

DETERRING FINANCIALLY-MOTIVATED CYBER CRIME

By Zachary K. Goldman
Executive Director, Center on Law and Security
NYU School of Law

Note: This is an early stage draft, sketching out a strategy to deter financially motivated cyber crime. The paper analyzes why a strategy targeting financially motivated cyber attacks differs from deterring acts of cyberwar and cyberattacks against critical infrastructure, the two main issues on which the cyber deterrence discussion has focused to this point. It also analyzes the legal and regulatory measures that can be used to deter financially motivated cyber crime, including, prominently, the administration's new cybersecurity sanctions program.

I. INTRODUCTION: THE DETERRENCE OF ECONOMICALLY-MOTIVATED CYBERCRIME

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 in order to prevent him from something 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 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 cyber crime has struggled to adapt it to the burgeoning world of cyber threats. Admiral Michael Rogers, Director of 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 practitioners of cybersecurity have noted that "deterrence is an undeveloped theoretical space in cyber war today."³

The difficulty in adapting deterrence to the cyber domain derives from the fact that cyber deterrence has thus far focused primarily on two types of cyber threats—threats to critical infrastructure, and the deterrence of cyberattacks in the context of an armed conflict—without explicitly addressing financially-motivated cyber crime. Commercially motivated cyberattacks, however, constitute a predominant portion of cyberattacks,⁴ and represent a significant drag on

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) (available at https://www.nsa.gov/public_info/_files/speeches_testimonies/022315_New_America_Foundation.pdf).

² *Hearing on Postures of U.S. Strategic Command, U.S. Transportation Command and U.S. Cyber Command: Hearing Before the S. Armed Services Committee*, 114th Cong. (2015) (Statement of Sen. John McCain, Chairman).

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

⁴ 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).

economic activity,⁵ and will require different deterrence strategies than other forms of cyber threats.

Focusing on deterring attacks on critical infrastructure and cyberattacks in the context of armed conflict is vitally important because the stakes are high. Cyberattacks that cripple important components of our critical infrastructure could have a devastating effect on the health, safety, and well-being of millions of innocent people. Cyberattacks in the context of anticipated or ongoing hostilities⁶ have the potential to disable important military capabilities at crucial moments during battle,⁷ threatening the viability of a country's defense capability.⁸ Discussions of cyber deterrence in the context of potential future conflicts with China also have received substantial scholarly attention.⁹

But financially-motivated cyberattacks are far more prevalent than cyberattacks that aim to disrupt or destroy critical infrastructure, or cyberattacks in the context of armed conflict.¹⁰ Financially-motivated cyberattacks seek data—generally 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 non-public information that can provide advantage in fiercely competitive global industries. In targeting this type of digital information, financially-motivated cyber criminals are participants in a marketplace for data—albeit a black market—that is “growing in size and complexity” and which has “emerged as a playground of financially driven, highly organized, and sophisticated groups.”¹¹

Because these actors are organized and are motivated by profits, they are acutely sensitive to the costs of their activities. Deterring them requires a defender to raise the cost in time or resources to an attacker of pursuing a particular target. Defenders can also deter attacks by lowering the anticipated benefits that an attacker will receive in a particular act of cyber theft.

⁵ Ellen Nakashima and Andrea Peterson, *Report: Cybercrime and espionage costs \$445 billion annually*, WASH. POST, June 9, 2014; Paul Taylor, *Cybercrime costs US \$100bn a year, report says*, FIN. TIMES, July 23, 2013.

⁶ Cite examples.

⁷ CLARKE AND KNAKE, CYBER WAR, at 5-8 (describing reported Israeli operations to blind Syria's air defense systems before striking a Syrian nuclear facility in September 2007).

⁸ See, e.g., MARTIN C. LIBICKI, RAND NATIONAL SECURITY RESEARCH DIVISION, BRANDISHING CYBERATTACK CAPABILITIES (2013).

⁹ See, e.g., Jon Lindsay, “The Impact of China on Cybersecurity: Fiction and Friction,” *International Security*, Vol. 39 No. 3 (Winter 2014-2015), 7-47.

¹⁰ Indeed, some argue that cyber war has not—and will not—take place. 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.”

¹¹ LILLIAN ABLON, MARTIN C. LIBICKI, ANDREA A. GOLAY, RAND NATIONAL SECURITY RESEARCH DIVISION, MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA (2014), at ix (hereinafter, “MARKETS FOR CYBERCRIME TOOLS”).

Deterrence of financially motivated cyber crime also will rely on different tools than the deterrence of attacks against military targets or critical infrastructure.¹² Instead of cyber retaliation, financial sanctions and other regulatory measures taken as part of a public/private collaboration have the best chance of deterring commercially-motivated cyber theft. This is because these types of interventions have the greatest likelihood of raising the cost—and diminishing the anticipated benefits—of engaging in digitally-enabled theft.

This article will present a strategy for deterring financially-motivated cybercrime that leverages the U.S. government's new financial sanctions program targeting "Significant Malicious Cyber-Enabled Activities,"¹³ as well as collaborative efforts undertaken between the government and private sector to mitigate cyber crime. Public/private collaborations like that between certain technology companies and law enforcement agencies 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 copyright, property law, and other legal regimes to "shut down and bring to justice cybercrime perpetrators."¹⁴

While this article is focused on deterring the most prevalent form of cyberattack—financially-motivated cyber crime—it seeks to establish the larger point that one cannot speak generically about "cyber deterrence." Rather, different kinds of malicious cyber activity demand different, tailored, deterrent strategies. This is because each category of cyber crime 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; and financially-motivated cyber theft.¹⁵ Because threat actors engage in each of these activities for different reasons, the costs to which they will be sensitive will vary, demanding different deterrence strategies.

Financially motivated cyber theft does not generally pose a risk of immediate acute catastrophe—the "Cyber Pearl Harbor" that Leon Panetta described in 2012.¹⁶ Rather, senior government officials are beginning to describe the main cyber crime threat as an "ongoing series of low-to-moderate level cyberattacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security."¹⁷ 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.

¹² See, Martin Libicki, *Cyberdeterrence and Cyberwar*, (Santa Monica, CA: RAND Corporation, 2009), especially pp. 91-116, for a discussion of the importance of retaliation in the deterrence of cyber threats against military or infrastructure targets.

¹³ Exec. Order No. 13694, 80 Fed. Reg. 63, 18077 (Apr. 2, 2015) (hereinafter "EO 13694").

¹⁴ http://blogs.technet.com/b/vertical_industries/archive/2014/09/29/putting-the-lid-on-cybercrime.aspx

¹⁵ Catherine A. Theohary and John W. Rollins, *Cyberwarfare and Cyberterrorism: In Brief*, Congressional Research Service Report R43955, March 27, 2015.

¹⁶ 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). I 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.

¹⁷ <http://www.lawfareblog.com/2015/03/what-we-must-do-about-cyber/>

II. WHAT IS DETERRENCE?

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.¹⁸ During the Cold War, deterrence was the dominant approach 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 the concept. 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.¹⁹

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 new security challenges in a range of contexts.²⁰

But as deterrence has been revived as an increasingly central component of American security strategy,²¹ it has evolved from its Cold War focus on "deterrence by punishment," in which adversaries are deterred by the credible threat of imposing unacceptably high costs unless they change their behavior. Instead, deterrence thinking has evolved, focusing more on "deterrence by denial," in which an adversary is deterred by the deployment of defensive measures that make a successful attack less likely, and on deterrence strategies specifically tailored to the threats a defender is most likely to encounter.²² In the counterterrorism context, for example, scholars have focused on disaggregating terrorist networks, and tailoring strategies to each component of those networks designed to shape the cost/benefit calculations of specific actors in the terrorism ecosystem (e.g. financiers, facilitators, recruiters, suicide bombers).²³

¹⁸ 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).

¹⁹ THE WHITE HOUSE, *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").

²⁰ See generally, Richard K. Betts, "The Lost Logic of Deterrence," *Foreign Affairs*, Vol. 92 No. 2 (March/April 2013).

²¹ Suzanne Nossel, *Obama Needs to Find His Inner Cold Warrior*, *FOREIGN POLICY*, June 25, 2014, available at http://www.foreignpolicy.com/articles/2014/06/25/obama_needs_to_find_his_inner_warmonger_iraq_syria_deterrence; Craig Cohen and Josiane Gabel eds., 2015 *GLOBAL FORECAST: CRISIS AND OPPORTUNITY*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (Nov. 2014) ("In the coming year, deterrence will be an aspect of virtually all of our security dealings.").

²² John Gearson, "Deterring Conventional Terrorism: From Punishment to Denial and Resilience," *Contemporary Security Policy* Vol. 33 No. 1 (2012), 171-198.

²³ Paul K. Davis & Brian Michael Jenkins, *Deterrence & Influence in Counterterrorism: A Component in the War on al Qaeda* (Santa Monica, CA: 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.²⁴ Cutting-edge research on deterrence today also has focused on how to manage the threat posed by regional nuclear powers,²⁵ and even questions about the continued efficacy of the U.S. nuclear force,²⁶ among other issues.

Deterring financially-motivated cybercrime will rely primarily on variations of the traditional understanding of “deterrence by denial.” In the realm of financially-motivated cyber crime, “dissuasion by denial” has a particularly high degree of salience, 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.”²⁷ This approach differs from the more common approach to deterrence, “deterrence by punishment.”

In emphasizing deterrence or dissuasion by denial, the approach herein is both more specifically tailored to the context of cyber crime, and has the virtue of eliding two problems that have vexed the application of traditional deterrence theory to cyberspace: attribution; and challenges attendant with effectively communicating threats in cyberspace derived from the secrecy with which the U.S. and other governments have treated their cyber capabilities.

a. What the cyber deterrence discussion has focused on to this point

The adaptation of traditional understandings of deterrence to cyberspace can be characterized along two axes: The first axis is the type of influence strategy cyber deterrence scholarship has deployed. As mentioned above, the discussion about cyber deterrence thus far generally has focused on *deterrence by punishment*, rather than deterrence by denial or deterrence by dissuasion.²⁸ The second axis focuses on the context in which scholars and practitioners have attempted to develop deterrence strategies. In this regard, the deterrence community largely has focused on deterrence in the context of cyberwar, and on deterring attacks against critical infrastructure.

The deterrence of financially motivated cyber crime differs along both axes. It addresses the deterrence of a different form of activity, namely theft motivated by a quest for profit, rather than disruption motivated by reasons of state. And it does so by denying attackers the anticipated benefits of their activities, rather than threatening attackers with unacceptable punishment.

b. Deterrence of Asymmetric and Distributed Threats

²⁴ Alex S. Wilner, “Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism,” *Journal of Strategic Studies*, Vol. 34, No. 1 (February 2011), 3-37; Andreas Wenger, et al., eds., *Deterring Terrorism: Theory and Practice* (Stanford, CA: Stanford University Press, 2012).

²⁵ VIPIN NARANG, NUCLEAR STRATEGY IN THE MODERN ERA: REGIONAL POWERS AND INTERNATIONAL CONFLICT (2014).

²⁶ Keir A. Lieber and Darryl G. Press, “The New Era of Nuclear Weapons, Deterrence, and Conflict,” *Strategic Studies Quarterly*, Vol. 7 no. 1 (Spring 2013).

²⁷ Paul Davis, *Deterrence, Influence, Cyber Attack, and Cyberwar*, 47 NYU J. INT’L L. & POLS. 327, 333 (2015).

²⁸ Indeed, this is the main focus of the leading text on cyberdeterrence: Libicki, *Cyberdeterrence and Cyberwar*, at 7-8.

III. FINANCIALLY-MOTIVATED CYBERCRIME

Cybercrime motivated by the quest for profit predominates over other motivations for cyber attacks.²⁹ Indeed, “cybercrime is no longer an individual ego driven phenomena, instead it is now organized and profit driven.”³⁰ Data stolen by organized cyber crime 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 can include information like credit card data, account information (e.g. from eCommerce, social media, or banking sites), email logins and passwords, fake ATM cards, and other similar records, black markets for which “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.”³¹

Recent attention also has focused on novel financially-motivated cyberattacks, such as the theft of personally identifiable information in order to fraudulently file tax returns and reap refunds, which one noted security researcher called a “\$6 billion-a-year problem.”³² In response to reports about rampant cyber-enabled tax fraud, IRS Commissioner John Koskinen was quoted as saying that the perpetrators are “organized crime syndicates that not only we but everybody in the financial industry are dealing with.”³³

In contrast to records, which can be fungible and for which a robust black market exists, IP is both non-fungible,³⁴ and “harder to put a value on because it can be so unique, and generally requires a specific buyer.”³⁵ Trade secrets, which can include litigation positions, proposed corporate finance activities, and similarly sensitive corporate plans, also are targets that can be difficult to value. This kind of sensitive data is often targeted by nation-states, “the theft of which many organizations are reluctant to report—if, in fact, they are aware this information has been stolen. Often there is no legal or regulatory requirement to do so, and the consequences of disclosing IP loss may, in some cases, cripple a business.”³⁶ Moreover, there is variation in the ways that such data is stolen, with responsibility distributed between insiders (mostly employees) and outsiders (mostly criminally-linked).³⁷ According to one authoritative private sector source, financial motivations still drive the majority of cyber incidents,³⁸ while the cost of breaches continue to rise as well (though there is substantial variation in the cost of a data breach depending on where it takes place and the industry in which the affected company operates).³⁹

²⁹ 2014 VERIZON DATA BREACH REPORT, at 9.

³⁰ Afroz, S., Garg, V., McCoy, D., Greenstadt, R.: Honor among thieves: A commons analysis of cybercrime economies. In: eCrime Researcher’s Summit. APWG, IEEE (2013), at 1.

³¹ MARKETS FOR CYBERCRIME TOOLS, at 10-11.

³² Brian Krebs, *States Seek Better Mousetrap to Stop Tax Refund Fraud*, KREBS ON SECURITY BLOG (Jun. 2, 2015 2:20 a.m.), <http://krebsonsecurity.com/2015/06/states-seek-better-mousetrap-to-stop-tax-refund-fraud>.

³³ Jada F. Smith, *Cyberattack Exposes I.R.S. Tax Returns*, N.Y. TIMES, May 26, 2015.

³⁴ MARKETS FOR CYBERCRIME TOOLS, at xi.

³⁵ *Id.*, at 15.

³⁶ PRICE WATERHOUSE COOPERS, U.S. CYBERCRIME: RISING RISKS, REDUCED READINESS 9 (2014).

³⁷ ERNST & YOUNG, GET AHEAD OF CYBERCRIME: EY’S GLOBAL INFORMATION SECURITY SURVEY 2014 3 (2014).

³⁸ 2014 VERIZON DATA BREACH REPORT, at 9.

³⁹ PONEMON INSTITUTE, 2015 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 1-3 (2015).

Reducing this activity is a significant priority for the United States government and the governments of its allies. But strategies to deter financially motivated cyber crime must be shaped to the specific reasons that parties engage in it. The costs of cyber crime must be increased, and the anticipated benefits must be reduced through regulatory measures designed to dry up the market for stolen data, and to make the conduct of cyber crime itself more costly.

Notably, the paradigm presented below is applicable to a broad range of actors, and acknowledges that financially motivated cybercrime may be committed by state or non-state actors, using a wide range of attack methodologies. Indeed, it is possible (and in some cases probable) that the same group of hackers may conduct different kinds of cyberattacks for many different reasons.⁴⁰ The critical factor, then, in deterring different types of cyber intrusion is to identify the motives behind any particular attack or category of illicit activity, and to develop strategies to address those particular motivations. The importance of curtailing this type of activity, therefore, does not diminish the importance of deterring attacks against critical infrastructure or military capabilities; it only recognizes that the tools necessary to do so will differ.

IV. DETERRING FINANCIALLY-MOTIVATED CYBERCRIME

a. Drying up the Market for Stolen Data: Financial Sanctions

i. Financial Sanctions

Financial sanctions are a tool of risk management, not a tool designed to achieve decisive outcomes. They are (at least as practiced in the United States) regulatory measures that impose obligations on financial institutions and other covered parties to refrain from certain kinds of business, or business with certain counterparties. In doing so, they bar those designated persons from the formal financial system.

Financial sanctions are generally imposed to frustrate or contain threats, or to engineer a change in behavior. In the counterterrorism context, for example, by “marshaling the support of the domestic and international private sectors, multilateral fora, foreign regulators, and foreign ministries, [the U.S. government] made it harder than ever for terrorists to raise, move, store, and use funds.”⁴¹ And in the context of international negotiations about the Iranian nuclear program, financial sanctions are widely credited with generating the leverage needed to bring the Iranian government to the negotiating table with the P5+1.

The effectiveness 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, most significant international commercial transactions,

⁴⁰ See, e.g., 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 in “political, economic, and military-related intelligence,” including the theft of valuable intellectual property from Western corporations).

⁴¹ David S. Cohen, Under Secretary for Terrorism and Financial Intelligence, “Confronting New Threats in Terrorist Financing” (Center for a New American Security, Washington, March 4, 2014), <http://www.treasury.gov/press-center/press-releases/Pages/jl2308.aspx>.

including the global energy trade, are denominated in U.S. dollars, which means that almost all financial transactions of consequence become subject to U.S. jurisdiction when they are cleared by banks in the United States. Moreover, most significant international financial institutions, whether or not they are formally subject to U.S. jurisdiction, bar transactions with persons designed by the U.S. Department of the Treasury. They do so because they are wary of the reputational risk involved in potentially processing transactions on behalf of designated persons, and of transgressing their legal obligations, even inadvertently.

This means that once natural or legal persons are designated under the new cybersecurity sanctions program, they will become toxic to financial institutions around the world.⁴²

Two characteristics of financial sanctions provide them with a comparative advantage over other means of controlling financially-motivated cybercrime: first, their characterization as preventive regulatory measures means that any judicial review of sanctions determinations is undertaken with substantial deference to the determinations of the executive branch; and second, the administrative record compiled to support the imposition of financial sanctions, and any future judicial review of those determinations, can rely in part on classified information. The latter is particularly important with respect to sanctions for cybercrime, where information tending to establish attribution of particular attacks is likely to rely at least partially on classified information.

The fact that the imposition of sanctions is an administrative action means that the evidentiary showing required is different than that needed for criminal prosecutions, commensurate with the understanding of sanctions as regulatory measures designed to protect the financial system, rather than acts intended to punish.⁴³ Financial sanctions go into effect after the Secretary of the Treasury makes a determination with respect to a person or entity, in consultation with the Attorney General and the Secretary of State, based on the compilation of an administrative record that describes the facts demonstrating that the legal criteria for designation have been met. The imposition of financial sanctions is treated as an agency determination subject to review under the Administrative Procedures Act (APA), and will be set aside if it is found by a reviewing court to be “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.”⁴⁴ A “highly deferential review applies to examination of a [sanctions] designation.”⁴⁵

⁴² 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.” David S. Cohen, “The Law and Policy of Iran Sanctions,” Remarks of Under Secretary for Terrorism and Financial Intelligence David Cohen before the New York University School of Law (Sept. 12, 2012), available at <http://www.treasury.gov/press-center/press-releases/Pages/tg1706.aspx>

⁴³ *But see*, Cian Murphy, EU COUNTER-TERRORISM LAW: PRE-EMPTION AND THE RULE OF LAW (2012) (arguing that the understanding of financial sanctions as preventive regulatory measures inappropriately privileges the executive and comes at a substantial cost to the due process rights of designated persons).

⁴⁴ 5 U.S.C.A. § 706(2)(A).

⁴⁵ *Kadi v. Geithner*, 42 F.Supp.3d 1, 10 (D.D.C. Mar. 19, 2012) (internal citations and quotation marks omitted).

This means that sanctions can be imposed in the range of cases in which the government cannot declassify sufficient information to meet the evidentiary burden necessary for a criminal prosecution, but for which there is substantial intelligence pointing to a particular bad actor. For information that cannot be declassified, the International Emergency Economic Powers Act (IEEPA), the statutory authority for the new cybersecurity sanctions program, permits the government to rely on classified information in its administrative record, and provides the authority for courts standing in review of sanctions determinations to rely on *in camera* examinations of classified portions of the administrative record.⁴⁶ Indeed, in a recent high-profile case reviewing the imposition of financial sanctions, the court made its determination that there was “substantial evidence” to support OFAC’s determination to impose sanctions on Yassin al-Kadi based on its review of both classified and unclassified materials.⁴⁷

Even still, the government “endeavor[s] with each and every designation to go out with a public press release that outlines the reason we’re taking the action,” which depends in part on declassified information.⁴⁸ This is designed to meet both due process obligations, and to provide at least some information to the public about the illicit conduct that the sanctioned person is engaged in.

ii. Cyber Sanctions

“Profit drives modern cybercrime ... [and] scammers relentlessly innovate to identify more lucrative niches to maximize their returns (e.g., counterfeit goods, fake anti-virus, ransomware, credit card theft, cryptocurrency mining, etc.).”⁴⁹ The key to deterring financially-motivated cybercrime, therefore, is to lower the expected returns, to or raise the cost of pursuing those returns, to the point where cybercrime can be reduced.

The new cybersecurity sanctions program is an effort to do just that. The program emerged in a context in which financial sanctions have achieved important national security objectives over the last several years, while the government continues to struggle in its attempt to stem the cybercrime threat. Over the last several years, various legislative proposals designed to address specific cybersecurity problems (like removing obstacles to information-sharing) have failed. And while the Obama administration has adopted several executive orders addressing different components of the cybersecurity problem, the administration felt 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.”⁵⁰

⁴⁶ 50 U.S.C. §1702(c).

⁴⁷ *Kadi v. Geithner*, supra note 36, at 24.

⁴⁸ 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,” April 1, 2015, <https://www.whitehouse.gov/the-press-office/2015/04/01/record-press-call-president-s-executive-order-blocking-property-certain->

⁴⁹ Paul Pearce et al., *Characterizing Large-Scale Click Fraud in ZeroAccess*, 2014 PROC. OF THE 2014 ACM SIGSAC CONF. ON COMPUTER & COMM. Security 141 (hereinafter, “*Click Fraud in ZeroAccess*”).

⁵⁰ 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>

The following sections will analyze ways in which this new capability, and other related regulatory tools, can be used to deter financially motivated cyber crime.

iii. Potential kinds of sanctions targets and differential deterrent effects

1. Beneficiaries of economically-motivated cybercrime

The most innovative provision of the executive order structuring the new cybersecurity sanctions program permits it to target persons determined “to be responsible for or complicit in, or to have engaged in, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of trade secrets misappropriated through cyber-enabled means.” The EO further requires that any person designated under that authority have received or used trade secrets “knowing they have been misappropriated,” and that the misappropriation is reasonably likely to result in or has materially contributed to a significant threat to American interests.⁵¹

This provision of the cyber EO 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.”⁵² 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 well as user account data, after “a highly sophisticated and targeted attack on our corporate infrastructure originating from China”;⁵³ 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;”⁵⁴ 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.⁵⁵

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 receive or use stolen intellectual property knowing that it has been misappropriated can be used to deprive them of the benefits of their hard-stolen information. This is because companies sanctioned under the order will be largely cut out of the international financial system. They will have any property or interests in property in the United States or under the control of a U.S. person blocked, and will have any transactions with U.S. persons prohibited. 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.

⁵¹ EO 13694, at §1(a)(ii)(A).

⁵² Josh Rogin, *NSA Chief: Cybercrime Constitutes the “Greatest Transfer of Wealth in History,”* FOREIGN POLICY, July 9, 2012, available at <http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/>

⁵³ David Drummond, *A New Approach to China*, GOOGLE OFFICIAL BLOG (Jan. 12, 2010), <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>

⁵⁴ Stephanie Yang and 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>

⁵⁵ SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX xii-xviii (2014).

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 (even though none of the five defendants has 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 cyber crime. It also might be beneficial in some future instance to designate the companies that benefitted from cyber crime at the same time as the Department of Justice prosecutes the individuals that committed the thefts (the companies that benefited from the cyber crime described in the indictment were not named). The combination of sanctions against companies benefitting from cyber crime 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 do so at all.⁵⁶

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).⁵⁷ The theft included trade secrets, such as pricing information that allowed companies to underbid U.S. competitors;⁵⁸ sensitive, internal communications "that would provide a competitor, or adversary in litigation, with insight into the strategy and vulnerabilities of the American entity";⁵⁹ 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.⁶⁰ The theft of this sensitive or proprietary information generated the potential for significant commercial advantage to the recipients of the information.

This information was provided to Chinese companies in circumstances suggesting they knew about—or potentially even 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 state-owned enterprise "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.'"⁶¹ If the Chinese SOEs described in the indictment did in fact direct the theft at issue, they would 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

⁵⁶ See, e.g., Press Release, U.S. Department of Justice, Russian Hacker Arrested for Computer Hacking Scheme that Victimized Thousands of Credit Card Customers (July 7, 2014) (available at <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.

⁵⁷ 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. filed May 1, 2014).

⁵⁸ Indictment, *US v. Wang Dong*, at 2.

⁵⁹ *Id.*, at 2-3.

⁶⁰ *Id.*, at 4.

⁶¹ *Id.*, at 3.

effectively excise them from the international financial system, rendering their exercise in misappropriation worthless.⁶²

By sanctioning the companies responsible for the activity at issue in the case, the cost to them of engaging in (or knowingly benefiting from) cyber crime can become very high, indeed. A cost that will be more pronounced because until this point, the beneficiaries of cyber crime have paid very little price at all.

Beyond this case, there is likely to be a far larger universe of companies as to whom intelligence exists about their use of stolen intellectual property, but about whom that intelligence cannot be declassified in sufficient quantity to bring a prosecution. It is this universe of cases that might be opportune targets for financial sanctions, in order to achieve whatever deterrent effects are possible without compromising the ability to prosecute criminally if that option is viable.

2. Perpetrators of economically-motivated cybercrime

The cybersecurity sanctions program also contains the authority to impose financial restrictions in more traditional circumstances, namely on those specific persons or entities determined to be “responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities” that pose a significant threat to American interests.⁶³ This component of 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 require to move and use ill-gotten funds). In this respect, the program resembles the design of other financial sanctions programs that freeze the assets of specific persons determined to be engaged in the proscribed activity governed by the executive order at issue. This portion of the new program achieves a deterrent effect by adding another way (beyond arrest) in which the perpetrators of cybercrime can have their activities disrupted. This raises the risk to them of engaging in illicit cyber activity and lowers the anticipated benefit.

iv. Impact of Shutting Down Cybercrime Nodes

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

In addition to sanctions that diminish the expected value of cyber crime to deter its commission, innovative public/private partnerships have emerged in the last several years that can raise the cost of cyber crime 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

⁶² 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.

⁶³ EO 13694, at §1(a)(i).

particular—partnerships to take down botnets—deserves analysis because botnets are an important tool for the perpetration of many forms of financially-motivated cybercrime.⁶⁴

Regulatory interventions that make it easier to take down botnets make it costlier to use them to perpetrate cyber crime, 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.”⁶⁵ Botnets can be operated by a small number of “command and control” servers, or in a peer-to-peer fashion that can be more difficult to mitigate.

Botnets can be used to generate spam, commit click-fraud, steal information, or conduct other kinds of financial crime, including fraudulently mine Bitcoins.⁶⁶ As the instrumentality through which substantial amounts of cybercrime takes place, increasing the legal and regulatory options available to disrupt botnets will increase the likelihood that any given botnet will be taken down, raising the potential cost of criminal activities. While botnets might at this point be commodity items, which are widely available and can even be rented,⁶⁷ the key point in this discussion is to 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 the aggregate, raise the cost and risk of illicit cyber activity.

The ZeroAccess botnet was one of the largest botnets in operation, which delivered a wide range of malware, but which 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.”⁶⁸ Security researchers estimated that ZeroAccess led to losses of \$2.7 million per month for advertisers.⁶⁹

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

⁶⁴ 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 and Julian E. Barnes, *Iran Blamed for Cyberattacks*, WASH. POST, Oct. 12, 2012.

⁶⁵ Complaint, *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), at 11 (hereinafter “ZeroAccess Complaint”).

⁶⁶ Danny Yuxing Huang et al., *Botcoin: Monetizing Stolen Cycles*, 2014 PROC. OF THE NETWORK AND DISTRIBUTED SYS. SECURITY SYMPOSIUM 1, available at <http://cseweb.ucsd.edu/~snoeren/papers/botcoin-ndss14.pdf>.

⁶⁷ Tim G., *Renting a Zombie Farm: Botnets and the Hacker Economy*, SYMANTEC OFFICIAL BLOG (Aug. 8, 2014), available at <http://www.symantec.com/connect/blogs/renting-zombie-farm-botnets-and-hacker-economy>

⁶⁸ *ZeroAccess Complaint*, at 10.

⁶⁹ Pearce, *Click Fraud in ZeroAccess*, at 142.

servers involved in fraudulent activity.⁷⁰ 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, and made changes to, Windows operating systems, search engines, and web browsers that Microsoft had licensed to individual computer users whose machines had been compromised and incorporated into the botnet.⁷¹ Microsoft also alleged claims under the Lanham Act (as well as common law theories) that the reduced performance and fraud that were a result of the botnet's operation caused "injury to Microsoft's brand, reputation and goodwill."⁷²

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 domain names that controlled the botnet.⁷³ The intention of the order was to sever communications between the command and control nodes of the botnet, and the infected computers themselves.

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 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."⁷⁴ Several months later the authors of the malware had revived the botnet, but did so with some of the functionality removed.⁷⁵

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 botnet was a sophisticated scheme that stole banking credentials and resulted in an estimated \$100 million in losses.⁷⁶ 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."⁷⁷ 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

⁷⁰ Press Release, Europol, Notorious Botnet Infecting 2 Million Computers Disrupted, available at <https://www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted>

⁷¹ *ZeroAccess Complaint*, at 15-18.

⁷² *Id.*, at 18, 20-26.

⁷³ *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.

⁷⁴ Pearce, *Click Fraud in ZeroAccess*, at 144.

⁷⁵ *Id.*

⁷⁶ Press Release, U.S. Department 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>)

⁷⁷ *Id.*

damage” to legitimate web traffic that might make use of the same or linked facilities.⁷⁸ Criticisms can also be levied about the effectiveness of such activities. But in this general approach, there is a method to gradually and systematically raise the cost of financially motivated cybercrime. Reform projects aimed at easing the path to botnet takedowns, like recently proposed amendments to Federal Rule of Criminal Procedure 41 and other proposals made by the Department of Justice,⁷⁹ should be adopted.

V. 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 cyber capabilities have been treated, and the problem of accurately determining with confidence the actual identity of the perpetrators of an attack. While these problems are still present in the discussion about cyber sanctions, the use of generally available regulatory measures, as opposed to specifically-imposed retaliatory actions, elides some of the difficulties that secrecy and the attribution problem have posed to the development of effective cyber deterrence strategies to this point.

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 potential target to a potential challenger. In this sense, 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.”⁸⁰

The secrecy with which cyber capabilities have been treated 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.⁸¹ Because most states have regarded their cyber capabilities as secrets of the highest order, establishing the kinds of clear statements of intent required to influence adversaries has proven challenging.⁸² Indeed, “Under the logic of deterrence, conveying some information to the challenger with great clarity, especially about one’s military capabilities, is beneficial.”⁸³

⁷⁸ See, e.g., Brian Krebs, *Microsoft Darkens 4MM Sites in Malware Fight*, Krebs on Security (Jul. 14, 2014) (available at <http://krebsonsecurity.com/2014/07/microsoft-darkens-4mm-sites-in-malware-fight/comment-page-1/>).

⁷⁹ *Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks: Hearing of the Subcomm. On Crime and Terrorism of the S. Comm. On the Judiciary*, 113th Cong. (Jul. 15, 2014) (statement of Leslie Caldwell, Assistant Attorney General for the Criminal Division, U.S. Department of Justice).

⁸⁰ MORGAN, *DETERRENCE NOW*, at 15.

⁸¹ T.V. Paul, introduction to *Complex Deterrence: Strategy in the Global Age*, ed. T.V. Paul et al., (Chicago, IL: University of Chicago Press, 2009), 2.

⁸² Austin Long, *Deterrence: The State of the Field*, 47 NYU J. INT’L L. & POLS 357, 374-376 (2015).

⁸³ MORGAN, *DETERRENCE NOW*, at 17.

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.”⁸⁴

An approach to deterring cybercrime that relies on regulatory measures to deprive criminals of the benefits they anticipate with their theft avoids this problem. It does so by focusing not on imposing punishment on particular actors, but rather by threatening to impose sanctions on persons (natural or legal) that engage in cyber theft, or on companies that knowingly benefit from malicious digital crime.

It therefore relies less on technical capabilities (though there is an important place for such capabilities, as highlighted in the discussion of attribution below) and more on an approach to deterrence that focuses on holding assets at risk about which cyber criminals care—namely, their hard-stolen data. This form of “manipulation of risk,” is slightly different from the way in which Thomas Schelling conceived of the manipulation of risk in the context of deterring Cold War threats.⁸⁵ There, deterrence originates in the risk that limited actions on the part of a challenger will escalate for reasons that are outside his control.

In using financial sanctions to deter financially motivated cyber crime, the U.S. government similarly is holding at risk assets that perpetrators care about. But it does so by offering a credible threat to render worthless a cyber criminal’s investment in stolen assets. What will matter here, therefore, is the regular demonstration of the threat to sanction persons that either engage in or benefit from significant malicious cyber activities. This, in turn, will require the political will to impose sanctions in a range of circumstances and against a range of targets in order to demonstrate the costs of cybercrime to a range of potential perpetrators.

b. Attribution

“Doing attribution well is at the core of virtually all forms of coercion and deterrence.”⁸⁶ This is because deterrence is fundamentally about communication; and one cannot tailor a deterrent message appropriately if one does not know with confidence who the recipient should be. With a strategy of deterrence dependent on imposing punishment, moreover, 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.⁸⁷

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.”⁸⁸

⁸⁴ 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).

⁸⁵ THOMAS SCHELLING, *ARMS AND INFLUENCE* 92-109 (2008 ed.).

⁸⁶ Thomas Rid and Ben Buchanan, *Attributing Cyber Attacks*, J. STRATEGIC STUDIES, Vol. 38 Nos. 1-2 (2015), at 4.

⁸⁷ See, the discussion in Libicki, *Cyberdeterrence and Cyberwar*, at 41-52.

⁸⁸ 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,” April 1, 2015, <https://www.whitehouse.gov/the-press-office/2015/04/01/record-press-call-president-s-executive->

Indeed, the scope of the challenge became clear in early 2015 when the F.B.I. and the intelligence community were forced 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.⁸⁹

An approach to deterring financially-motivated cyber crime 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 the U.S. government must have confidence that it understands who is responsible for perpetrating a given act of cyber theft (or for receiving misappropriated data). But if sanctions are imposed and botnets taken down with sufficient regularity, cybercriminals contemplating cyber crime 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."⁹⁰ 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."⁹¹ 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").⁹²

The sanctions and other interventions described above lower the stakes involved in the attribution discussion in two ways. First, they are principally directed at natural and legal persons, rather than at nation-states per se (complicating factors include individuals or entities, such as the five Chinese military officers indicted last year, linked to states). It is common for individuals and entities to be prosecuted and subject to sanctions in a range of different contexts, so targets may be selected in such a way as to guard against inadvertent escalation. Second, once used a sufficient number of times, financial sanctions and regulatory interventions raise the general risk that misappropriated assets in which cyber thieves have invested will be rendered worthless, diminishing their 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, and diminish the need to impose sanctions frequently over time.

[order-blocking-property-certain](#); see also, Leon Panetta, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City (Oct. 11, 2012) (available at <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>) ("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.")

⁸⁹ Ellen Nakashima, *FBI director offers new evidence to back claim North Korea hacked Sony*, WASH. POST, Jan. 7, 2015.

⁹⁰ Rid and Buchanan, *Attributing Cyber Attacks*, at 7.

⁹¹ *Id.*, at 30.

⁹² *Id.*, at 10.

Furthermore, the U.S. government has demonstrated on several occasions that it is capable of making public attribution information regarding the digital theft of intellectual property. This is most often in the context of criminal prosecutions, which require a higher evidentiary burden than the imposition of financial sanctions.⁹³ And, while the government has not yet (to the public's knowledge) made a decision to retaliate kinetically or in cyberspace against a cyberattack, the government has publicly 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 has 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 "Hackers working for the Chinese state."⁹⁴

In addition to the nation-state linked attributions just described, the government regularly prosecutes data breaches and cyber crime cases that are not linked to nation states. While the stakes in these cases (invoking Rid's taxonomy) are lower, they nonetheless still require the attribution of specific attacks to specific individuals with a high degree of confidence.⁹⁵

The sources of information that support the imposition of financial sanctions also enhance the ability of the government to attribute with confidence. One source of data will include 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 both in the compilation of the administrative record that supports a sanctions designation, and in any litigation that might follow from the imposition of sanctions, it can combine technical attribution data with any available HUMINT or SIGINT reporting to increase its level of confidence in the decision.

Conversely, 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.

The attribution problem in cyberspace is inescapable, but it need not paralyze. As with any government intervention, there are tradeoffs to be made both between various options for pursuing difficult cases—should the government prosecute a particular offender, or impose sanctions; should it engage diplomatically, or retaliate through intelligence means? And at a higher level of abstraction, there always will be difficult questions to weigh about the risks of inadvertently escalating situations. But the government has demonstrated its ability to 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

⁹³ See, Indictment, *United States v. Pang et al.*, no. Cr-15-00106-EJD (N.D.Ca. filed Apr. 1, 2015).

⁹⁴ Ellen Nakashima, *Chinese breach data of 4 million federal workers*, WASH. POST, June 4, 2015.

⁹⁵ See, e.g., the following recent indictments for cases where the Department of Justice is prosecuting individuals for hacking-related crimes: Indictment, *United States v. Nasenkov et al.*, No. 1:09 CR 01093, 2013 WL 3884139, (S.D.N.Y. filed 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. filed Apr. 25, 2013).

large global media companies. There is no reason to expect that the attribution issue will be more vexatious in the context of financial sanctions.

VI. ADDITIONAL CONSIDERATIONS

- a. A High Standard for Sanctions**
- b. Controlling Escalation and Retribution**

VII. CONCLUSION