of attack or for other reasons,[4] and the unwillingness of states to discuss publicly capabilities that they treat as highly classified.

But part of the problem is also conceptual, derived from the fact that cyberattacks are motivated by an array of factors – cyber espionage is motivated

---

* Zachary K. Goldman is the Executive Director of the Center on Law and Security and an Adjunct Professor of Law at NYU School of Law.

** Damon McCoy is an Assistant Professor of Computer Science and Engineering at NYU's Tandon School of Engineering. This work war partially funded by National Science Founded grant number 1619620.

1. Admiral Michael S. Rogers (USN), Director, National Security Agency, and Commander, U.S. Cyber Command, Remarks at the New America Foundation Conference on Cybersecurity (Feb. 23, 2015).

2. *Hearing to Receive Testimony on U.S. Strategic Command, U.S. Transportation Command, and U.S. Cyber Command In Review of the Defense Authorization Request for Fiscal Year 2016 and the Future Years Defense Program: Hearing Before the S. Armed Services Comm.*, 114th Cong. (2015) (Statement of Sen. John McCain, Chairman).

3. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 189 (2010).

4. MARTIN LIBICKI, CYBERDETERRENCE AND CYBERWAR 45-47 (2009) (hereinafter "LIBICKI, CYBERDETERRENCE AND CYBERWAR").

by different interests than attacks on critical infrastructure – and involve a range of actors with varying degrees of linkage to states. Deterrence strategies therefore must be tailored for each set of motivations and each set of actors, a task that has proven to be a significant challenge.

Within the spectrum of motivations for the infliction of cyber harms, this article addresses financially motivated cyberattacks because they constitute a substantial portion of cyberattacks,[5] and represent a significant drag on economic activity.[6] Deterring them will require different strategies than those used to deter other forms of cyber threat like attacks on critical infrastructure or cyberattacks in the context of armed conflicts.[7]

We use the term "financially motivated cyberattacks" in this paper to refer to attacks that use malicious cyber capabilities to generate a profit; like other businesses, this activity is sensitive to costs. Financially motivated cyberattacks often seek data – credit card data, health records, or other personally identifiable information – that can be monetized quickly. Financially motivated cyber criminals also seek valuable intellectual property, trade secrets, or material nonpublic information about companies that can provide strategic or competitive advantage.[8] Financially motivated cybercrime also includes the sale of counterfeit or fraudulent goods perpetrated through digital intrusions – the kinds of spam messages that clog our email inboxes each day.

In targeting digital information, financially motivated cyber criminals are participants in a (black) marketplace for data or goods that is "growing in size and complexity" and which has "emerged as a playground of financially driven,

---

5. VERIZON ENTERPRISE SOLUTIONS, 2014 DATA BREACH INVESTIGATIONS REPORT 9 (2014) [hereinafter 2014 VERIZON DATA BREACH REPORT] (noting that approximately 60% of data breaches are financially motivated).

6. Estimates about the cost of cybercrime to the economy vary widely and measuring the cost of breaches with any precision is difficult. Ellen Nakashima & Andrea Peterson, *Report: Cybercrime and espionage costs $445 billion annually*, WASH. POST (June 9, 2014), https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html; Paul Taylor, *Cybercrime costs US $100bn a year, report says*, FIN. TIMES (July 23, 2013), www.ft.com/cms/s/0/45bf9898-f3bf-11e2-942f-00144feabdc0.html. *See* Ross Anderson et al., Measuring the Cost of Cybercrime (2012) (paper for the Workshop on the Economics of Information Security), http://cseweb.ucsd.edu/savage/papers/WEIS2012.pdf.

7. Indeed, some argue that cyber war has not – and will not – take place. *See, e.g.*, THOMAS RID, CYBER WAR WILL NOT TAKE PLACE (2013). Rid, a noted theorist of military strategy, argues instead that much of what we consider acts of cyber war are in fact better understood as one or a combination of espionage, sabotage, or subversion. Rid argues that cyberattacks largely do not amount to acts of war "because the use of force in war is violent, instrumental, and political." *Id*. at 4. Cyberattacks have, however, been used in the context of armed hostilities. *See* CLARKE AND KNAKE, *supra* note 3, at 5-8 (describing reported Israeli cyber operations to blind Syria's air defense systems before striking a nuclear facility there in September 2007). Russia also accompanied its 2008 attack on Georgia with crippling cyberattacks against the country. *Id.* at 18-21.

8. Press Release, Federal Bureau of Investigation, Nine People Charged in Largest Known Computer Hacking and Securities Fraud Scheme: More than 150,000 Press Releases Stolen from Three Major Newswire Companies, Used to Generate Approximately $30 Million in Illegal Trading Profits (Aug. 11, 2015), https://www.fbi.gov/newyork/press-releases/2015/nine-people-charged-in-largest-known-computer-hacking-and-securities-fraud-scheme.

highly organized, and sophisticated groups."[9]

Deterring financially motivated cybercrime requires a defender to raise the cost in time or resources of pursuing a particular target. Defenders can also deter attacks by lowering the anticipated benefits that an attacker will receive through a particular act of cyber theft. In the context of the strategies discussed in this paper, cyberattacks can be deterred by making it harder for criminals to monetize the goods they have counterfeited or data they have stolen.

Because deterrence of financially motivated cybercrime involves manipulating the financial costs and benefits of an attack, it will rely on different tools than the deterrence of attacks against military targets or critical infrastructure.[10] Instead of punishing retaliation against the means and instrumentalities of the attack, financial sanctions and other measures taken by the private sector can raise the cost of commercially motivated theft.

This article will present a strategy for deterring financially motivated cybercrime that leverages the U.S. government's financial sanctions program targeting "Significant Malicious Cyber-Enabled Activities,"[11] as well as private sector efforts to mitigate cybercrime. Public/private collaborations like those described below are an important part of a deterrence strategy designed to deprive cyber thieves of the expected value of criminal behavior. These partnerships have done important work to use intellectual property law and other legal regimes to play "offense against cybercriminals . . . taking legal action to clean up malware and help ensure customers stay safer online."[12] The article also discusses techniques that credit card companies are using to make it more difficult to profit from cybercrime.

While this article focuses on deterring financially motivated cybercrime, it also seeks to establish the larger point that one cannot speak generically about "cyber deterrence." Rather, different kinds of malicious cyber activity demand different, tailored, deterrence strategies. This is because each category of cyber threat has a different motivation, and therefore will be sensitive to a different type of cost. Broadly, one can distinguish between cyber war, cyber activism ("hacktivism"), cyber espionage, cyber terrorism, cyberattacks against critical infrastructure, and financially motivated cyber theft.[13]

Financially motivated cyber theft does not generally pose a risk of acute catastrophe – the "Cyber Pearl Harbor" that then-Defense Secretary Leon Pan-

9. LILLIAN ABLON, MARTIN C. LIBICKI & ANDREA A. GOLAY, MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA ix (2014) [hereinafter MARKETS FOR CYBERCRIME TOOLS].

10. LIBICKI, CYBERDETERRENCE AND CYBERWAR, *supra* note 4, at 91-116 (for a discussion of the importance of retaliation in the deterrence of cyber threats against military or infrastructure targets).

11. Exec. Order No. 13694, 31 C.F.R. 578 (Apr. 2, 2015) [hereinafter EO 13694].

12. Richard Domingues Boscovich, *Microsoft Takes on Global Cybercrime Epidemic in Tenth Malware Disruption*, THE OFFICIAL MICROSOFT BLOG (June 30, 2014), http://blogs.microsoft.com/blog/2014/06/30/microsoft-takes-on-global-cybercrime-epidemic-in-tenth-malware-disruption.

13. Catherine A. Theohary & John W. Rollins, Cong. Research Serv., R43955, *Cyberwarfare and Cyberterrorism: In Brief*, (2015).

etta described in 2012.[14] Rather, senior government officials are beginning to describe the main cybercrime threat as an "ongoing series of low-to-moderate level cyberattacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security."[15] While these might prove catastrophic to a particular victim company at a particular moment, the strategy for deterring them similarly lies in a distributed approach to raising the costs of attack, and targeting what cyber thieves care about most: their wallets.

The paper proceeds as follows. Section I outlines the challenge of deterrence in cyber space, while section II describes the phenomenon of financially motivated cybercrime by illuminating how markets for stolen data operate, identifying the reasons that deterring financially motivated cybercrime has been such a challenge. Section II also describes three strategies to deter financially motivated cybercrime by diminishing the ability of thieves to monetize illicit goods or data: the imposition of financial sanctions; public/private partnerships to disrupt tools of cybercrime like botnets; and activities undertaken by credit card companies to disrupt payment networks run by criminals who sell fraudulent goods over the Internet. It also discusses some of the challenges associated with these approaches. Section III illustrates the ways in which this approach to deterrence of financially motivated cybercrime elides some of the traditional challenges of cyber deterrence like attribution and secrecy.

I. THE CHALLENGE OF DETERRENCE IN CYBER SPACE

The scholarly and policy communities have faced two distinct sets of problems in developing frameworks for deterrence in cyber space. The first pertains to challenges inherent in the cyber domain – chiefly the pervasive difficulty of attribution and the secrecy with which governments and private actors treat cyber capabilities. A second set of conceptual challenges revolves around the field's disproportionate focus on deterrence in the context of armed conflict and attacks on critical infrastructure. While cyber war and attacks on critical infrastructure like the power grid demand attention from scholars and policymakers, approaches to deterring these threats will differ from approaches designed to deter financially motivated cybercrime. Targeting the incentives to which financially motivated cyber attackers respond and reducing their ability to profit from cybercrime is the foundation of an effective strategy for deterring the attacks that plague companies and individuals around the world and cost tens or hundreds of billions of dollars each year.[16]

---

14. Leon Panetta, U.S. Secretary of Defense, Keynote Address to the Business Executives for National Security: "Defending the Nation from Cyber Attack" (Oct. 11, 2012). We leave aside questions about what might happen if a financially motivated cyberattack produces unintended consequences because of digital interdependencies that are poorly understood by attackers.

15. Susan Landau, *What We Must Do About Cyber*, LAWFARE BLOG (Mar. 10, 2015), http://www.lawfareblog.com/2015/03/what-we-must-do-about-cyber.

16. *See supra* note 6 for discussion of varying estimates of the cost of cybercrime.

Data stolen by cybercrime rings generally falls into one of two categories: records (like credit card or health records) that can be monetized for use in fraud; and stolen intellectual property (IP) or other kinds of trade secrets. Stolen records include information like credit card data, account information (e.g. from eCommerce or online banking sites), email logins and passwords, and ATM card data. The black markets on which this kind of data is traded "operate in the same ways traditional markets do. Easily exchanged goods such as PII or account data, are prey to the normal microeconomic fluctuations of supply and demand."[17] Cybercriminal rings also use tools like botnets to promote the sale of counterfeit or intellectual-property infringing goods (e.g., pharmaceuticals, software, luxury goods) over the Internet.

Financially motivated cyberattacks are pervasive, and cyber criminals are constantly innovating in the types of activity in which they engage. In addition to more traditional data breaches, news reports in 2015, for example,[18] described the ways in which organized criminal groups used stolen data to fraudulently file tax returns and obtain refunds, which one noted security researcher called a "$6 billion-a-year problem."[19]

In contrast to records, which can be fungible and for which a robust black market exists, intellectual property is both non-fungible,[20] and "harder to put a value on because it can be so unique, and generally requires a specific buyer."[21] Trade secrets, which can include litigation positions, proposed corporate finance activities, and similarly sensitive corporate plans, are targets that can be difficult to value, but which criminals seek. There are also variations in the ways such data is stolen, with responsibility distributed between insiders (mostly employees) and outside hackers.[22] According to one authoritative private sector source, financial motivations still drive the majority of cyber incidents,[23] while the cost of breaches continues to rise.[24]

Reducing this activity is a significant priority for the United States government and its allies, as well as for the private sector. But strategies to deter financially motivated cybercrime must address the specific reasons that parties engage in it.[25] The cost to perpetrators of committing cybercrime must be increased, and the anticipated benefits must be reduced through regulatory and

17. MARKETS FOR CYBERCRIME TOOLS, *supra* note 9, at 10-11.

18. Jada F. Smith, *Cyberattack Exposes I.R.S. Tax Returns*, N.Y. TIMES (May 26, 2015), http://www.nytimes.com/2015/05/27/business/breach-exposes-irs-tax-returns.html.

19. Brian Krebs, *States Seek Better Mousetrap to Stop Tax Refund Fraud*, KREBS ON SECURITY BLOG (Jun. 2, 2015), http://krebsonsecurity.com/2015/06/states-seek-better-mousetrap-to-stop-tax-refund-fraud.

20. MARKETS FOR CYBERCRIME TOOLS, *supra* note 9, at xi.

21. *Id.* at 15.

22. ERNST & YOUNG, GET AHEAD OF CYBERCRIME: EY'S GLOBAL INFORMATION SECURITY SURVEY 2014 3 (2014) (noting the importance of employees as a potential source of threat).

23. 2014 VERIZON DATA BREACH REPORT, *supra* note 5, at 9.

24. PONEMON INSTITUTE, 2015 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 1-3 (2015).

25. See, for example, MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 9 (2013), for a description of the ways in which a Chinese military cyber operations unit is suspected of engaging

other measures designed to dry up the market for stolen data, and to make the conduct of cybercrime more costly.

Because of the multiplicity of motives involved in different types of cyberattacks it has been difficult to adapt the theory and strategy of deterrence to cyber space. Deterrence is a theory of influence. It is the act of shaping an adversary's cost/benefit calculations to convince him to refrain from doing something that you do not want him to do.[26] During the Cold War, deterrence was the dominant concept and strategy governing the security relationship between the United States and the Soviet Union. As that era ended, however, scholars and practitioners questioned the continued relevance of deterrence. After the terrorist attacks of 9/11, deterrence lost its salience as a principal component of the U.S. Government's security strategy, and was replaced, in the 2002 National Security Strategy, by paradigms of preemption and prevention.[27] In recent years, however, ideas about the relevance of deterrence have been revised, and the concept is playing an increasingly important role in how scholars and practitioners think about managing security challenges in a range of contexts.[28]

But as deterrence has been revived as an increasingly central component of American security strategy,[29] it has evolved from the way strategists thought about it during the Cold War. During that time, scholars and practitioners focused primarily (but not exclusively) on "deterrence by punishment," in which adversaries are deterred by the credible threat of imposing unacceptably high costs unless they change their behavior. Recent work has built upon Cold War efforts to develop concepts like "deterrence by denial," in which an adversary is deterred by the deployment of defensive measures that make a successful attack less likely. Scholars also have made progress in specifically adapting deterrence strategies to different threats.[30] In the counterterrorism context, for example, researchers have focused on disaggregating terrorist networks into their constituent parts and tailoring approaches to shape the

---

in "political, economic, and military-related intelligence," including the theft of valuable intellectual property from Western corporations.

26. *See* PHILIP BOBBITT, DEMOCRACY AND DETERRENCE: THE HISTORY AND FUTURE OF NUCLEAR STRATEGY 9 (1988). Patrick Morgan formulates the concept elegantly: "deterrence has generally been conceived as an effort by one actor to convince another to not attack by using threats of a forceful response to alter the other's cost–benefit calculations." PATRICK MORGAN, DETERRENCE NOW 44 (2003).

27. OFFICE OF THE PRESIDENT, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 15 (2002) ("Traditional concepts of deterrence will not work against a terrorist enemy whose avowed tactics are wanton destruction and the targeting of innocents; whose so-called soldiers seek martyrdom in death and whose most potent protection is statelessness").

28. *See generally* Richard K. Betts, *The Lost Logic of Deterrence*, FOREIGN AFF. (Feb. 11, 2013), https://www.foreignaffairs.com/articles/united-states/2013-02-11/lost-logic-deterrence.

29. Suzanne Nossel, *Obama Needs to Find His Inner Cold Warrior*, FOREIGN POLICY (June 25, 2014), http://foreignpolicy.com/2014/06/25/obama-needs-to-find-his-inner-cold-warrior; KATHLEEN H. HICKS, 2015 GLOBAL FORECAST: CRISIS AND OPPORTUNITY, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES 11 (Craig Cohen & Josiane Gabel eds., 2014) ("In the coming year, deterrence will be an aspect of virtually all of our security dealings.").

30. John Gearson, *Deterring Conventional Terrorism: From Punishment to Denial and Resilience*, 33 CONTEMP. SECURITY POL'Y 171, 171-198 (2012).

cost/benefit calculations of specific actors in the terrorism ecosystem (e.g. financiers, facilitators, recruiters).[31]

Deterring financially motivated cybercrime will rely primarily on concepts of deterrence by denial. In the realm of financially motivated cybercrime, "dissuasion by denial," a concept that Paul Davis defines as "dissuading an action by having the adversary see a credible capability to prevent him from achieving potential gains adequate to motivate the action,"[32] is particularly salient. This approach is well suited to diminishing the threat from cybercrime as it is explicitly focused on diminishing the anticipated benefits of action.

The scholarly focus on cyber deterrence has encountered a series of challenges that have prevented the development of a rich articulation of the concept.[33] The first challenge relates to attribution. Scholars and policymakers often have noted that without strong attribution deterrence is difficult. This is because a victim either would not know with confidence against whom to retaliate,[34] or cannot know with confidence in sufficient time for retaliation to shape the aggressor's behavior before the next attack.[35] Attribution of attacks is difficult because attacks conducted over the Internet can easily be masked and routed through intermediate points between the aggressor and his victim. A second problem is that the same act – intruding into a network without authorized access – is the first step required to engage in a range of activities, whether destructive cyber attacks, or data theft, or something in between. Defenders thus may not know what an unauthorized party in their network seeks to do harm until it is too late. Network intrusions themselves also may lie undetected for a long period of time.[36] A final challenge relates to the fact that many perpetrators of cyberattacks are non-state actors, which means that they will have fewer

---

31. PAUL K. DAVIS & BRIAN MICHAEL JENKINS, DETERRENCE & INFLUENCE IN COUNTERTERRORISM: A COMPONENT IN THE WAR ON AL QAEDA (RAND Corporation, 2002). Scholars also have focused on new forms of deterrence, like "deterrence by delegitimization," which attempts to undermine the ideological foundations of terrorism. *See* Alex S. Wilner, *Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism*, 34 J. STRATEGIC STUD. 3, 3-37 (2011); ANDREAS WENGER, ET AL., EDS., Deterring Terrorism: Theory and Practice (Stanford University Press, 2012).

32. Paul K. Davis, *Deterrence, Influence, Cyber Attack, and Cyberwar*, 47 NYU J. INT'L L. & POLS. 327, 333 (2015).

33. Indeed, this is the main focus of the leading text on cyberdeterrence: LIBICKI, CYBERDETERRENCE AND CYBERWAR, *supra* note 4, at 7-8. *See also* NATIONAL RESEARCH COUNCIL, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY (2010); Jon R. Lindsay, *The Impact of China on Cybersecurity: Fiction and Friction*, 39 INT'L SECURITY, 7, 7-47 (2015).

34. Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L. J. 317, 370-72 (2015).

35. Eric Talbot Jensen, *Cyber Deterrence*, 26 EMORY INT'L L. REV. 773–824 (2012).

36. William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, 89 FOREIGN AFF. (2010); Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 415, 438-440 (2012); K.A. Taipale, *Cyber-deterrence*, *in* LAW, POLICY AND TECHNOLOGY: CYBERTERRORISM, INFORMATION WARFARE, DIGITAL AND INTERNET IMMOBILIZATION 1–62, 3–4 (Pauline C. Reich & Eduardo Gelbstein eds., 2010). *See also* MANDIANT, 2014 M-TRENDS THREAT REPORT: BEYOND THE BREACH 3 (2014), https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf (noting that threat groups were present in a victim's network for a median time of 229 days before detection).

easily-identifiable assets to hold at risk as part of a deterrence by punishment strategy.[37]

II. DETERRING FINANCIALLY MOTIVATED CYBERCRIME

This section will describe a strategic framework for deterring financially motivated cybercrime by making it harder for criminals to profit from engaging in it. The strategy depends on a series of legal instruments that make it easier for the U.S. government and for the private sector to deprive hackers of the proceeds of their crimes. As it becomes harder for criminals to make money from cyber intrusions their incentives to engage in them will diminish. This section will present and analyze three legal instruments that can be deployed to deter financially motivated cybercrime: financial sanctions; botnet takedowns; and civil and contractual remedies used to disrupt the flow of funds to cybercriminals. These approaches are not without drawbacks, some of which are discussed more fully below. But they represent the beginnings of a systematic effort to raise the cost of cybercrime.

A. Drying up the Market for Stolen Data: Sanctioning Hackers

Recognizing that "Profit drives modern cybercrime . . . [and] scammers relentlessly innovate to identify more lucrative niches to maximize their returns,"[38] the U.S. government recently established a financial sanctions program to target the activities of cyber criminals. The Obama administration inaugurated the program in April 2015 with the adoption of Executive Order 13694,[39] which emerged from a context in which the U.S. government and the private sector continue to struggle to stem losses from cybercrime. While the Obama administration has promulgated several executive orders addressing different components of the cybersecurity problem, the administration's adoption of the program outlined in E.O. 13694 fulfilled the need for "a capability to deter and impose costs on those responsible for significant harmful cyber activity . . . [and] to remove a powerful economic motivation for committing these acts in the first place."[40]

The program envisions two main groups of targets – those who perpetrate cybercrime by breaking into networks and stealing data,[41] and, more innovatively, those who knowingly receive or use trade secrets misappropriated by

37. LIBICKI, CYBERDETERRENCE AND CYBERWAR, *supra* note 4, at 117 ("if the attacker is a nonstate entity, it is unlikely to present much of a target for the defending state to hit back against.").

38. Paul Pearce et al., *Characterizing Large-Scale Click Fraud in ZeroAccess*, *in* PROCEEDINGS OF THE 2014 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 141 (2014) [hereinafter *Click Fraud in ZeroAccess*].

39. E.O. 13694, *supra* note 11.

40. Lisa Monaco, *Expanding Our Ability to Combat Cyber Threats*, THE WHITE HOUSE, NATIONAL SECURITY COUNCIL BLOG (Apr. 1, 2015), https://www.whitehouse.gov/blog/2015/04/01/expanding-our-ability-combat-cyber-threats.

41. EO 13694, *supra* note11, at §1(a)(i).

cyber-enabled means for commercial advantage.[42] The program can be used to target the perpetrators of financially motivated cybercrime, as well as those providing them with material support (such as the financial services they need to move and store money), and in so doing adds another means beyond arrest and criminal prosecution by which the government can disrupt the perpetrators of cybercrime. The use of financial sanctions to target cyber criminals builds on the success of sanctions in containing threats or engineering a change in behavior in other contexts. Since 9/11, the United States and its allies have made it harder "for terrorists to raise, move, store, and use funds."[43] And in the context of international negotiations about the Iranian nuclear program, financial sanctions are widely credited with generating the leverage needed to incentivize Iran to reach an agreement about its nuclear program.[44]

The power of economic sanctions imposed by the United States is determined by structural features of the international financial system that make the U.S. uniquely positioned to project financial power. Specifically, many significant international commercial transactions, including the global energy trade, are denominated in U.S. dollars, which means that when U.S. banks clear U.S. dollar transactions, the parties to those transactions become subject to U.S. jurisdiction (at least for limited purposes). Moreover, most significant international financial institutions, whether or not they are formally subject to U.S. jurisdiction, bar transactions with persons sanctioned by the U.S. government. They do so because they are wary of the reputational risk involved in potentially processing transactions on behalf of designated persons, even inadvertently.[45]

The cyber sanctions program therefore has the potential to address one of the most vexing types of cybercrime: the theft of commercially-valuable intellectual property, which former NSA Director Gen. Keith Alexander has called the "greatest transfer of wealth in history."[46] The examples of leading American companies that have reportedly had their most valuable intellectual property stolen are legion: In 2010, Google had valuable intellectual property stolen, as

42. EO 13694, *supra* note 11, at §1(a)(ii)(A).

43. Remarks by David S. Cohen, Under Sec'y for Terrorism and Fin. Intelligence, Confronting New Threats in Terrorist Financing, at Center for a New American Security (Mar. 4, 2014), http://www.treasury.gov/press-center/press-releases/Pages/jl2308.aspx.

44. Zachary Goldman, *Iran and Three Questions on the Effectiveness of Sanctions*, JUST SECURITY (Apr. 10, 2015), https://www.justsecurity.org/21898/efficacy-financial-sanctions-case-iran-larger-questions.

45. In a 2012 speech given in the context of the accelerating Iran sanctions campaign, then-Under Secretary of the Treasury for Terrorism and Financial Intelligence David S. Cohen said, "[A]lthough foreign banks are not generally obligated to abide by these sanctions – they reach only U.S. persons and those operating in the U.S. – many foreign banks, acting out of enlightened self-interest to protect their reputations, chose to terminate relationships with sanctioned Iranian banks." Remarks by David S. Cohen, Under Sec'y for Terrorism and Fin. Intelligence, The Law and Policy of Iran Sanctions, at N.Y. Univ. Sch. of Law (Sept. 12, 2012), http://www.treasury.gov/press-center/press-releases/Pages/tg1706.aspx.

46. Josh Rogin, *NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History*, FOREIGN POL'Y (July 9, 2012), http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history.

well as user account data, after "a highly sophisticated and targeted attack on our corporate infrastructure originating from China";[47] also in 2010, cyberattacks that originated in Russia struck the NASDAQ stock exchange, which investigators later concluded were motivated at least in part "to collect information for their own stock exchanges, Micex and RTS;"[48] and, perhaps most notoriously, hacks attributed to the Chinese military led to the theft of the U.S. military's plans for the Fifth Generation F-35 fighter.[49]

This intellectual property is stolen to enhance the competitive position of companies that benefit from the cyber theft. Sanctions under EO 13694 imposed on companies that knowingly receive or use stolen intellectual property can be used to deprive them of benefits they anticipate from purloined information. This is because companies sanctioned under the order will be largely cut out of the international financial system. They will have property subject to U.S. jurisdiction blocked, and will be prohibited from engaging in transactions with U.S. persons. It will become virtually impossible for those companies to use the international financial system, to transact in U.S. dollars, and to market their products or services to a broad global audience. Their investments in stolen intellectual property will put at risk their entire business operation.

A May 2014 indictment of five members of the Chinese military illustrates a scenario that might be well suited to using the regulatory measures established by EO 13694. In that case, it was possible to release enough information about the crimes and the criminals to support indictments (none of the five defendants has yet been arrested). But it is easy to imagine future cases in which it might not be possible to release sufficient information to permit criminal prosecutions, making the availability of sanctions an important policy tool to raise the cost of financially motivated cybercrime.[50] It also might be beneficial in some future instance to designate the companies that benefitted from cybercrime at the same time as the Department of Justice prosecutes the individuals that committed thefts (the United States did not name the companies that benefited from the cybercrime described in the May 2014 indictment). The combination of sanctions against companies benefitting from cybercrime and prosecutions of individuals perpetrating it can be particularly potent, especially in those cases where it might take a substantial amount of time to arrest a defendant, if it is possible to

47. David Drummond, *A New Approach to China*, GOOGLE OFFICIAL BLOG (Jan. 12, 2010), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

48. Stephanie Yang & Elena Holodny, *The Massive Hack of the NASDAQ that has Wall Street Terrified of Cyber Attacks*, BUSINESS INSIDER (Jul. 17, 2014), http://www.businessinsider.com/nasdaq-attacked-by-hackers-2014-7.

49. SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX xii-xviii (2014).

50. The use of financial sanctions, which impose burdens on designated persons, has attracted some degree of criticism because those burdens are not accompanied by the same procedural protections involved in criminal prosecutions. Sanctions determinations are, however, subject to extensive legal review within the executive branch and are subject to ex post judicial review, and generally do provide designated persons with an opportunity to challenge the restrictions imposed on them.

do so at all.[51]

The May 2014 indictment focused on five members of the Chinese People's Liberation Army (PLA) alleged to have conspired to steal information from U.S. companies that would be useful to competitors in China, including state-owned enterprises (SOEs).[52] The theft included trade secrets, pricing information that allowed companies to underbid U.S. competitors;[53] sensitive, internal communications "that would provide a competitor, or adversary in litigation, with insight into the strategy and vulnerabilities of the American entity";[54] and "proprietary and confidential technical and design specifications" for components of nuclear power plants that a U.S. firm had been contracted to build in China.[55] The theft of this sensitive or proprietary information generated the potential for significant commercial advantage to the recipients of the data.

This information was provided to Chinese companies in circumstances suggesting they knew about – or potentially directed – the theft of the intellectual property at issue, rendering them subject to financial sanctions under EO 13694. Indeed, "Chinese firms hired the same PLA Unit where the defendants worked to provide information technology services," while one Chinese SOE "involved in trade litigation against some of the American victims mentioned [in the indictment] hired the Unit, and one of the co-conspirators charged herein, to build a 'secret' database to hold corporate 'intelligence.'"[56] If the Chinese SOEs described in the indictment did direct the theft at issue, they could almost certainly be subject to sanctions under EO 13694 (as they would be if they knowingly received or used misappropriated property for financial gain). Imposing such sanctions on the companies would cut them out of the international financial system, rendering their exercise in misappropriation worthless.[57]

There are three main potential drawbacks to the use of sanctions in the cybersecurity context – the potential to provoke retaliation by the government of the sanctions targets (e.g. Russia or China); potential difficulties for technology companies in implementing cyber security sanctions; and due process questions pertaining to the use of classified evidence to impose financial

---

51. *See, e.g.*, Press Release, U.S. Dep't of Justice, Russian Hacker Arrested for Computer Hacking Scheme that Victimized Thousands of Credit Card Customers (July 7, 2014), http://www.justice.gov/usao-wdwa/pr/russian-hacker-arrested-computer-hacking-scheme-victimized-thousands-credit-card (noting that more than three years elapsed between the indictment and arrest of Russian national Roman Seleznev for hacking point of sale terminals and stealing credit card data).

52. The facts as alleged by the Department of Justice are contained in Indictment, *United States v. Wang Dong et al.*, Cr. No. 14-118 (W.D.Pa. May 1, 2014).

53. *Id*. at 2.

54. *Id.* at 2-3.

55. *Id.* at 4.

56. *Id.* at 3.

57. The Treasury Department has imposed sanctions on companies linked to Chinese state-owned enterprises in the past, as in 2012 when it imposed sanctions on Bank of Kunlun, a unit of the state-owned China National Petroleum Co., for conducting transactions with Iran that transgressed U.S. sanctions. Wayne Ma, *China Scolds U.S. Over Iran-Related Bank Sanctions*, WALL ST. J. (Aug. 1, 2012), http://www.wsj.com/articles/SB10000872396390444320704577562330527832056.

sanctions.[58] These drawbacks notwithstanding, the tool remains a powerful option for combating financially motivated cybercrime.

Perhaps the most important challenge regarding the implementation of cybersecurity sanctions pertains to the threat of retaliation. Both Russia and China – two countries whose nationals would likely be the target of sanctions under EO 13694 – have shown an increased willingness to use the tools of economic statecraft to their perceived advantage, which might pose a threat to U.S. companies against whom Russia and China may retaliate with sanctions measures of their own. China, for example, recently threatened sanctions against companies that sell arms to Taiwan, and in 2010 cut off supplies of rare earth metals to Japan in the midst of tension between the two Asian nations.[59] So too has Russia banned imports of certain European goods after the imposition of sanctions following Russia's aggression in Ukraine in 2014.[60] When contemplating the use of sanctions in the cybersecurity context, therefore, U.S. officials must weigh the expected benefits of doing so against the anticipated costs and potential for retaliation. Sanctions also should not proceed without robust diplomatic outreach to the home jurisdiction of the potential target conducted with an eye toward shutting down the offending activity. Failing the success of a collaborative approach, government officials may proceed with sanctions, but should conduct outreach to the private sector to help it prepare for any retaliatory measures it may anticipate.

The second important potential negative consequence of using financial sanctions in the cybersecurity context are difficulties that technology and telecommunications companies may have in implementing them. U.S. persons – no matter the industry – are obligated to adhere to U.S. law, including with respect to financial sanctions. But while the financial services industry has significant experience in developing programs to help them comply with sanctions restrictions, technology firms (particularly young start-ups) may have less experience

58. There are two other broad categories of concern/criticism that have been levied in the financial sanctions context. The first pertains to whether sanctions are effective in achieving their stated goal – typically either incentivizing a change in behavior in the target or denying the target access to the financial resources it needs to engage in illicit activity. *See, e.g.*, ELIZABETH ROSENBERG, ZACHARY K. GOLDMAN, DR. DANIEL DREZNER & JULIA SOLOMON-STRAUSS, THE NEW TOOLS OF ECONOMIC WARFARE: EFFECTS AND EFFECTIVENESS OF CONTEMPORARY U.S. FINANCIAL SANCTIONS, CENTER FOR A NEW AMERICAN SECURITY (2016), http://www.cnas.org/sites/default/files/publications-pdf/CNASReport-EconomicWarfare-160408v02.pdf, for a detailed discussion and citations to literature about ways to conceptualize and measure the effectiveness of financial sanctions. The second pertains to questions about basic procedural fairness regarding measures applied against individuals or entities according to administrative processes that differ in their procedural protections from criminal trials. *See, e.g.*, CIAN MURPHY, EU COUNTER-TERRORISM LAW: PRE-EMPTION AND THE RULE OF LAW (2012).

59. *China Threatens Sanctions Against Firms in Taiwan Arms Sale*, ASSOCIATED PRESS (Dec. 16, 2015), http://bigstory.ap.org/article/012fb53178554ae1ab58615be7ed8f10/china-threatens-sanctions-against-firms-taiwan-arms-sale; Keith Bradsher, *Amid Tension, China Blocks Vital Exports to Japan*, N.Y. TIMES (Sept. 22, 2010), http://www.nytimes.com/2010/09/23/business/global/23rare.html.

60. Paul Sonne & Anton Troianovski, *Russia Bans Food Imports in Retaliation for Western Sanctions*, WALL ST. J., (Aug. 7, 2014), http://www.wsj.com/articles/russia-bans-food-imports-in-retaliation-to-western-sanctions-1407403035.

in doing so. Indeed, in 2015, PayPal reached a settlement with the Treasury Department over apparent sanctions violations because PayPal did "not appear to have implemented effective compliance procedures and processes to identify, interdict, and prevent transactions in apparent violation of the sanctions programs administered by OFAC [Office of Foreign Assets Control]."[61] The government's use of this authority should, therefore, be accompanied by outreach to the technology community to ensure that companies in that sector understand their compliance obligations and are able to adhere to the restrictions without unduly hindering innovation.

A final criticism of sanctions programs more broadly pertains to due process implications derived from the use of classified evidence in designations. The International Emergency Economic Powers Act (IEEPA), the statutory authority on which EO 13694 is based, contains a provision permitting *in camera ex parte* judicial review of any classified information relied on by the government in the administrative record underlying a sanctions designation if that designation is challenged in court.[62] Courts have long held that the government is permitted to use classified information in the designation process so long as the government provides sufficient portions of the unclassified administrative record to the designated party to rebut the claims against it.[63] The ability to use classified information in the administrative record and in judicial review of a sanctions decision will be particularly important with respect to sanctions for cybercrime, where there may be important classified information tending to establish attribution of particular attack in addition to unclassified information. Notwithstanding the utility of classified information in this context, the government should endeavor to release as much information as possible when imposing cybersecurity sanctions. And when the government enacted EO 13694, the Acting Director of OFAC noted that it "endeavor[s] with each and every designation to go out with a public press release that outlines the reason we're taking the action."[64] Doing so will be critical to garnering as broad a base of support as possible for the government's actions, particularly among technolo-

61. Settlement Agreement between U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and PayPal, Inc., No. MUL-762365 (Mar. 23, 2015), https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20150325_paypal_settlement.pdf.

62. 50 U.S.C. §1702(c).

63. *See*, *e.g.*, People's Mojahedin Org. of Iran v. U.S. Dep't of State, 613 F.3d 220 (D.C. Cir. 2010); Kadi v. Geithner, 42 F. Supp. 3d 1, 29 (D.D.C. 2012) (upholding designation of Kadi where he "did not receive the full unclassified administrative record prior to the March 2004 decision, [but] he did receive an opportunity, in substance, to rebut the evidence found in the unclassified administrative record through his own submissions to OFAC, as well as the opportunity to respond robustly to OFAC's follow-up questions."). Further complicating matters is the fact that non-citizens outside the United States who do not have a "substantial connection" to the U.S. generally do not have the right to raise constitutional claims in U.S. courts. *See Kadi*, 42 F. Supp. 3d at 25-29.

64. John Smith, Acting Director, Office of Foreign Assets Control, On-the-Record Press Call on the President's Executive Order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (Apr. 1, 2015), https://www.whitehouse.gov/the-press-office/2015/04/01/record-press-call-president-s-executive-order-blocking-property-certain-.

gists who often have "anti-secret and libertarian inclinations."[65]

B. Hybrid Models: Public/Private Partnerships to Attack Instrumentalities of Financially Motivated Cybercrime

In addition to sanctions that diminish the expected value of cybercrime to deter its commission, innovative public/private partnerships have emerged in the last several years that can raise the cost of cybercrime to its perpetrators. These activities leverage existing legal instruments, like trademark law and the Computer Fraud and Abuse Act (CFAA) to disrupt the actual instrumentalities of financially motivated cybercrime. One method of collaboration in particular – partnerships to take down botnets – deserves analysis because botnets are an important tool for the perpetration of many types of financially motivated cybercrime.[66]

Regulatory interventions that make it easier to take down botnets make it costlier to use them to perpetrate cybercrime, deterring such criminal activity through the same mechanism of influence as financial sanctions. Botnets are networks of "individual computers, each running software that allows communication among those computers and allows centralized or decentralized communication with other computers providing control instructions. The individual computers in a botnet often belong to individual users who have unknowingly downloaded or been infected by malware, assimilating computer into botnet."[67] Botnets can be operated by a small number of "command and control" servers, or in a peer-to-peer fashion.

Botnets can be used to generate spam, commit click-fraud, steal information, or conduct other kinds of financial crime, like fraudulently mine Bitcoins.[68] As botnets are the instrumentality through which substantial amounts of cybercrime takes place, disrupting them can raise the potential cost of criminal activities.

While botnets might at this point be commodity items, which are widely available and can even be rented,[69] the key point in this discussion is to

---

65. PETER SWIRE, THE DECLINING HALF-LIFE OF SECRETS AND THE FUTURE OF SIGNALS INTELLIGENCE 4 (2015), https://static.newamerica.org/attachments/4425-the-declining-half-life-of-secrets/Swire_DecliningHalf-LifeOfSecrets.f8ba7c96a6c049108dfa85b5f79024d8.pdf.

66. Botnets are also commonly used for Denial of Service attacks, often considered a form of "hacktivism," like the DOS attacks against prominent banks in September 2012 attributed to Iran. *See* Siobhan Gorman & Julian E. Barnes, *Iran Blamed for Cyberattacks*, WALL STREET JOURNAL (Oct. 12, 2012), http://www.wsj.com/articles/SB10000872396390444657804578052931555576700.

67. Complaint at 11, Microsoft Corp. v. John Does 1-8 Controlling a Computer Botnet Thereby Injuring Microsoft and its Customers, No. A 13-CV-1014 (W.D. Tx. 2013) [hereinafter *ZeroAccess Complaint*].

68. Danny Yuxing Huang et al., *Botcoin: Monetizing Stolen Cycles*, 2014 PROC. OF THE NETWORK AND DISTRIBUTED SYS. SECURITY SYMPOSIUM 1, http://cseweb.ucsd.edu/snoeren/papers/botcoin-ndss14.pdf.

69. Tim G., *Renting a Zombie Farm: Botnets and the Hacker Economy*, SYMANTEC OFFICIAL BLOG (Aug. 8, 2014), http://www.symantec.com/connect/blogs/renting-zombie-farm-botnets-and-hacker-economy; *see also* Juan Caballero et al., *Measuring Pay-per-Install*: *The Commoditization of Malware Distribution*, PROC. OF THE 20TH USENIX SECURITY SYMPOSIUM, SAN FRANCISCO, CA (Aug. 2011), https://www.usenix.org/legacy/event/sec11/tech/full_papers/Caballero.pdf.

illustrate the ways in which legal and regulatory instruments can be used to raise the cost of engaging in financially motivated cyberattacks. What follows will be a description and analysis of two botnet takedowns that were a result of innovative models of public/private partnership. Bolstering these kinds of tools might not have decisive effects on cybercrime. They will, however, affect the ability of cyber criminals to achieve their objectives in specific instances, and will, in aggregate, raise the cost and risk of illicit cyber activity.

The ZeroAccess botnet, once one of the largest botnets in operation, delivered a wide range of malware, but was used primarily to engage in "click-fraud." Click-fraud is a type of cybercrime in which malware "imitate[s] a legitimate user's clicking of an advertisement for the sole purpose of generating a charge per click, but fail[s] to reflect or monetize any interest in the product or service being advertised."[70] Security researchers estimated that ZeroAccess led to losses of $2.7 million per month for advertisers.[71]

ZeroAccess was taken down in December 2013 in a concerted effort between Microsoft, Europol, and law enforcement agencies of several European countries. On the date of the takedown, the law enforcement agencies executed search warrants and seizure orders on several servers involved in fraudulent activity.[72] At the same time, Microsoft filed suit against eight John Doe defendants alleging harms under a number of theories. These included claims under the CFAA alleging that the botmasters gained unauthorized access to, and changed, Windows operating systems, search engines, and web browsers that Microsoft had licensed to computer users whose machines were incorporated into the botnet.[73] Microsoft also alleged claims under the Lanham Act that the botnet reduced the performance of Windows products and caused "injury to Microsoft's brand, reputation and goodwill."[74]

Perhaps more important, however, Microsoft sought – and the Court in the Western District of Texas granted – injunctive relief that ordered Internet Service Providers (ISPs) to block traffic coming from the servers, IP addresses, and domains that controlled the botnet.[75] The intention of the order was to sever communications between the command and control nodes of the botnet and the infected computers.

The takedown of the ZeroAccess botnet had some effect, though it proved to be transient. Certain portions of the botnet were taken down by the combined Microsoft and Europol activity, while the next day "the malware authors

70. *ZeroAccess Complaint*, *supra* note 67, at 10.

71. *Click Fraud in ZeroAccess*, *supra* note 38, at 142.

72. Press Release, Europol, Notorious Botnet Infecting 2 Million Computers Disrupted, https://www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted.

73. *ZeroAccess Complaint*, *supra* note 67, at 15-18.

74. *Id.* at 18, 20-26.

75. *Ex parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction, Microsoft Corp. v. John Does 1-8 Controlling a Computer Botnet Thereby Injuring Microsoft and its Customers, No. A 13-CV-1014 (W.D.Tx. Nov. 25, 2013), ECF No. 17.

distributed a new set of modules that halted all click fraud activity but left the . . . network intact. Inspection of these modules revealed the . . . text 'WHITE FLAG' in apparent surrender."[76] Several months later the authors of the malware had revived the botnet, but did so with some of the functionality removed.[77]

Similar public/private collaborations were responsible for the disruption of the Gameover Zeus Botnet (and also Cryptolocker, an online extortion scheme) in the summer of 2014. The Gameover Zeus botnet was a sophisticated scheme that stole banking credentials and resulted in an estimated $100 million in losses.[78] The disruption was effected by obtaining court orders "authorizing measures to redirect the automated requests by victim computers for additional instructions away from the criminal operators to substitute servers established pursuant to court order."[79] The botnet disruption was accompanied by the indictment of the Russian national alleged to be the administrator of Gameover Zeus.

The efforts of Microsoft and law enforcement agencies to take down botnets through injunctive relief and other legal mechanics have not been without controversy, grounded specifically in the criticism that in the course of taking down fraudulent web activity there is substantial "collateral damage" to legitimate web traffic that might make use of the same or linked facilities.[80] Criticisms can also be levied about the effectiveness of such activities. But in this general approach, there is a method systematically to raise the cost of financially motivated cybercrime. Reform projects aimed at easing the path to botnet takedowns should be considered, but in doing so the advantages of facilitating botnet disruptions and other activities must be weighed against the anticipated collateral damage, which should be mitigated as much as possible.

C. Reducing the Incentive to Steal: Interdicting the Proceeds of Cybercrime

The two interventions described above focus on ways to raise the cost of data theft, reducing the incentives for its commission. This section instead focuses on making it more difficult for the perpetrators of financially motivated cybercrime to obtain access to their ill-gotten gains by interfering with the financial institutions that (wittingly or unwittingly) facilitate it. This approach has been implemented most effectively in the context of cybercrime leading to the sale of intellectual property-infringing goods, and is grounded in the insight that bank-

76. *Click Fraud in ZeroAccess*, *supra* note 38, at 144.

77. *Id.*

78. Press Release, U.S. Dep't of Justice, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (Jun. 2, 2014), http://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.

79. *Id.*

80. *See, e.g.*, Brian Krebs, *Microsoft Darkens 4MM Sites in Malware Fight*, KREBS ON SECURITY (July 14, 2014), http://krebsonsecurity.com/2014/07/microsoft-darkens-4mm-sites-in-malware-fight/comment-page-1.

ing relationships are indispensable for the monetization of cybercrime, but are fragile and difficult to replace once disrupted.

Many botnets are monetized by directly sending email spam or rented as building blocks for other forms of abusive advertising, such as creating accounts to spam Facebook, Twitter and other social networking sites.[81] Studies have documented that the bulk of spam advertises intellectual property-infringing products, such as counterfeit pharmaceuticals, luxury goods, and pirated media (e.g., software),[82] purchased mostly by consumers in North America and Western Europe.[83]

While there are a number of payment options available to online consumers, researchers found that cybercriminals depend substantially on credit card payments to operate their illicit networks. Credit cards were used, for example, in 95% of all purchases for organization selling counterfeit pharmaceuticals online that had annualized gross revenues of $68 million in 2009.[84] The use of credit cards can scale in a way that the use of Bitcoin to facilitate payments for fraudulent goods cannot.[85] If this wealth transfer can be disrupted, it will deter cybercriminals from engaging in this form of profit-motivated cybercrime by making it substantially costlier and riskier to run their networks, discouraging them from engaging in cybercrime.

The manner in which payment networks such as Visa and MasterCard facilitate payments between merchants and consumers can be leveraged to disrupt the transfer of value to cybercrime networks. Companies like MasterCard and Visa do not directly issue payment cards and interact with merchants. Instead they create networks with established rules and standards with respect to payment processing that third-party issuers and acquirers must follow to participate in the credit card networks. Credit card payments using open-loop networks involve five entities: a cardholder (customer); an issuing bank that manages the customer's account; a merchant (in our case a cybercriminal

81. Kurt Thomas, et al., *Framing Dependencies Introduced by Underground Commoditization*, WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY, AMSTERDAM, NL 1-3, 5 (June 2015), https://cseweb.ucsd.edu/savage/papers/WEIS15.pdf [hereinafter *Framing Dependencies*].

82. Kirill Levchenko, et al, *Click Trajectories: End-to-End Analysis of the Spam Value Chain*, PROCEEDINGS OF THE IEEE SYMPOSIUM AND SECURITY AND PRIVACY, OAKLAND, CA 6 (May 2011), https://cseweb.ucsd.edu/savage/papers/Oakland11.pdf.

83. Chris Kanich, et al., *Show Me the Money: Characterizing Spam-advertised Revenue*, PROCEEDINGS OF THE USENIX SECURITY SYMPOSIUM, SAN FRANCISCO, CA, 11 (Aug. 2011), https://www.usenix.org/legacy/events/sec11/tech/full_papers/Kanich.pdf.

84. Damon McCoy, et al, *PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs*, 13, 15, 21ST USENIX SECURITY SYMPOSIUM 12, WA (2012), https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final204.pdf.

85. The total global market capitalization of Bitcoin, for example, is estimated at $6.5 billion. *See* Jemma Kelly, *Record Highs Predicted for Bitcoin in 2016 as New Supply Halves*, REUTERS (Dec. 23, 2015), http://www.reuters.com/article/us-global-markets-bitcoin-analysis-idUSKBN0U60GM20151223. While the total market capitalization of Bitcoin may grow with time, the number of people using credit cards for payment substantially exceeds that using Bitcoin (or other virtual currencies) and so is attractive to criminals seeking to obtain as much revenue as possible. Additionally, at present, Bitcoin can only support a limited number of transactions per second.

selling counterfeit goods); an acquiring bank that manages the merchant's account; and a cardholder association (e.g., Visa or MasterCard) that manages the credit card network and strikes agreements with banks. In their relationships with acquiring banks the card networks provide that the banks must "ensure" that merchants to whom they provide services "do not process illegal transactions or undertake illegal activities."[86]

If merchants that sell fraudulent goods through cybercrime lack access to banking services, they will be unable to realize a profit through criminal activity and will be less likely to engage in it. To the extent that this kind of cybercrime is concentrated in a small number of financial institutions, disrupting those monetization nodes can have a disproportionate impact on the financial viability of cybercrime.

A recent study found that there is just such a concentration of banking services for illicit merchants, at least some of the time: for a particular spam network, just three acquiring banks managed the merchant accounts for 95% of the nearly 1 billion spam messages analyzed.[87] This small number of banks willing to underwrite accounts for "high risk" merchants can be attributed to the fact that banks take on liability (charge backs and fines imposed by cardholder associations) for the activities of merchants with whom they do business. Because there are not many banks willing to work with high-risk merchants who are more likely to engage in cybercrime, the relationships between acquiring banks and cybercriminals are incredibly important and difficult to replicate. This dynamic makes these relationships an attractive place to attempt to raise the cost of monetizing the sale of fraudulent goods.

Recognizing the importance of the small number of banks that facilitate cybercrime, credit card companies have taken action to disrupt the relationship between acquiring banks and high-risk merchants in order to make it harder for them to profit from digital crime. In 2011 Visa enacted a number of changes to their acquiring bank regulations that strengthened their Global Brand Protection Program (GBPP). The GBPP imposed controls on acquiring banks to "ensure that their merchants do not process transactions that are illegal" or that might have negative reputational costs for the banks or the credit card networks.[88] The document describing the GBPP provides examples of illicit transactions it covers, including "Unlawful sale of prescription drugs" and "Sale of counterfeit or trademark infringing products or services."[89] It also specifies that acquiring banks that violate these rules by issuing accounts to merchants selling these classes of goods could be subject to escalating fines for repeated infractions.[90]

86. VISA GLOBAL BRAND PROTECTION, PROGRAM GUIDE FOR ACQUIRERS 6 (2011) (on file with authors) [hereinafter VISA GBPP GUIDE].

87. *See* Levchenko et al., *supra* note 82, at 13-14.

88. VISA GBPP GUIDE, *supra* note 86, at 1.

89. *Id.* at 9-10.

90. *Id.* at 12-15.

At the same time that Visa was adopting the GBPP, a series of negotiations between brand holders like luxury goods companies and pharmaceutical companies, payment providers, and the White House's Intellectual Property Enforcement Coordinator developed strategies to address the sale of counterfeit goods on the Internet.[91] Through this effort, individual brand holders can submit evidence of infringement (e.g. from undercover purchases of their products) to the card networks, who then identify the associated acquiring bank and request remediation.[92] The card networks can then impose fines and further action for continued or additional non-compliance.

In addition to the independent actions of brand holders and card networks, in January 2012 the International Anti-Counterfeiting Coalition (IACC) announced their RogueBlock initiative, which provides a standard portal by which brand holders can report infringing e-commerce sites.[93] The IACC, with their contractors and the card networks, engages in the test purchases required to identify merchant accounts used to monetize reported infringing sites and manages the formal complaint process through the card networks. As of October 2015, the IACC reported that their Rogue Block program had resulted in the termination of over 5,000 merchant accounts.[94]

NYU security researchers found that persistent brand holder intervention from 2011–2012 disrupted payment processing for criminals for months at a time.[95] This insight is critical for two reasons. First, it inverts the conventional wisdom about cybercrime that suggests that attackers have an asymmetric advantage. While attackers might have an advantage in penetrating a network in the first instance, this method of disrupting the payment networks of cybercriminals demonstrates that there is a corresponding advantage for the defender in disrupting the payment networks that feed cybercrime, at least to the extent that those networks use credit cards to monetize fraud or engage in the sale of intellectual property-infringing goods. This is because it takes a defender only one successful test product purchase to identify abuse and notify the merchant bank involved, facilitating severance of the relationship between an acquiring bank and a fraudulent merchant and a disruption of the monetization chain.

Second, unlike other forms of disruption or intervention, disrupting the relationship between acquiring banks and merchants selling fraudulent goods can have a large financial impact: assets seized by a merchant bank in response

---

91. Brian Krebs, *Ever Wondered Who's Behind Those Viagra Emails*, POLITICO MAG., Dec. 16, 2014, http://www.politico.com/magazine/story/2014/12/pharma-spam-113562. *See also* EXEC. OFFICE OF THE PRESIDENT, 2010 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR ANNUAL REPORT ON INTELLECTUAL PROPERTY ENFORCEMENT (2010).

92. Damon McCoy et al., Priceless: The Role of Payments in Abuse-advertised Goods, *in* PROCEEDINGS OF THE 2012 ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 845, 848 (2012) [hereinafter *Priceless*].

93. INTERNET ANTICOUNTERFEITING COALITION, ROGUEBLOCK, http://www.iacc.org/online-initiatives/rogueblock.

94. *Id.*

95. *Priceless, supra* note 92, at 853, 855.

to an intervention from a credit card network or brand holder can exceed $1 million.[96] In the aftermath of a disruptive event, criminals must find new merchant banks that they can deceive into taking on their high risk activity, the bureaucratic process for which is very complicated.

Discussions in certain underground cybercrime forums have recorded qualitative evidence of the impact of a brand holder's intervention. As one poetically-inclined cybercriminal wrote (translated from the Russian), "The sun is setting on the OEM [Original Equipment Manufacturer] era," – a reference to the actions on the part of Microsoft to undermine payment processing for the sale of counterfeit software.[97] In reaction to the payment disruption efforts of a major pharmaceutical company, a leading underground figure wrote (again translated from the Russian), "Right now most affiliate []programs have a mass of declines, cancels and pendings, and it doesn't depend much on the program IMHO, there is a general sad picture, . . . Visa is burning us with napalm."[98]

Recent litigation has bolstered the ability of companies to engage in this kind of disruptive activity by facilitating the ability of brand holders to obtain discovery about bank accounts held by cybercriminals alleged to have infringed on their brands. In September 2015, for example, a court in the Southern District of New York granted Gucci's motion to compel the Bank of China to comply with subpoenas requesting the production of account documents relating to defendant counterfeit merchants in Gucci's trademark infringement case.[99] Obtaining information about the assets held by alleged infringers paves the way for brand holders to pursue asset seizure and forfeiture claims in addition to encouraging the cardholder associations to terminate merchant accounts in accordance with their rules barring the use of their networks for illicit activity.

These payment intervention strategies have not gone unopposed by criminal merchants fighting to retain their ability to monetize cybercrime. Their main responses have been to contract third-party Payment Service Providers that have escalated efforts to detect and filter test purchases, which are required for Visa or MasterCard to link merchants committing cybercrime to their bank accounts.[100] Foreign and domestic bank secrecy laws may also pose an obstacle to pursuing this approach at scale. Work continues to map the monetization networks for stolen data in the same way that scholars have unraveled the payment networks that make the digital sale of copyright infringing goods.[101] But while the seizure of funds linked to stolen or counterfeit property may not

96. *Id.* at 9.

97. *Id.* (internal quotation marks omitted).

98. *Id.* (internal quotation marks omitted).

99. Gucci America, Inc. v. Weixing Li, et al., No. 10 Civ. 4974(RJS), 2015 WL 5707135, at *15 (S.D.N.Y., Sept. 29, 2015).

100. *Priceless, supra* note 92, at 854-855.

101. *See, e.g.*, Damon McCoy, N.Y.U., Bullet-Proof Credit Card Processing, Presentation at USENIX Enigma Conference (Jan. 25-27, 2016).

be a panacea, it does suggest a promising way to diminish the expected benefits of cybercrime.

III. TRADITIONAL CHALLENGES TO CYBER DETERRENCE: SECRECY OF CAPABILITIES AND ATTRIBUTION

Two traditional obstacles to developing strategies of deterrence in cyberspace are the secrecy with which states treat cyber capabilities, and the problem of determining with confidence the actual identity of the perpetrators of an attack. While these problems are still present in the discussion about the measures described above, the use of generally available regulatory tools, as opposed to specifically-imposed retaliatory capabilities, elides some of the difficulties that secrecy and the attribution problem have posed to the development of effective cyber deterrence strategies.

A. Secrecy Surrounding Cyber Response Capabilities

Secrecy poses a challenge to deterrence. This is because deterrence depends upon the credible communication of a threat of retaliation by a target to a challenger. The credible communication of retaliatory options is central to deterrence theory and to specific deterrence strategies, because fundamentally "it [is] not a state's capacity to do harm that enable[s] it to practice deterrence, it [is] others' belief that it ha[s] such a capacity."[102]

The secrecy with which governments have treated cyber capabilities is, therefore, inconsistent with the traditional understanding of what is required for a deterrent threat to be effective – namely, the clear communication of a credible threat of retaliation to a challenger.[103] Because most states regard their cyber capabilities as secrets of the highest order, establishing the clear statements of intent required to influence adversaries has proven challenging.[104] Indeed, "Under the logic of deterrence, conveying some information to the challenger with great clarity, especially about one's military capabilities, is beneficial."[105] The secrecy surrounding cyber capabilities also has posed a challenge to the development of international law in cyberspace, as the law "cannot be significantly clarified or developed without a pool of publicly acknowledged state practice."[106]

An approach to deterring cybercrime that relies on regulatory measures to deprive criminals of the benefits they anticipate with their theft avoids some of the problems posed by secrecy. It does so by focusing deterrence efforts not on

---

102. MORGAN, DETERRENCE NOW, *supra* note 26, at 15.

103. T.V. Paul, *Introduction* to COMPLEX DETERRENCE: STRATEGY IN THE GLOBAL AGE 2 (T.V. Paul et al. eds., 2009).

104. Austin Long, *Deterrence: The State of the Field*, 47 NYU J. INT'L L. & POLS 357, 374-376 (2015).

105. MORGAN, DETERRENCE NOW, *supra* note 26, at 17.

106. Alexandra H. Perina, *Black Holes and Open Secrets: The Impact of Covert Action on International Law*, 53 COLUM. J. TRANSNAT'L L. 507, 582 (2015).

attacking particular actors in the cyber domain, but rather by using generally available regulatory tools to deprive criminals of the value of their stolen assets. Deterring financially motivated cybercrime in the manner described above therefore relies less on technical capabilities (though there is an important place for such capabilities, highlighted below in the discussion of attribution) and more on an approach to deterrence that focuses on holding assets at risk about which cyber criminals care – namely, their hard-stolen money.

In using financial sanctions and other measures to deter financially motivated cybercrime, victims and their governments hold at risk assets that perpetrators care about. But they do so by offering a credible threat to render worthless a cyber criminal's investment in stolen assets. What will matter here, therefore, is regular demonstration of the willingness to engage in the activities described above.

B. Attribution

"Doing attribution well is at the core of virtually all forms of coercion and deterrence."[107] This is because deterrence is fundamentally about communication, and one cannot tailor a deterrent message appropriately if one does not know with confidence whom the recipient should be. With a strategy of deterrence dependent on imposing punishment, effective deterrence depends on punishing the right person. Without confidence in attribution, the victim of an attack cannot convince potential attackers or third parties that specific actions will have repercussions, and, conversely, that innocence will shield a party from negative consequences.[108]

It is generally understood that attributing cyberattacks to their ultimate perpetrators with a high degree of confidence remains difficult, and while senior government officials have noted their improved ability to attribute cyberattacks in recent years, "it continues to be a challenge."[109] Indeed, the scope of the challenge became clear in early 2015 when the F.B.I. and the Intelligence Community were compelled to release progressively greater amounts of information about North Korea's responsibility for a devastating attack against Sony Pictures to assuage public skepticism about the Hermit Kingdom's culpability.[110]

---

107. Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUD. 1-2, 4 (2015).

108. *See* discussion in LIBICKI, CYBERDETERRENCE AND CYBERWAR, *supra* note 4, at 41-52.

109. Michael Daniel, White House Cybersecurity Coordinator, On-the-Record Press Call on the President's Executive Order, Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities (Apr. 1, 2015); *see also* Leon E. Panetta, Secretary of Defense, Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012) ("DoD has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment. Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America.").

110. Ellen Nakashima, *FBI Director Offers New Evidence to Back Claim North Korea Hacked Sony*, WASH. POST, Jan. 7, 2015, https://www.washingtonpost.com/world/national-security/fbi-director-offers-new-evidence-to-back-claim-north-korea-hacked-sony/2015/01/07/ce667980-969a-11e4-8005-1924ede3e54a_story.html.

An approach to deterring financially motivated cybercrime that relies on generally available regulatory measures, however, avoids some of the attribution problems attendant with an approach to cyber deterrence that depends on retaliation in cyberspace or in other domains.

To be clear, a regulatory approach to cyber deterrence does not escape entirely the challenge of attribution. In order to impose sanctions, take down botnets, or seize assets, the U.S. government and the victims of cybercrime must have confidence that they understand who is responsible for perpetrating a given act of cyber theft. But if sanctions are imposed and botnets taken down with sufficient regularity, cybercriminals contemplating cybercrime for profit will be forced to think twice about their activities.

Moreover, the noted theorist of military strategy Thomas Rid reminds us that attribution is not binary. It is, rather, a nuanced process, "an art as much as a science," and, crucially for these purposes, "is a function of what is at stake politically."[111] In this regard, "The more severe the consequences of a specific incident, and the higher its damage, the more resources and political capital will a government invest in identifying the perpetrators."[112] Rid also emphasizes the importance of combining technical determinations regarding attack vectors (the "how") with operational and strategic analysis about the attacker's profile, as well as the attack's rationale, significance, and appropriate response (the "what," "who," and "why").[113]

The sanctions and other interventions described above change the stakes involved in the attribution discussion in two ways. First, they are principally directed at non-state actors, rather than at nation-states per se, reducing the chances that acts of cyber retaliation will lead to conflict between states. In this way, deterrence of financially motivated cybercrime mimics other ways of cracking down on illicit activities, where it is common for private individuals and entities to be prosecuted and subject to sanctions in a range of different contexts. Second, once used in a sufficient number of instances, financial sanctions and regulatory interventions raise the general risk that misappropriated assets will be rendered worthless, diminishing cyber thieves' motivation to engage in cyber-enabled theft in the first instance. This general deterrence will, with time, reduce the attractiveness of certain kinds of targeted activity.

Furthermore, the U.S. government often demonstrates that it is capable of making public attribution information regarding the digital theft of intellectual property. This occurs most often in the context of criminal prosecutions, which require a higher evidentiary burden than the imposition of financial sanctions.[114] And while the government has not yet (to the public's knowledge) retaliated kinetically or in cyberspace against a cyberattack, the government has publicly

111. Rid & Buchanan, *supra* note 105, at 7.
112. *Id.* at 30.
113. *Id.* at 10.
114. *See* Indictment, United States v. Pang, No. Cr-15-00106-EJD (N.D.Ca. Apr. 1, 2015).

attributed specific attacks (e.g. the 2014 attack against Sony) to nation-states like North Korea. The president himself, as well as several of his most senior advisors, also more generally identified China-based cyber theft of intellectual property as a strategic problem. And in June 2015, "U.S. officials" attributed a significant data breach at the Office of Personnel Management to "[h]ackers working for the Chinese state."[115]

In addition to the nation-state linked attributions just described, the government regularly prosecutes data breaches and cybercrime cases that are not linked to nation-states. While the stakes in these cases (invoking Rid's taxonomy) are lower, they nonetheless require the attribution of specific attacks to specific individuals with a high degree of confidence ("beyond a reasonable doubt" for conviction by a jury of the hacker's peers).[116]

In the case of financial sanctions, the sources of information that support a designation decision also enhance the ability of the government to attribute with confidence because the government is likely to have access to unclassified attribution data in addition to classified sources of information. One source will likely be technical data about the intrusion that comes from the victim company. This data generally is not classified, and so the government might have the ability to use it (or use it in a sanitized form) to make a public case that the imposition of sanctions is justified. A second source of data will be classified technical and non-technical data that comes from the U.S. Intelligence Community. Because the Department of the Treasury has the ability to make use of classified information in the compilation of the administrative record that supports a sanctions designation, it can combine technical attribution data with any available human or signals intelligence reporting to increase its level of confidence in the decision.

At the same time, the imposition of financial sanctions is a public act, and the government will need to be able to publicize sufficient information about the perpetrators of cyber theft to convince a sometimes-skeptical public of the accuracy of its determination (including, perhaps, technical attribution data). This is a reversal from the standard practice where the amount of information revealed in the context of a sanctions designation is minimal.

The attribution problem in cyberspace is inescapable, but it need not paralyze action. As with any government intervention, there are tradeoffs to be made among various options for pursuing difficult cases: should the government prosecute a particular offender, or impose sanctions; should it engage diplomati-

115. Ellen Nakashima, *Chinese Breach Data of 4 Million Federal Workers*, WASH. POST, Jun. 4, 2015, https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.

116. See, for example, the following recent indictments for cases where the Department of Justice is prosecuting individuals for hacking-related crimes: Indictment, United States v. Nasenkov, No. 1:09CR01093, (S.D.N.Y. Jul. 24, 2013) (alleging involvement in a variety of ATM hacking schemes and various other financial crimes); Indictment, United States v. Lajud-Pena et al., Cr. No. 13-0259 (E.D.N.Y. Apr. 25, 2013).

cally, or retaliate through intelligence means? At a higher level of abstraction, there always will be difficult questions to weigh about the risks of inadvertently escalating situations by deploying sanctions or taking down botnets.

But the government has demonstrated its ability to publicly attribute attacks with a degree of confidence appropriate for the case in many recent instances, from criminal prosecutions of individual hackers to breaches conducted by sovereign entities against large global media companies. There is no reason to expect that the attribution issue will be more vexatious in the context of financial sanctions or disruption of maliciously-used merchant bank accounts than in other instances.

CONCLUSION

Financially motivated cybercrime constitutes a significant portion of malicious cyber activities that plague the web; as such, deterring its commission is a high order priority. Doing so will require holding at risk the asset that motivates cyber criminals: money. Financial sanctions, measures to take down botnets, and civil or contractual actions that seize the proceeds of cybercrime all can reduce the motivations for malevolent actors to commit financially motivated cybercrime. The methods and strategies described above will not address all types of cyber attacks; acts of cyber war, hacktivism, and attacks on critical infrastructure are generally conducted for a different set of reasons. But, by following the money, at least some progress is possible.

***