U.C.L.A. Law Review

Privatizing Cybersecurity

Nathan Alexander Sales

ABSTRACT

In an earlier work entitled *Regulating Cybersecurity*, I argued that cyber defense should be understood not just as a matter for law enforcement and the armed forces, but as a regulatory problem in need of regulatory solutions. This companion article proposes a series of market-based responses to complement those governmental responses. It argues that hackers and other private actors are an important source of cybersecurity data—especially information about vulnerabilities and how to exploit them. Yet the white market, in which researchers can sell bugs to vendors that will patch them, suffers from high transaction costs, low prices, and other imperfections. Many hackers therefore choose to sell on the gray market to military and intelligence agencies that will exploit the flaws, which means that vulnerabilities persist and users remain exposed to attacks by hostile powers that have found the same flaws. The solution, I argue, is twofold: fostering white market brokers to reduce the transaction costs of legitimate bug sales, and increasing the payouts offered on the white market through a combination of liability protections, tax benefits, and subsidies.

AUTHORS

This Article was written and accepted for publication when the author was Associate Professor of Law, Syracuse University College of Law. The views expressed in this Article are those of the author and not necessarily those of the U.S. Government. Thanks to Derek Bambauer, Joel Brenner, Mary DeRosa, Mailyn Fidler, Andreas Kuehn, Peter Margulies, Andrea Matwyshyn, Greg Nojeim, Paul Rosenzweig, and Michael Schmitt for their helpful comments. I'm also grateful to participants in a workshop cosponsored by Syracuse University's Institute for National Security and Counterterrorism and the NATO Cooperative Cyber Defence Centre of Excellence.

65 UCLA L. Rev. 620 (2018)

TABLE OF CONTENTS

INTRODUCTION

The FBI had a problem.

On December 2, 2015, two gunmen wearing black ski masks and tactical gear had opened fire at a Christmas party for county employees in San Bernardino, California. Armed with AR-15 assault rifles and 9mm pistols, the pair had methodically sprayed the first-floor conference room where the workers had gathered with bullets, killing fourteen people and injuring twenty-one others.[1] It was the deadliest mass shooting the country had seen since the Sandy Hook massacre in 2012.[2]

The attackers—Chicago-born Syed Rizwan Farook and his wife Tashfeen Malik, a recent immigrant from Pakistan by way of Saudi Arabia—were gunned down hours later in a shootout with police, but not before Tashfeen posted on Facebook a bayat, or loyalty oath, to the Islamic State, the self-proclaimed caliphate that controlled huge swaths of territory in Syria and Iraq.[3] Within days, ISIS, which had carried out a horrific series of attacks in Paris the month before, issued a statement lauding the pair as "soldiers of the caliphate."[4] And investigators discovered that Tashfeen had used her Facebook account to send messages "pledging her support for Islamic jihad and saying she hoped to join the fight one day."[5]

Now the FBI needed to find out if the husband and wife had been in contact with terrorists overseas. Were they ISIS operatives, dispatched by the

[1] Rong-Gong Lin II & Richard Winton, *San Bernardino Suspects 'Sprayed the Room With Bullets,' Police Chief Says*, L.A. TIMES (Dec. 4, 2015, 3:06 AM), http://www.latimes.com/ local/lanow/la-me-ln-san-bernardino-suspects-sprayed-the-room-with-bullets-20151203-story.html [https://perma.cc/E6X8-CGDR]; Eli Saslow & Stephanie McCrummen, *'Where's Syed?': How the San Bernardino Shooting Unfolded*, WASH. POST (Dec. 3, 2015), https://www.washingtonpost.com/ national/wheres-syed-how-the-san-bernardino-shootingunfolded/2015/12/03/2ee90128-9a15-11e5-8917-653b65c809eb_story.html [https://perma.cc/N8XC-Q5K2].

[2] *See* Mark Berman et al., *At Least 14 People Killed, 17 Injured in Mass Shooting in San Bernardino, Calif.; Two Suspects Killed in Shootout With Police*, WASH. POST (Dec. 2, 2015), https://www.washingtonpost.com/news/post-nation/wp/2015/12/02/police-in-san-bernadino-calif-responding-report-of-shooting/ [https://perma.cc/Y6BE-628A].

[3] *See* Rukmini Callimachi, *Islamic State Says 'Soldiers of Caliphate' Attacked in San Bernardino*, N.Y. TIMES (Dec. 5, 2015), https://www.nytimes.com/2015/12/06/world/ middleeast/islamic-state-san-bernardino-massacre.html.

[4] *Id.*

[5] Richard A. Serrano, *Tashfeen Malik Messaged Facebook Friends About Her Support for Jihad*, L.A. TIMES (Dec. 14, 2015, 5:41 PM), http://www.latimes.com/local/lanow/la-me-ln-malik-facebook-messages-jihad-20151214-story.html [https://perma.cc/MUE2-6S9L].

same masterminds who had spilled so much blood in Paris? Or were they lone wolves who'd concocted their murderous scheme on their own?

One obvious lead was Syed's iPhone. The owner of the device—Syed's employer, the same county office he'd shot up—was fine with the Bureau inspecting it.[6] But the phone was locked and the data on it encrypted. Agents could attempt a brute force attack, entering random four-digit passcodes until they eventually found the right one. But the iPhone had a self-destruct mechanism of sorts; ten incorrect tries and it would wipe itself clean.[7] The FBI approached Apple but it refused to help unlock the device.[8] A federal magistrate judge in California ordered the company to write new code that would bypass the phone's security features, but Apple was vowing to resist, and a judge in Brooklyn had sided with the tech giant in a similar dispute.[9] The FBI's next move was to, as Director James Comey put it, "'engage[] all parts of the U.S. government' to ask 'does anybody have a way, short of asking Apple to do it,' to unlock Farook's phone." The response was unequivocal: "'[W]e do not.'"[10] The technological and legal challenges seemed insurmountable.

So the Bureau hired some hackers.

The details remain murky, but it appears the hackers found a way to disable the iPhone's auto-erase function.[11] In cyber parlance, they developed an exploit to take advantage of a previously unknown vulnerability. On March 28, 2016, government lawyers filed a terse pleading in the California case announcing that they had "successfully accessed the data" on Syed's device and

[6] *See* Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html [https://perma.cc/S357-VXU9].

[7] *See id.*

[8] *See id.*

[9] Eric Lichtblau & Joseph Goldstein, *Justice Dept. Appeals Ruling in Apple iPhone Case in Brooklyn*, N.Y. TIMES (Mar. 7, 2016), https://www.nytimes.com/2016/03/08/technology/justice-dept-appeals-ruling-in-apple-iphone-case-in-brooklyn.html.

[10] Ellen Nakashima, *FBI May Not Need Apple to Unlock San Bernardino Shooter's iPhone*, WASH. POST (Mar. 21, 2016), https://www.washingtonpost.com/world/national-security/apple-hearing-in-san-bernardino-over-locked-iphone-has-been-canceled/2016/03/21/1141a56e-efb8-11e5-85a6-2132cf446d0a_story.html [https://perma.cc/65GL-6RAL].

[11] *See* Ellen Nakashima, *FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone*, WASH. POST (Apr. 12, 2016), https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html [https://perma.cc/TR78-ESP2].

no longer needed Apple's help.[12] The phone turned out to have no evidence that the shooters were in touch with ISIS, and investigators concluded that they most likely were self-radicalized free agents who had acted independently.[13] Comey later revealed that the hackers were paid "more than I will make in the remainder of this job, which is seven years and four months, for sure"—at least $1.3 million.[14]

It wasn't the highly capable NSA or some other intelligence agency that cracked the San Bernardino shooter's iPhone. It was private hackers.

In an earlier work entitled *Regulating Cybersecurity*, I argued that cyber defense should be understood not just as a matter for law enforcement and the armed forces, but as a regulatory problem to be addressed with responses drawn from, for example, environmental and antitrust law.[15] This companion article proposes a complementary series of solutions to foster a more robust market for cybersecurity data. It argues that the private sector is a critical source of information about vulnerabilities in software products and how to exploit them. Yet the white market, in which well-intentioned hackers can sell bugs to vendors that will patch them, suffers from a number of distortions. Because fewer sales take place, vulnerabilities persist, and users remain exposed to attacks by criminals, foreign governments, and terrorist organizations that have found the same flaws.

The white market remains underdeveloped for two main reasons. First, bug sales are plagued by high transaction costs. It can be difficult for hackers and vendors to connect with each other and verify their good faith. There are also information asymmetries: Sellers can't persuade vendors to buy unless they demonstrate that their discoveries are legitimate, but that can enable vendors to reverse engineer the bugs, obviating the need to pay. Second, many hackers are biased in favor of offense: They prefer to sell flaws on the gray market to

[12] Matt Zapotosky, *FBI Has Accessed San Bernardino Shooter's Phone Without Apple's Help*, WASH. POST (Mar. 28, 2016), https://www.washingtonpost.com/world/national-security/fbi-has-accessed-san-bernardino-shooters-phone-without-apples-help/2016/03/28/e593a0e2-f52b-11e5-9804-537defcc3cf6_story.html [https://perma.cc/KW2A-ZMEK] (quoting a court filing by federal prosecutors).

[13] *See* Ellen Nakashima & Adam Goldman, *No Links to Foreign Terrorists Found on San Bernardino iPhone So Far, Officials Say*, WASH. POST (Apr. 14, 2016), https://www.washingtonpost.com/world/national-security/no-links-to-foreign-terrorists-found-on-san-bernardino-iphone-so-far-officials-say/2016/04/14/f1aa52ce-0276-11e6-9203-7b8670959b88_story.html [https://perma.cc/D626-ULL8].

[14] Mark Berman & Matt Zapotosky, *The FBI Paid More Than $1 Million to Crack the San Bernardino iPhone*, WASH. POST (Apr. 21, 2016), https://www.washingtonpost.com/news/post-nation/wp/2016/04/21/the-fbi-paid-more-than-1-million-to-crack-the-san-bernardino-iphone/ [https://perma.cc/PD9T-GEQ8].

[15] *See* Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503 (2013).

military and intelligence agencies that will use them in attacks, instead of on the white market to vendors that will fix them. This is so because government buyers pay better than vendors—orders of magnitude better. Selling to the government also carries an implicit assurance of immunity from civil and criminal liability that vendors cannot match. These market imperfections ensure that critical vulnerabilities often go unpatched.

Two concrete steps would strengthen the white market. First, policymakers should establish vulnerability brokers to facilitate sales between buyers and sellers. These intermediaries already exist in the illicit black and shady gray markets but they're largely absent from the white market in part because legitimate sales aren't very lucrative. Brokers would reduce search costs, enable hackers to demonstrate a flaw's severity without destroying its economic value, and redress severe power imbalances between sellers and buyers. Second, policymakers should increase white market payouts, thereby luring researchers away from the shadier corners of the internet. One way to do that would be to offer white hat hackers the same immunity they'd receive if they sold to the government. Policymakers also should exempt from taxation the payments hackers receive from vendors' bug bounty programs, or even supplement them with matching payments. In short, incentives matter. Conventional regulatory solutions must be paired with market-based solutions that can incentivize hackers to sell the bugs they find to vendors that will patch them.

This Article builds on an important literature on vulnerability markets that a group of economists and computer scientists developed in the early 2000s. Although their work has been largely ignored by law reviews,[16] these scholars proposed a variety of innovative solutions such as bug auctions, in which researchers would sell information about flaws they've discovered to software vendors;[17] exploit derivatives, which would enable users to trade contracts that would pay out upon the occurrence or nonoccurrence of a breach;[18] vulnerability credits, where software developers would, as in cap-and-

[16] *But see* Mailyn Fidler, *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis*, 11 I/S: J.L. & POL'Y INFO. SOC'Y 405 (2015); Jay P. Kesan & Carol M. Hayes, *Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities*, 58 ARIZ. L. REV. 753 (2016); Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 NW. U. L. REV. 795, 824 n.146 (2013).

[17] *See* Andy Ozment, Bug Auctions: Vulnerability Markets Reconsidered 7–10 (May 2004) (unpublished manuscript), https://www.dtc.umn.edu/weis2004/ozment.pdf [https://perma.cc/34F7-27XE].

[18] *See* RAINER BÖHME, VULNERABILITY MARKETS: WHAT IS THE ECONOMIC VALUE OF A ZERO-DAY EXPLOIT? 3 (2005), https://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf.

trade schemes for carbon emissions, be assigned an initial allocation of credits for flaws in their products that then could be exchanged;[19] and similar measures.[20] Yet essentially just one market mechanism has been tried: Bug bounties, in which some—but by no means all—vendors pay relatively modest sums to hackers who alert them to flaws in their products. The previous decade's rich theoretical literature has had little impact in the real world; law and policy have lagged far behind theory. This Article tries to correct that deficiency.

To be precise, the proposals that follow are market-inspired or market-based, not pure-market solutions. Many involve government intervention—tax benefits, subsidies, and so on. These nudges are a departure from strict Hayekian orthodoxy, but they seem fitting given the government's contribution to today's market failure. Lavish government payments are systematically distorting the market, and some government prodding is needed as a corrective. The key distinction is not so much between government action and private action, but between regulatory measures and incentive-based ones. The question then becomes, why would officials pursue these reforms when they benefit from the ready availability of bugs on the gray market? Because while some players gain from the status quo (offense-minded agencies like the NSA and CIA), others decidedly do not (DHS and others responsible for defending cyber assets). These entities seemingly would favor bolstering the white market at the expense of the gray.[21] Ditto members of Congress, who would have to enact and fund the measures I'm proposing, as the underdeveloped white market leaves their constituents exposed to attacks.

Finally, a quick note on terminology. A "vulnerability" is a flaw that allows outsiders to gain access to a protected system.[22] A "zero-day" is a flaw that the product's developer doesn't know about and therefore hasn't patched;[23] they take their name from the fact that vendors have "zero days" to

[19] *See* L. Jean Camp & Catherine D. Wolfram, *Pricing Security: A Market in Vulnerabilities*, *in* ECONOMICS OF INFORMATION SECURITY 17, 25–31 (L. Jean Camp & Stephen Lewis eds., 2004).

[20] *See* Mailyn Fidler, Anarchy or Regulation: Controlling the Global Trade in Zero-Day Vulnerabilities 28–32 (May 2014) (unpublished B.A.H. thesis, Stanford University) (on file with Interschool Honors Program in International Security Studies, Center for International Security and Cooperation, Stanford University) (summarizing literature).

[21] *See infra* notes 295–296 and accompanying text.

[22] Rainer Böhme, *A Comparison of Market Approaches to Software Vulnerability Disclosure*, *in* EMERGING TRENDS IN INFORMATION AND COMMUNICATION SECURITY 298, 298 (Günter Müller ed., 2006); Camp & Wolfram, *supra* note 19, at 25.

[23] LILLIAN ABLON ET AL., RAND NAT'L SEC. RESEARCH DIV., MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA: HACKERS' BAZAAR 25 (2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

fix them before malicious hackers can target them.[24] The tools that intruders use to take advantage of zero-days and other flaws are called "exploits."[25] In other words, a vulnerability is mere information, whereas an exploit is a product—software that uses a flaw to attack a system.[26] "Hacker" also needs clarification. Today, the term has largely negative connotations, referring to outlaws or others bent on mischief, but it originally meant no more than a highly skilled computer enthusiast.[27] This Article uses "hacker" in its original, neutral sense, essentially as a synonym of "researcher." When referring to people with more sinister designs, I use "malicious hackers," "attackers," "black hats," and the like.

Part I discusses the private sector's considerable expertise at generating cybersecurity data. Part II describes the current market, as well as the distortions from which it suffers. In Part III, I explain why the regulatory solutions favored by most scholars are unlikely to strengthen the white market or curb the black and gray markets. Part IV describes cybersecurity brokers and other measures that could foster a more robust white market.

[https://perma.cc/E93K-74ZU]; Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1078 (2014); Kesan & Hayes, *supra* note 16, at 788.

[24] Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 482 (2017); Fidler, *supra* note 16, at 408; Joseph Menn, *U.S. Cyberwar Strategy Stokes Fear of Blowback*, REUTERS (May 10, 2013), http://www.reuters.com/article/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510 [https://perma.cc/K5AH-RMEK]; Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. TIMES (July 13, 2013), http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html.

[25] James Ball, *Secrecy Surrounding 'Zero-Day Exploits' Industry Spurs Calls for Government Oversight*, WASH. POST (Sept. 1, 2012), https://www.washingtonpost.com/world/national-security/secrecy-surrounding-zero-day-exploits-industry-spurs-calls-for-government-oversight/2012/09/01/46d664a6-edf7-11e1-afd6-f55f84bc0c41_story.html [https://perma.cc/SDU7-T7JT]; Michele Golabek-Goldman, *A New Strategy for Reducing the Threat of Dangerous ∅day Sales to Global Security and the Economy* 9 (Mar. 25, 2014) (unpublished policy analysis exercise presented to Deputy Assistant Sec'y of Def. Eric Rosenbach), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2438164; *see also* Kesan & Hayes, *supra* note 16, at 759.

[26] *See* Fidler, *supra* note 16, at 408–10; Andreas Kuehn & Milton Mueller, *Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities* 2–3 (Geo. Mason U. 2014 TPRC / 42d Research Conference on Commc'n, Info. & Internet Policy, Working Paper, Aug. 1, 2014).

[27] Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1097, 1099 (2011); Mary M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 172 n.4 (2000).

I. PRIVATE SECTOR EXPERTISE

Most scholars emphasize regulatory responses to cybersecurity problems.[28] A leading think tank warns that "it is completely inadequate" to leave cybersecurity "to the private sector and the market."[29] Other commentators call for "direct government regulation" of cybersecurity,[30] urge that a federal regulatory scheme is preferable to "pure reliance on the private market,"[31] and claim that "a market-based approach to public safety and national security would never work."[32] An ABA task force has even called for the government "to 'semi-nationalize' some sectors (like the electricity grid) where isolation is not an option and the adverse consequences of certain low probability events are likely to be very high."[33]

In fact, the private sector is highly skilled at generating the information on which cyber defense depends. Threat data is important (that is, newly discovered exploits and other kinds of malicious code[34]), as is information about countermeasures (that is, steps to defeat a particular intrusion or to cure a particular vulnerability[35]). But information about vulnerabilities is particularly vital. Flaws are ubiquitous. "Bugs happen. Inevitably, software code is imperfect."[36] Partly this is due to software's complexity; the fallible human beings who write it invariably will make

[28] *See, e.g.*, Bambauer, *supra* note 23, at 1017–18; Calkins, *supra* note 27, at 174; Emily Frye, *The Tragedy of the Cybercommons: Overcoming Fundamental Vulnerabilities to Critical Infrastructures in a Networked World*, 58 BUS. LAW. 349, 370–71 (2002).

[29] JAMES R. LANGEVIN ET AL., CSIS COMM'N ON CYBERSECURITY FOR THE 44TH PRESIDENCY, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 15 (2008).

[30] Neal Kumar Katyal, *Digital Architecture as Crime Control*, 112 YALE L.J. 2261, 2284, 2286 (2003).

[31] Calkins, *supra* note 27, at 174.

[32] JOINT ECON. COMM. 107TH CONG., SECURITY IN THE INFORMATION AGE 58 (Comm. Print 2002).

[33] AM. BAR ASS'N, NATIONAL SECURITY THREATS IN CYBERSPACE 27 (2009). For exceptions to the pro-regulation consensus, see, for example, PAUL ROSENZWEIG, HOOVER INST., CYBERSECURITY AND PUBLIC GOODS: THE PUBLIC/PRIVATE "PARTNERSHIP" (2012), https://www.hoover.org/sites/default/files/research/docs/emergingthreats_rosenzweig.pdf [https://perma.cc/L9TK-HACT]; Christopher J. Coyne & Peter T. Leeson, *Who's to Protect Cyberspace?*, 1 J.L. ECON. & POL'Y 473, 488 (2005); Eichensehr, *supra* note 24, at 469–73; Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 286 (2006); and Kesan & Hayes, *supra* note 16, at 758–59.

[34] *See* Sales, *supra* note 15, at 1546; *see also* Frye, *supra* note 28, at 368–69.

[35] *See* Sales, *supra* note 15, at 1546.

[36] Bambauer & Day, *supra* note 27, at 1060; *see also* Jennifer Stisa Granick, *The Price of Restricting Vulnerability Publications*, 9 INT'L J. COMM. L. & POL'Y 1, 4 (2005); Kesan & Hayes, *supra* note 16, at 780.

mistakes.[37] Perverse incentives also play a role. The software industry is characterized by a pronounced first mover advantage, so developers tend to rush imperfect software to the market in a bid to lock consumers in to their products.[38] In addition, the costs of flawed products are not borne entirely by vendors but are partly externalized onto consumers.[39] Victims of insecure software are typically unable to sue the developer because tort law's economic loss doctrine generally prevents recovery for purely financial injuries.[40]

Attacks that target zero-day vulnerabilities are especially damaging. Because users by definition are unaware of such flaws, there is essentially no way to defeat exploits that target them. Derek Bambauer likens a zero-day attack to the devastating crane kick from *The Karate Kid*: "[I]f it is done properly, no defense is possible."[41] Of course, even known vulnerabilities can be exploited to catastrophic effect.[42] The average vulnerability remains unpatched for 312 days after discovery by the vendor.[43] Intruders might target these known but unpatched flaws with a "one-day" or "two-day" attack that can be plenty harmful.[44] Indeed, the Stuxnet attack on Iran's nuclear program exploited several vulnerabilities that may have been previously reported.[45] But zero-days are uniquely problematic because they are "unknown unknowns"[46]—threats of which the targets are not even aware.

Attackers might target flaws in widely used products like web browsers to steal credit card numbers and other sensitive information—a fairly common

[37] *See* Bambauer, *supra* note 23, at 1020–21; Hahn & Layne-Farrar, *supra* note 33, at 292; Taiwo A. Oriola, *Bugs for Sale: Legal and Ethical Proprieties of the Market in Software Vulnerabilities*, 28 J. MARSHALL J. COMPUTER & INFO. L. 451, 458–59 (2011).

[38] *See* Ross Anderson, Why Information Security Is Hard—An Economic Perspective 2 (Dec. 2001) (unpublished manuscript presented at the 17th Annual Computer Security Applications Conference), https://www.acsac.org/2001/papers/110.pdf [https://perma.cc/W5K7-UFYC].

[39] *See* Bambauer & Day, *supra* note 27, at 1059; *see also* Sales, *supra* note 15, at 1535–36.

[40] *See infra* notes 195–196 and accompanying text.

[41] Bambauer, *supra* note 23, at 1079; *see also* Leyla Bilge & Tudor Dumitras, *Before We Knew It*, 2012 PROC. ACM CONF. ON COMPUTER & COMM. SECURITY 833, 833; STEFAN FREI & FRANCISCO ARTES, INTERNATIONAL VULNERABILITY PURCHASE PROGRAM: WHY BUYING ALL VULNERABILITIES ABOVE BLACK MARKET PRICES IS ECONOMICALLY SOUND 6 (Dec. 2013), https://www.nsslabs.com/linkservid/0CD6E177-5056-9046-93F5BAB40096E936/ [https://perma.cc/G2BR-2EQK]; Kesan & Hayes, *supra* note 16, at 779–80.

[42] *See* Bambauer, *supra* note 23, at 1050–52.

[43] *See* Bilge & Dumitras, *supra* note 41, at 834.

[44] *Cf.* ABLON ET AL., *supra* note 23, at 26 (describing "half-days" as a partial substitute for zero-days).

[45] *See* Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED (July 11, 2011, 7:00 AM), https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet [http://perma.cc/3D3P-R6QS]; *see also infra* notes 62–67 and accompanying text.

[46] Bambauer, *supra* note 23, at 1078.

occurrence.[47] On a grander scale, they might purloin companies' most valuable trade secrets.[48] They might take control of a smartphone and turn it into a tool of espionage. In 2016, attackers used a trio of vulnerabilities in Apple's iOS operating system to break into iPhones used by journalists and human rights advocates; the attackers accessed the devices' cameras, microphones, and locations, intercepted text messages and emails, and recorded phone calls and messages sent by various communications apps.[49] Some exploits might even cause physical damage, injury, and death. In 2015, a pair of researchers hacked into a Jeep Cherokee as it sped along the highway through a vulnerability in the vehicle's entertainment system, giving them control over its air conditioning, radio, and, more alarmingly, its steering wheel, accelerator, and brakes.[50] Nearly half a million cars on the road had the same flaw.[51] Malicious hackers likewise might exploit vulnerabilities in the industrial control systems that are used to run the electrical grid, destroying key components like turbines and leaving millions of people in the dark for months.[52]

All of which is why it is vital to patch bugs before attackers can take advantage of them. San Bernardino is an especially dramatic example of the private sector's capabilities, but it illustrates a more mundane truth: Hackers are really good at finding flaws. As Andrea Matwyshyn puts it, "security researchers are the 'fact-checkers' of the information technology ecosystem."[53] Hackers' efforts to scour code for flaws are capable of dramatically improving cybersecurity. Stefan Frei and Francisco Artes estimate that vulnerability reports generated by private security researchers could reduce society's total losses from cyber intrusions by 10 percent, and that's a "conservative" estimate.[54] Sam Ransbotham et al. likewise find that private bug hunting "delays the onset and reduces the penetration of the attack diffusion process,"

[47] *See* Bambauer & Day, *supra* note 27, at 1058–60; Hahn & Layne-Farrar, *supra* note 33, at 293; Tom Simonite, *Welcome to the Malware-Industrial Complex*, MIT TECH. REV. (Feb. 13, 2013), https://www.technologyreview.com/s/507971/welcome-to-the-malware-industrial-complex [https://perma.cc/T9MH-6SLM].

[48] *See* Hahn & Layne-Farrar, *supra* note 33, at 294.

[49] *See* Heather Kelly, *iPhone Vulnerability Used to Target Journalists, Aid Workers*, CNN (Aug. 25, 2016, 4:35 PM), http://money.cnn.com/2016/08/25/technology/apple-iphone-hack/index.html [https://perma.cc/PN2R-4EKV].

[50] *See* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway [https://perma.cc/ACD7-WM78].

[51] *See id.* ("Chrysler has issued a recall for 1.4 million vehicles as a result of [the flaw].").

[52] Sales, *supra* note 15, at 1514.

[53] Matwyshyn, *supra* note 16, at 821.

[54] FREI & ARTES, *supra* note 41, at 2.

"decreases the risk of first attack," and "decreases the volume of attacks corresponding to a vulnerability."[55]

Private entities are not just good, in absolute terms, at discovering vulnerabilities. They are often better than the government. This is so for familiar reasons having to do with the costs of acquiring knowledge. As F.A. Hayek emphasized, knowledge "use never exists in concentrated or integrated form but solely as the dispersed bits of incomplete and frequently contradictory knowledge which all the separate individuals possess."[56] That is certainly true in cyberspace. Individual pieces of cybersecurity data are widely distributed among millions of private companies, academic researchers, hackers, and others. These users often have local knowledge that central authorities lack about the vulnerabilities in their systems, the malware they have encountered, the most effective countermeasures, and so on.[57] It would be impossible for a central regulator to generate the voluminous data that private entities spontaneously generate in their ordinary, everyday activities.[58] That may be why President Obama's

[55] Sam Ransbotham et al., *Are Markets for Vulnerabilities Effective?*, 36 MIS Q. 43, 59 (2012); *see also* Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCIENCE 610, 611 (2006); Matthew Finifter et al., *An Empirical Study of Vulnerability Rewards Programs*, 2013 PROC. 22D USENIX SECURITY SYMP. 273, 273; Bruce Schneier, *The Vulnerabilities Market and the Future of Security*, FORBES (May 30, 2012, 12:43 PM), https://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/#7cc034ec7536 [https://perma.cc/3EGR-JP5Y]; Kim Zetter, *With Millions Paid in Hacker Bug Bounties, Is the Internet Any Safer?*, WIRED (Nov. 8, 2012, 6:30 AM), https://www.wired.com/2012/11/bug-bounties/ [https://perma.cc/E45G-9RV8]. The assumption is that researchers are finding flaws that would have been independently discovered and exploited by malicious hackers. Most scholars think rediscovery is likely. *See, e.g.*, Bambauer & Day, *supra* note 27, at 1101; Andy Ozment, The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting 3 (June 3, 2005) (unpublished manuscript presented at the Workshop on Economics and Information Security), http://infosecon.net/workshop/pdf/10.pdf [https://perma.cc/8CYM-Q8EB]. But some believe that the probability is low and that bug hunting therefore does not improve security. *See, e.g.*, Eric Rescorla, *Is Finding Security Holes a Good Idea?*, IEEE SECURITY & PRIVACY, Jan.–Feb. 2005, at 14, 17–19.

[56] F.A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 519 (1945).

[57] *See* Greg Rattray et al., *American Security in the Cyber Commons*, *in* CONTESTED COMMONS: THE FUTURE OF AMERICAN POWER IN A MULTIPOLAR WORLD 137, 146 (Abraham M. Denmark & James Mulvenon eds., 2010); Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1091 (2001); Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SEC. L. & POL'Y 119, 135 (2010).

[58] *See* Coyne & Leeson, *supra* note 33, at 489; Benjamin Powell, *Is Cybersecurity a Public Good? Evidence From the Financial Services Industry*, 1 J.L. ECON. & POL'Y 497, 505 (2005).

homeland security advisor acknowledged that the "private sector has vital information we don't always see unless they share it with us."[59]

The private sector also boasts analytical abilities that rival those of the world's most sophisticated intelligence agencies,[60] including in the notoriously difficult task of attack attribution.[61] Stuxnet is perhaps the preeminent example. When Stuxnet was first noticed in June 2010, most observers regarded it as a minor and unremarkable piece of malware, probably designed for the routine task of stealing data.[62] Its true nature was exposed through an informal collaboration among researchers at Symantec, the American cybersecurity company, and a three-person German firm called Langner. The team's curiosity was piqued by the fact that the malware used two valid but stolen security certificates; perhaps coincidentally, the companies that issued them were located in the same office park.[63] Just as unusually, Stuxnet exploited a number of zero-day vulnerabilities.[64] Here was a bug whose author had the means to acquire—and the willingness to burn—cyber assets of the utmost value and sensitivity. What could be that important? The team plunged into the project, working on several continents around the clock for months. What they discovered was that Stuxnet was "the most sophisticated cyberweapon ever deployed," carefully engineered to cripple uranium enrichment facilities in Iran and thereby prevent the Islamic Republic from building a nuclear weapon.[65] The researchers' work was so thorough that officials at Homeland Security, the Pentagon, the FBI, and other government agencies here and abroad asked them for briefings.[66] Two years later, the White House confirmed what everyone already knew: Stuxnet was the work of the U.S. government, with an assist from Israel.[67]

[59] Lisa O. Monaco, Assistant to the President for Homeland Sec. & Counterterrorism, Strengthening Our Nation's Cyber Defenses (Feb. 10, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/02/11/remarks-prepared-delivery-assistant-president-homeland-security-and-coun [https://perma.cc/G5L6-AFF4].

[60] *See* Eichensehr, *supra* note 24, at 489.

[61] *See* Sales, *supra* note 15, at 1524–25.

[62] *See* Zetter, *supra* note 45.

[63] *See id.*

[64] *See id.*; *see also* Ball, *supra* note 25; Menn, *supra* note 24; Simonite, *supra* note 47, at 16.

[65] William J. Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), http://nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

[66] Zetter, *supra* note 45.

[67] Ellen Nakashima & Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, WASH. POST (June 2, 2012), https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.8eb861fc2d3c [http://perma.cc/T9ZR-WKAR].

A more recent example comes from the 2016 election. Someone hacked into the Gmail account of John Podesta, the chairman of Hillary Clinton's presidential campaign, stealing dozens of embarrassing emails that were soon posted on the internet. Private researchers quickly determined that the hackers were affiliated with the Kremlin. Indeed, according to two former members of the House Intelligence Committee, "[i]t took the private cyber security firm Crowdstrike a month to investigate the digital break-in at the Democratic National Committee and publish a detailed report attributing the hack to Russia. It took the intelligence community several months to consolidate around the same assessment."[68]

II. Problems With the Current Market

A. Of Hats and Markets: White, Black, and Gray

The market for cybersecurity information contains three distinct sectors.[69] First is the white market, in which so-called white hat or ethical hackers—researchers "who probe for computer software and hardware flaws with the goal of discovering, not exploiting, them"[70]—sell their discoveries to buyers who will fix the flaws. There is also a shadowy black market, where less scrupulous black hats sell to the highest bidder. Buyers include international criminals, hostile foreign governments, and terrorist groups. In between these two worlds is a thriving gray market. The major buyer here is the U.S. government—primarily the NSA, but other agencies as well. The government pays top dollar for bugs and uses them for various offensive purposes, such as gathering intelligence, conducting covert operations (Stuxnet is a good example), tracking criminal suspects, and so

[68] Jane Harman & Peter Hoekstra, *Trump's Intel Reform Is a Good First Step*, WALL ST. J. (Jan. 22, 2017, 5:08 PM), https://wsj.com/articles/trumps-intel-reform-is-a-good-first-step-1485122926; *see also* Eichensehr, *supra* note 24, at 491 n.118 (providing other examples of private sector attribution, sometimes in partnership with the government).

[69] *See* Fidler, *supra* note 16, at 410; Cassandra Kirsch, *The Grey Hat Hacker*, 41 N. KY. L. REV. 383, 386 (2014); *see also* Robert Lemos, *Private Market Growing for Zero-Day Exploits and Vulnerabilities*, SEARCHSECURITY (Nov. 27, 2012), http://searchsecurity.techtarget.com/feature/Private-market-growing-for-zero-day-exploits-and-vulnerabilities [https://perma.cc/D84C-XQVT].

[70] Bambauer & Day, *supra* note 27, at 1053.

on. The boundaries between these sectors can be fuzzy, as market participants might swap hats depending on the available opportunities on any given day.[71]

1. A Whiter Shade of Pale

The white market is underdeveloped and unsophisticated.[72] There are essentially two mechanisms for legitimate sales of cybersecurity information. First are bug bounty programs, in which software vendors and other companies offer modest cash rewards to researchers who report vulnerabilities in their products and then issue patches for the flaws. Second, some independent security firms purchase vulnerability information and offer their subscribers a variety of services, such as intrusion detection, until vendors patch the bugs.[73]

Netscape—remember them?—established the industry's first bug bounty program in 1995.[74] The program didn't take off, but Netscape was ahead of its time. Today, a number of leading software vendors pay independent researchers who report flaws in their products.[75] Take, for instance, Google, whose program launched in 2010 and is now "widely considered an exemplar of a mature, successful" program.[76] Initially the company only offered maximum payouts of $1337 and then $3133.70[77]—modest and idiosyncratic sums that paid homage to the hacker slang term for "elite" ("1337" = "leet").[78] Today it pays as much as $30,000 for the most severe bugs.[79] As of 2013, Google's payments

[71] *See* ABLON ET AL., *supra* note 23, at 1–2; Fidler, *supra* note 16, at 415–16; *cf.* Oriola, *supra* note 37, at 512 (describing the "real possibility that vulnerabilities information derived from underground market could end up for sale in legal markets and vice-versa").

[72] *See* Fidler, *supra* note 20, at 32; *see also* FREI & ARTES, *supra* note 41, at 10.

[73] Several nonmarket players also receive vulnerability reports from researchers without paying compensation. The best known is probably CERT—the Computer Emergency Response Team, a federally funded research center at Carnegie Mellon University. *See* Karthik Kannan & Rahul Telang, An Economic Analysis of Market for Software Vulnerabilities 1–2 (May 3, 2004) (unpublished manuscript), https://www.dtc.umn.edu/weis2004/kannan-telang.pdf [https://perma.cc/A2RM-2475]; *see also* Pu Li & H. Raghav Rao, *An Examination of Private Intermediaries' Roles in Software Vulnerabilities Disclosure*, 9 INFO. SYS. FRONTIERS 531, 531 (2007).

[74] *See* Zetter, *supra* note 55.

[75] For a helpful chart summarizing various bounty programs, see *id.*

[76] Finifter et al., *supra* note 55, at 274.

[77] *See id.*; Andy Greenberg, *Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits*, FORBES (Mar. 23, 2012, 9:43 AM), https://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/#7ae51b6e2660 [https://perma.cc/HU3A-TWKA].

[78] *See* Matwyshyn, *supra* note 16, at 826 n.159.

[79] *See* Finifter et al., *supra* note 55, at 274; Perlroth & Sanger, *supra* note 24.

totaled more than $2 million.[80] Scholars estimate that Google's programs have been responsible for identifying 28 percent of the patched vulnerabilities in the company's products.[81] Google also hosts the Pwnium contest, which awards up to $60,000 to researchers who demonstrate a working exploit for a flaw in a Google product.[82] Other firms have similar programs. Facebook offers a maximum of $20,000 for the most critical flaws; its program paid out at least $1 million between its launch in 2011 and 2013.[83] Microsoft began buying bugs in 2013 after resisting pressure to establish its own program for years,[84] and Apple did the same in 2016, though its program is invite-only.

Yet many other companies continue to resist creating their own bug bounty programs.[85] Kristen Eichensehr points out that "94% of companies included in the Forbes Global 2000 'did not advertise a way for so-called ethical hackers to report bugs,' much less pay hackers to report them."[86] And Frei and Artes found that seven of the ten software vendors with the most reported vulnerabilities in 2012 did not pay bounties.[87] Holdouts include household names like Adobe.[88] As of 2011, some 99 percent of personal computers globally and in the U.S. were running the company's popular Flash Player.[89]

In recent years, a handful of brokers have emerged to connect white hats with vendors, though they don't appear to be as well developed as their gray- and black-market counterparts. The most prominent is probably HackerOne, founded in 2011.[90] The company has facilitated around 9000 bug sales with hackers receiving more than $3 million in bounties; it earns a 20 percent

[80] *See* Dennis Fisher, *After Paying $2M in Rewards, Google Multiplies Some Bug Bounties Five Times*, ThreatPost (Aug. 13, 2013, 10:03 AM), https://threatpost.com/after-paying-2m-in-rewards-google-multiplies-some-bug-bounties-five-times/101973/ [https://perma.cc/GU33-YQDA].

[81] *See* Finifter et al., *supra* note 55, at 273.

[82] *See* Zetter, *supra* note 55.

[83] *See* Perlroth & Sanger, *supra* note 24.

[84] *See* Dennis Fisher, *Researchers Find Bug Bounty Programs Pay Economic Rewards*, ThreatPost (July 10, 2013, 12:12 PM), https://threatpost.com/researchers-find-bug-bounty-programs-pay-economic-rewards/101243/ [https://perma.cc442L-TZYK].

[85] *See* Menn, *supra* note 24.

[86] Eichensehr, *supra* note 24, at 486 n.90.

[87] *See* Frei & Artes, *supra* note 41, at 16.

[88] *See* Zetter, *supra* note 55.

[89] *See Adobe Flash Platform Runtimes*, ADOBE, [https://perma.cc/T7N9-X93J].

[90] *See* Serena Saitto, *The Big Business of Smashing Bugs*, Bloomberg (Mar. 12, 2015, 2:49 PM), https://www.bloomberg.com/news/articles/2015-03-12/ethical-hackers-booming-job-market [https://perma.cc/HCV7-HS9Z].

commission on each sale.[91] HackerOne has raised an impressive amount of money from venture capitalists—$9 million in 2014,[92] followed by another $40 million in 2017—though it has yet to turn a profit.[93] That may be due to the white market's relatively low prices; HackerOne's average payout is just $500.[94] Other white market brokers tend to keep a lower profile, but they may face similar challenges.

The second mechanism for legitimate bug sales is programs run by independent security companies, such as TippingPoint's Zero Day Initiative (ZDI) and the Verisign iDefense Vulnerability Contributor Program (VCP). ZDI, established in 2005, and VCP, established in 2002, operate in subtly different ways, but they are broadly similar in their essentials.[95] Each offers cash rewards to researchers who report flaws, then pass the reports to the responsible developers, usually for free, with the expectation that the firms will fix the problems. ZDI and VCP pay less—often considerably less—than vendors, let alone black- or gray-market buyers. They reportedly pay up to $10,000,[96] though most awards are said to be between $1000 and $5000, with the bulk of them below $2000.[97] Nevertheless, ZDI and VCP have been fairly successful at bringing bugs to light. Frei and Artes report that they "have jointly purchased an average of 17 percent of all vulnerabilities affecting major software vendors" since they were founded.[98] Those are indeed "remarkable number[s]"[99] considering the modest payouts.

Many scholars refer to ZDI and VCP as "brokers,"[100] but it's more accurate to call them subscription-based security firms. Their business model is to provide security services, such as intrusion detection and other

[91] *See* Nicole Perlroth, *HackerOne Connects Hackers With Companies, and Hopes for a Win-Win*, N.Y. TIMES (June 7, 2015), https://www.nytimes.com/2015/06/08/technology/ hackerone-connects-hackers-with-companies-and-hopes-for-a-win-win.html.

[92] *See* Saitto, *supra* note 90, at 2.

[93] *See* Matt Weinberger, *The Startup Paying People to Legally Hack Uber, Nintendo, and Starbucks Just Got Another $40 Million to Keep Growing*, BUS. INSIDER (Feb. 8, 2017, 10:01 AM), http://www.businessinsider.com/hackerone-raises-40-million-series-c-2017-2 [https://perma.cc/Z3QE-VXD4].

[94] *See id.*

[95] *See* Anderson & Moore, *supra* note 55, at 612; Fidler, *supra* note 16, at 413–14; Li & Rao, *supra* note 73, at 531–32; Lemos, *supra* note 69; Zetter, *supra* note 55.

[96] *See* Bilge & Dumitras, *supra* note 41, at 836.

[97] *See* Lemos, *supra* note 69.

[98] FREI & ARTES, *supra* note 41, at 7.

[99] STEFAN FREI, NSS LABS, THE KNOWN UNKNOWNS: EMPIRICAL ANALYSIS OF PUBLICLY UNKNOWN SECURITY VULNERABILITIES 10 (2013).

[100] *See, e.g.*, Böhme, *supra* note 22, at 302–03; *see also, e.g.*, BÖHME, *supra* note 18, at 3; Kesan & Hayes, *supra* note 16, at 761; Fidler, *supra* note 20, at 29–30.

countermeasures, to clients that reportedly range from Fortune 500 companies to government agencies.[101] These products enable subscribers to reduce the risk of attack before the vendor issues a patch.[102] Business is apparently booming; a subscription is said to cost "more than ten times the reward for a vulnerability report."[103]

Remunerative programs like bug bounties have grown more common because researchers increasingly expect monetary compensation for their efforts. Many hackers have intrinsic motivations; for them, the research is its own reward.[104] They hunt bugs because of simple curiosity, the thrill of discovery, and so on.[105] Others want to burnish their reputations among their hacker peers.[106] Because they have been moved more by fun and fame than fortune, these researchers traditionally were willing to report flaws for little more than public recognition, such as having their names posted to a vendor's "Hall of Fame," or corporate tchotchkes, like hats and t-shirts. Of course, the resulting fame can be monetized. Well-regarded researchers might leverage their reputations into jobs with private firms or government agencies.[107]

Today, the link between hacking and compensation is more direct. "[B]ugs for bucks"[108] is the new normal.[109] "Providing professional work for free to a vendor is unethical," one hacker said. "Providing professional work almost for free to security companies that make their business with your research is even more unethical."[110] The trend is especially pronounced for the most capable researchers. NSA analyst turned hacker Charlie Miller claims that "the best researchers are now motivated more by

[101] *See* Li & Rao, *supra* note 73, at 532; Ransbotham et al., *supra* note 55, at 46; *see also* CHARLIE MILLER, INDEP. SEC. EVALUATORS, THE LEGITIMATE VULNERABILITY MARKET: INSIDE THE SECRETIVE WORLD OF 0-DAY EXPLOIT SALES 1, 2 (2007).

[102] *See* Anderson & Moore, *supra* note 55, at 612; Böhme, *supra* note 22, at 5.

[103] Böhme, *supra* note 22, at 302.

[104] *See* Alexander E. Voiskounsky & Olga V. Smyslova, *Flow-Based Model of Computer Hackers' Motivation*, 6 CYBERPSYCHOLOGY & BEHAV. 171, 172–73 (2003).

[105] *See* Bambauer & Day, *supra* note 27, at 1066; Coyne & Leeson, *supra* note 33, at 481.

[106] *See* Yochai Benkler, *Coase's Penguin, or, Linux and* The Nature of the Firm, 112 YALE L.J. 369, 424–25 (2002); Serge Egelman et al., *Markets for Zero-Day Exploits: Ethics and Implications*, 2013 NEW SECURITY PARADIGMS WORKSHOP 41, 43 (2013); Kesan & Hayes, *supra* note 16, at 782–83.

[107] *See* Benkler, *supra* note 106, at 424–25; Egelman et al., *supra* note 106, at 44.

[108] Kuehn & Mueller, *supra* note 26, at 4.

[109] *See*, *e.g.*, MILLER, *supra* note 101, at 2; Golabek-Goldman, *supra* note 25, at 21; *see also, e.g.*, Paul N. Stockton & Michele Golabek-Goldman, *Curbing the Market for Cyber Weapons*, 32 YALE L. & POL'Y REV. 239, 247 (2013); Tom Gjelten, *In Cyberwar, Software Flaws Are a Hot Commodity*, NPR (Feb. 12, 2013, 3:25 AM), https://www.npr.org/2013/02/12/ 171737191/in-cyberwar-software-flaws-are-a-hot-commodity; Menn, *supra* note 24.

[110] Perlroth & Sanger, *supra* note 24 (quoting Luigi Auriemma, founder of ReVuln).

monetary gain than prestige."[111] Amateurs may be content with token compensation for finding a nuisance bug. But researchers who are capable of discovering and exploiting a critical flaw in the software that runs the nation's power grid expect a bigger payday. These changed expectations may well be a response to the lucrative opportunities that await researchers in the black and gray markets.[112]

2. Back in Black

Alongside the white market is a shadowy netherworld where black hats sell vulnerabilities and exploits to outlaw buyers like hostile foreign governments and terrorist groups. Little is known about this obscure and "anarchic"[113] corner of the internet, for good reason: "Criminals try to hide what they do; their markets are clandestine by nature . . . ."[114] But its outlines are coming into sharper focus thanks to recent scholarly work.[115]

Black market sales often take place in specialized online forums where buyers and sellers meet, negotiate, and agree to terms.[116] Jaziar Radianti et al. found at least a dozen forums that are visible to the public, but there are more rarefied tiers that are invite-only.[117] Access is granted after "extensive vetting" to those with the right contacts and "a good reputation, especially for being trustworthy."[118] These entry barriers serve at least two purposes. Not only do they help prevent infiltration by law enforcement, they also manage the risk of fraud that is endemic to these sorts of illicit deals.[119] Nearly a third of black market sellers are said to be "rippers," and defrauded buyers get their money back just 15 to 20 percent of the time.[120] If you're an ISIS operative who gets scammed trying to buy an exploit kit for a vulnerability at a nuclear plant, you can't exactly complain to the FBI.

[111] MILLER, *supra* note 101, at 2.

[112] *See* Gjelten, *supra* note 109.

[113] Ryan Gallagher, *Cyberwar's Gray Market*, SLATE (Jan. 16, 2013, 9:00 AM), http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html [https://perma.cc/Z8N9-C2SR].

[114] ABLON ET AL., *supra* note 23, at 2.

[115] *See id.*; Jaziar Radianti et al., *Vulnerability Black Markets: Empirical Evidence and Scenario Simulation*, 2009 PROC. 42D HAW. INT'L CONF. ON SYS. SCI. 1.

[116] *See* Radianti, *supra* note 115, at 3.

[117] *Id.*; *accord* ABLON ET AL., *supra* note 23, at 7.

[118] ABLON ET AL., *supra* note 23, at 5–6, 16; *see also* Radianti, *supra* note 115, at 3, 9.

[119] ABLON ET AL., *supra* note 23, at 16.

[120] *Id.* at 17; *see also* Radianti, *supra* note 115, at 4.

Black market players reportedly rely on intermediaries to facilitate sales. For instance, a marketplace known as TheRealDeal charges around 3 percent of the sale price for each transaction it brokers.[121] It maintains various countermeasures against surveillance and fraud: The site "uses the anonymity software Tor and the digital currency bitcoin to hide the identities of its buyers, sellers, and administrators," and it holds payments in escrow so participants can get their money back if they're scammed.[122] Specific numbers are hard to come by, but black market prices are significantly higher than their licit counterparts.[123] Radianti describes a vulnerability that cost $2500 on the white market fetching $30,000 on the black.[124]

3. Shades of Gray

The newest and most lucrative sector is the gray market, in which government agencies acquire bugs for use in intelligence gathering, covert operations, and the like.[125] As recently as 2006, two scholars reported that there was no public evidence of government buyers paying for vulnerability information.[126] Times have changed. The gray market has exploded in recent years.[127] The key buyer here is the NSA.[128] (Fort Meade also is said to develop vulnerability data and exploits in-house.[129]) The NSA reportedly spent more

[121] Andy Greenberg, *New Dark-Web Market Is Selling Zero-Day Exploits to Hackers*, WIRED (Apr. 17, 2015, 6:25 AM), https://www.wired.com/2015/04/therealdeal-zero-day-exploits [https://perma.cc/CC7A-F935].

[122] *Id.*

[123] Bambauer & Day, *supra* note 27, at 1067; Fidler, *supra* note 20, at 38.

[124] Jaziar Radianti, *Eliciting Information on the Vulnerability Black Market From Interviews*, 2010 FOURTH INT'L CONF. ON EMERGING SECURITY INFO. SYSS. & TECHS. 157.

[125] Menn, *supra* note 24; Mathew J. Schwartz, *NSA Contracted With Zero-Day Vendor Vupen*, DARKREADING (Sept. 17, 2013, 10:19 AM), http://www.darkreading.com/risk-management/nsa-contracted-with-zero-day-vendor-vupen/d/d-id/1111564 [https://perma.cc/DL5T-47RX]; Simonite, *supra* note 47; Chris Strohm & Michael Riley, *FBI Keeps Internet Flaws Secret to Defend Against Hackers*, BLOOMBERG (Apr. 29, 2014 9:00 PM), https://www.bloomberg.com/news/articles/2014-04-30/fbi-keeps-internet-flaws-secret-to-defend-against-hackers [https://perma.cc/F8P9-H38J].

[126] Michael Sutton & Frank Nagle, *Emerging Economic Models for Vulnerability Research*, 2006 FIFTH WORKSHOP ON ECON. INFO. SECURITY 4.

[127] *See* FREI, *supra* note 99, at 14; Greenberg, *supra* note 77; *see also* Matwyshyn, *supra* note 16, at 841 n.216.

[128] SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX 94 (2014).

[129] Barton Gellman & Ellen Nakashima, *U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show*, WASH. POST (Aug. 30, 2013), https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html?utm_term=.4d0a0f74a647 [http://perma.cc/E8AB-9H3L].

than $25 million on bugs in 2013,[130] and it is far from alone. Other U.S. buyers include intelligence agencies, the armed forces, and the FBI.[131] Indeed, the U.S. may have purchased one of the zero-days exploited by Stuxnet on the gray market.[132] Foreign governments also buy bugs, both friendly ones (Israel, Singapore, the U.K.) and not so friendly (Iran, North Korea, Russia).[133] China doesn't appear especially active, as it reportedly develops most of its vulnerabilities and exploits internally or acquires them from "patriotic" Chinese citizens.[134] A handful of private companies also buy on the gray market. Mostly these are security firms that use the bugs in penetration testing—probing clients' systems to see how resistant they are to cyberattacks.[135] As one seller explains, "[i]f you test a bullet proof vest, you use a bullet, not a squirt gun."[136]

Gray market buyers pay top dollar. Indeed, prices are even higher on the gray market than on the black market.[137] The average bug reportedly sells for between $35,000 and $160,000,[138] and prices easily can climb into the hundreds of thousands of dollars.[139] One established player scoffed at $250,000 as a "lowball[]" offer.[140] Flaws in Apple's famously secure iOS are among the most coveted, with one reportedly fetching $500,000,[141] not to mention the million-dollar payout to the San Bernardino hackers.[142] Charlie Miller was able to buy "a fabulous new kitchen" with his earnings from a sale, inspiring one wag to propose a new metric for valuing vulnerabilities: Bugs "should be rated based on the number of kitchen remodeling projects they could sponsor."[143]

These lavish payouts have lured at least three kinds of intermediaries into the market. First are the individual brokers. Take, for instance, "the Grugq," a

[130] *Id.*; *see also* Stockton & Golabek-Goldman, *supra* note 109, at 249.

[131] Menn, *supra* note 24; Simonite, *supra* note 47; Strohm & Riley, *supra* note 125.

[132] Menn, *supra* note 24.

[133] Fidler, *supra* note 16, at 406; Perlroth & Sanger, *supra* note 24.

[134] Perlroth & Sanger, *supra* note 24; *see also* Greenberg, *supra* note 77; Menn, *supra* note 24. *But see* Golabek-Goldman, *supra* note 25, at 11 (claiming that China "also purchase[s] Ødays on the worldwide vulnerability market").

[135] Fidler, *supra* note 16, at 415–16; Lemos, *supra* note 69.

[136] Greenberg, *supra* note 77.

[137] *Id.*

[138] Perlroth & Sanger, *supra* note 24. To see price lists for various gray market transactions, see ABLON ET AL., *supra* note 23, at 27, and Greenberg, *supra* note 77.

[139] *See, e.g.*, ABLON ET AL., *supra* note 23, at 26; Lemos, *supra* note 69; Schneier, *supra* note 55.

[140] Greenberg, *supra* note 77.

[141] Perlroth & Sanger, *supra* note 24.

[142] *See supra* notes 11–14 and accompanying text.

[143] Mathew J. Schwartz, *Weaponized Bugs: Time for Digital Arms Control*, DARKREADING (Oct. 5, 2012, 12:34 PM), http://www.darkreading.com/attacks-and-breaches/weaponized-bugs-time-for-digital-arms-control/d/d-id/1106686 [https://perma.cc/5U3H-5UBY].

South African hacker and middleman who is based in Bangkok—and the guy who admired Charlie Miller's kitchen. The Grugq charges his sellers a 15 percent commission, and he only handles big-ticket items; he won't touch transactions worth less than $50,000.[144] In 2012 he was on track to earn more than $1 million, and in the previous December alone he raked in $250,000 from deals with government buyers. "The end-of-year budget burnout was awesome," he boasts.[145] The Grugq's clients tend to be his hacker buddies;[146] as in the black market, access to the marketplace can depend on having the right personal contacts.[147]

Second, a number of companies connect hackers with gray market buyers.[148] A half dozen such firms are known to exist, and there are probably others keeping a low profile.[149] The most famous are Malta-based ReVuln and the French firm Vupen.[150] ReVuln, founded in 2012, specializes in vulnerabilities in industrial control systems.[151] In addition to serving as a middleman, the company does some vulnerability research and writes exploit code in-house; it is both researcher and go-between.[152] Vupen was founded in 2008 as a white market broker, and until 2010, it notified vendors for free when flaws came to light.[153] But the company soon shifted to the far more lucrative gray market. Many—maybe even all—of Vupen's vulnerabilities and exploits are generated internally.[154] These companies have no interest in working with vendors to improve product security. At a 2012 hacking contest in Vancouver, Vupen demonstrated an exploit that compromised Google's Chrome web browser—then refused to hand it over for the $60,000 prize money.[155] "We wouldn't share this with Google for even $1 million," boasted

[144] Schwartz, *supra* note 125.

[145] Andy Greenberg, *Meet the Hackers Who Sell Spies the Tools to Crack Your PC (and Get Paid Six-Figure Fees)*, FORBES (Mar. 21, 2012, 9:08 AM), https://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/#1da4c4081f74 [http://perma.cc/65KJ-GVCZ].

[146] *Id.*

[147] Charlie Miller reports that he was able to sell a bug to the NSA, his old employer, only because of personal "contacts" that fostered "a certain level of trust in the vulnerability I had." MILLER, *supra* note 101, at 8.

[148] ABLON ET AL., *supra* note 23, at 26; Ball, *supra* note 25; Perlroth & Sanger, *supra* note 24.

[149] For a table of known gray market sellers, see Fidler, *supra* note 16, at 419–21.

[150] Stockton & Golabek-Goldman, *supra* note 109, at 250–51.

[151] *Id.* at 250.

[152] Lemos, *supra* note 69; Menn, *supra* note 24.

[153] Greenberg, *supra* note 145; Menn, *supra* note 24.

[154] Some scholars describe Vupen as a broker. *See, e.g.*, ABLON ET AL., *supra* note 23, at 26 n.5. However, the company's CEO has said that "'all of our research is done in-house' and that his firm doesn't buy or sell third-party exploits." Schwartz, *supra* note 125.

[155] Greenberg, *supra* note 145; *see also* Matwyshyn, *supra* note 16, at 835.

the company's CEO. "We don't want to give them any knowledge that can help them in fixing this exploit or other similar exploits. We want to keep this for our customers."[156]

Finally, some defense contractors act as middlemen, including firms like Lockheed Martin and Raytheon.[157] Some buy bugs from outside researchers and resell them to their government clients, while others hunt for vulnerabilities or write exploit code in-house.[158] Very little is known about these firms' activities.[159] But their role in the gray market is probably not a small one. One analyst points to bugs as "a growing area of the defense business at the same time that the rest of the defense business is shrinking."[160] Mailyn Fidler likewise cites the substantial gap between the sums the government is known to spend and the profits of other gray market sellers as evidence that defense contractors must be active in the market.[161]

Gray market brokers have come under a fair amount of criticism. The ACLU's Chris Soghoian blasts them as "cowboys," "ticking bomb[s]," "modern-day merchants of death," and, the unkindest cut of all, "the *Jersey Shore* of the exploit trade."[162] Perhaps in response, some brokers have adopted policies to keep their gray market sales from turning black. The Grugq won't work with Russian or Chinese buyers.[163] This is for self-interest as much as principle; he complains that "[s]elling a bug to the Russian mafia guarantees it will be dead in no time, and they pay very little money," whereas the market in China "is very depressed" because of the glut of Chinese hackers who sell only to their government.[164] Vupen likewise only sells to NATO members or partners or to countries that are not currently subject to international sanctions.[165] ReVuln evidently has no such scruples. The company's cofounder says "I don't see bad guys or good guys. It's just business."[166]

[156] Ball, *supra* note 25.

[157] HARRIS, *supra* note 128, at 94; Fidler, *supra* note 16, at 417; Menn, *supra* note 24; Schneier, *supra* note 55; Simonite, *supra* note 47.

[158] Fidler, *supra* note 16, at 417; Menn, *supra* note 24.

[159] FREI, *supra* note 99, at 14; Simonite, *supra* note 47.

[160] Simonite, *supra* note 47 (quoting Peter Singer of the Brookings Institution).

[161] Fidler, *supra* note 16, at 423; *see also* FREI, *supra* note 99, at 14.

[162] Ryan Naraine, *'0-day Exploit Middlemen Are Cowboys, Ticking Bomb'*, ZDNET (Feb. 16, 2012, 10:19 AM), http://www.zdnet.com/article/0-day-exploit-middlemen-are-cowboys-ticking-bomb/ [https://perma.cc/B3KD-BDBM]; *see also* Gallagher, *supra* note 113; Greenberg, *supra* note 145.

[163] Greenberg, *supra* note 77.

[164] *Id.*

[165] Gallagher, *supra* note 113; *see also* Stockton & Golabek-Goldman, *supra* note 109, at 250.

[166] Gjelten, *supra* note 109.

B. Transaction Costs and Structural Defects

The white market shows great potential but "suffers from a number of imperfections."[167] As explained in this Subpart, it is plagued by significant transaction costs and other structural defects.[168] And, as discussed below, many hackers prefer to sell on the gray market, as vendors cannot compete with the lavish payouts offered by government buyers. As a result, fewer bugs are sold to vendors, flaws go unpatched, and users remain exposed to cyberattacks.

The first problem with the white market is the search costs.[169] Consider what a bug sale looks like from a hacker's standpoint. Suppose a white hat finds a critical flaw in iOS. Whom should he tell? The answer isn't always obvious. "Many software vendors still have no well-documented or established process by which they communicate with or respond to researchers, or they do not wish to engage with researchers at all."[170] So should the hacker reach out to Apple's senior management? The general counsel's office? Tech support? Unless he is a repeat player who has sold bugs in the past, he is unlikely to have contacts at the company with which he hopes to do business. As a result, he may be reduced to cold calling the vendor and hoping that his offer eventually is routed to the appropriate decisionmakers.[171] Of course the seller's search costs can be mitigated if the vendor has a bug bounty program, but many major players don't.[172]

Apple will incur substantial costs of its own as it works to verify the seller's good faith.[173] Vendors receive thousands of reports each year about claimed flaws in their products, and it's hard to separate the wheat from the chaff. Does a given report describe an actual vulnerability or is it just a prank? Is the seller a legitimate researcher or an extortionist? Many developers regard bug hunting as a form of blackmail—pay me or I'll exploit this vulnerability.[174] If the researcher is an unknown quantity, the vendor can only speculate about his intentions.

[167] BÖHME, *supra* note 18, at 2.

[168] Bambauer & Day, *supra* note 27, at 1100; Matwyshyn, *supra* note 16, at 825; *see also* MILLER, *supra* note 101, at 3–4.

[169] *See* ABLON ET AL., *supra* note 23, at 25; Bambauer & Day, *supra* note 27, at 1100; Kuehn & Mueller, *supra* note 26, at 6.

[170] FREI & ARTES, *supra* note 41, at 14; *see also* Bambauer & Day, *supra* note 27, at 1100.

[171] MILLER, *supra* note 101, at 3.

[172] *See supra* notes 85–88 and accompanying text.

[173] ABLON ET AL., *supra* note 23, at 25; Bambauer & Day, *supra* note 27, at 1100; *see also* MILLER, *supra* note 101, at 4.

[174] FREI, *supra* note 99, at 6. One gray market vulnerability broker has stated: "If we approached a vendor and said, 'Hey guys, we've got this awesome zero-day and we want you to buy it,' that's either borderline extortion, or it's extortion . . . . I can't do that." Ball, *supra* note 25.

Second, because of the significant power imbalance between buyers and sellers, "the market price is set by the demand side."[175] This imbalance is due in part to the fact that software vendors are sophisticated firms, while those who uncover flaws in their products are often individual researchers.[176] Market structure also plays a role. The buyer's side is highly concentrated. A hacker who finds a flaw in Windows realistically can only sell it to Microsoft; he certainly can't sell to Apple. The white market thus is a quasi-monopsony—there is essentially a single buyer for a given vulnerability.[177] Monopsony generally means lower prices, and some anecdotal evidence suggests that monopsonistic buyers do indeed drive down prices in vulnerability markets. The Grugq claims that China's zero-day market "is very depressed"; "the country has too many hackers who sell only to the Chinese government, pushing down prices."[178]

A third problem is the information asymmetry between hackers and vendors. Because a seller will always know more about a bug than a buyer, the buyer inevitably will bid down the sale price. The problem is a variation of George Akerlof's famous analysis of "lemon" cars.[179] Imagine a market for used automobiles. There are one hundred that are reliable and one hundred others that are not—they're lemons. A good car is worth $3000, while a lemon is worth just $1000. Suppose further that dealers know which cars are lemons but buyers don't. How will this affect price and quality? If buyers know that they have a 50 percent chance of getting a lemon, they'll refuse to pay more than $2000. But at that price, dealers will only offer lemons; why sell a good car for less than its market value? The bad products will drive out the good ones. Buyers in turn will observe that all of the cars being sold are lemons, and the price will further drop to $1000. Information asymmetries thus can dramatically drive down the sale price and the quality of the goods.

[175] BÖHME, *supra* note 18, at 2; *see also* Fidler, *supra* note 20, at 29, 32.

[176] *Cf.* Bambauer & Day, *supra* note 27, at 1087 ("Many researchers have limited resources and legal acumen . . . .").

[177] *See* Ozment, *supra* note 17, at 7. To be precise, the market is not a strict monopsony, because a hacker can always sell to an independent security company or, if he wishes to venture onto the gray or black markets, to governments or criminals.

[178] Greenberg, *supra* note 77.

[179] George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488 (1970); *see also* BÖHME, *supra* note 18, at 1; Anderson, *supra* note 38, at 5–6.

The same issue can arise with vulnerability sales.[180] A researcher who discovers a flaw will know considerably more about its severity than the vendor. The vendor therefore will be unwilling to pay a price that reflects the bug's fair market value and instead will bid down the sale price to a level that reflects the probability that the information is worthless. This "downward pressure on both price and quality" is likely to be "severe."[181] Some hackers might respond by giving up on research altogether, while others take their talents to the more lucrative black and gray markets. The ones who remain are likely to be less skilled, with corresponding declines in the quality of their discoveries. Vendors will quickly catch on, causing them to pay even less for bug reports. And the death spiral continues.

The hacker could attempt to prove the flaw's severity, but that only raises a fourth difficulty: the Arrow information paradox.[182] Kenneth Arrow recognized that a seller who attempts to demonstrate the quality of an information good faces a dilemma. If he reveals too little, the buyer might underestimate its quality and decide not to purchase it. But if the seller reveals too much, he effectively conveys the information to the buyer without payment; this is so because the information is both nonrivalrous (the seller and buyer can possess it simultaneously) and nonexcludable (the seller cannot deny the buyer access to the information once exposed to it).[183] In short, efforts to demonstrate the quality of information can destroy its economic value.[184]

Bug sales raise the same paradox.[185] A vendor understandably will want some assurances that the bug on offer is indeed a critical flaw. But, from the hacker's standpoint, describing the bug might enable the buyer to reverse engineer it, thus obviating the need to pay.[186] Nor is it a solution for the hacker to prove value by demonstrating a working exploit. Running the exploit on the vendor's system could allow it to reverse-engineer the flaw, and "[i]t is not possible to exploit a system in the possession of the researcher because the seller will not be able to verify that the system has not been altered in some

[180] *See* Bambauer & Day, *supra* note 27, at 1100; *see also* BÖHME, *supra* note 18, at 1; Granick, *supra* note 36, at 29.

[181] Anderson, *supra* note 38, at 6.

[182] Kenneth J. Arrow, *Economic Welfare and the Allocation of Resources for Invention*, *in* THE RATE AND DIRECTION OF INVENTIVE ACTIVITY: ECONOMIC AND SOCIAL FACTORS 609, 616–19 (1962).

[183] *Cf.* MILLER, *supra* note 101, at 4 (emphasizing that the "problem is true for information goods in general").

[184] Bambauer & Day, *supra* note 27, at 1100–01; Kesan & Hayes, *supra* note 16, at 801.

[185] MILLER, *supra* note 101, at 3–4; Egelman et al., *supra* note 106, at 44.

[186] *See* MILLER, *supra* note 101, at 5.

fashion."[187] Researchers thus face an intractable dilemma: "[D]isclose too little, and vendors may not believe the problem is real; disclose too much, and a software company may take the information without compensation."[188]

C. Offense Bias

The second major problem is what might be called offense bias. Bugs tend to be sold on the gray and black markets where they are used for offensive purposes, such as espionage and crime, rather than on the white market where vendors can patch them. Subpart II.C.1 offers several explanations for this trend. The most obvious reason is money—governments and criminals offer payments that are literally "orders of magnitude" greater than what white market buyers are paying.[189] In addition, hackers face a substantial risk of legal liability when they do business on the white market, whereas sales to government agencies carry an implicit guarantee of immunity. Subpart II.C.2 explains why gray market sales are problematic. Not only do they leave users vulnerable to attacks by adversaries who've discovered the same flaw, there is also a risk of proliferation: A seemingly legitimate gray market buyer might be a proxy for a malicious actor, or the U.S. government's use of an exploit might give adversaries the know-how to create new and more dangerous forms of malware.

1. Why It Exists

Offense bias is present on both sides of a transaction. On the supply side, many hackers would rather sell to the NSA than to defense-minded vendors or security companies. On the demand side, government buyers prefer to stockpile flaws for use against adversaries rather than alerting vendors.[190] Why? For hackers, it comes down to two factors: money and liability.

The gray market pays better than the white market—a lot better. A researcher on the gray market "could earn 10–100 times what a software vendor with a bug bounty would pay,"[191] and many understandably regard

[187] *Id.* at 4.

[188] Bambauer & Day, *supra* note 27, at 1101; *see also* Kesan & Hayes, *supra* note 16, at 801–02; Kuehn & Mueller, *supra* note 26, at 6.

[189] *See* MILLER, *supra* note 101, at 5.

[190] *See* Fidler, *supra* note 16, at 444.

[191] ABLON ET AL., *supra* note 23, at 26; *see also* Finifter et al., *supra* note 55, at 273; Menn, *supra* note 24.

white market rewards as "lame."[192] Consider the situation from a hacker's standpoint. You've just discovered a severe flaw in iOS; what are you going to do with it? One option is to alert Apple, but that probably means only token compensation. Or you could sell it to an independent security company like the Zero Day Initiative for $10,000 at best. Or you could call your buddy the Grugq and have him broker a deal with the NSA for half a million dollars. Selling to the government is a perfectly rational choice.

Why are white market bounties so small? Partly because of the depth of the players' respective pockets. The government simply has more resources than even the most established firms in the industry.[193] Externalities are an important part of the story as well.[194] As I argued in a companion piece, software vendors don't bear the full costs of flaws in their products and therefore have weaker incentives to fix them.[195] Nor is there an effective way to internalize users' costs onto the vendors. Tort lawsuits generally aren't an option, as the economic loss doctrine normally excuses defendants that cause freestanding economic injuries (as distinct from economic harms that result from physical harms).[196] Flaws are less costly to vendors, so vendors have less reason to reward the hackers who find them. Bounties thus tend to be modest because of the same incentives that produce vulnerabilities in the first place.

Hackers are also influenced by liability concerns. "[S]ome companies are more likely to sue a researcher who discovers a flaw than pay them."[197] Indeed, white hats face a substantial risk of criminal and civil liability under federal laws like the Computer Fraud and Abuse Act (CFAA) and the Digital Millennium

[192] Gallagher, *supra* note 113.

[193] *See* Bambauer, *supra* note 23, at 1081; Eichensehr, *supra* note 24, at 486–87; Schwartz, *supra* note 143.

[194] Bruce Schneier, *Debating Full Disclosure*, SCHNEIER ON SECURITY (Jan. 23, 2007, 6:45 AM), https://www.schneier.com/blog/archives/2007/01/debating_full_d.html [https://perma.cc/4DSS-PDVH] ("To a software company, vulnerabilities are largely an externality.").

[195] *See* Sales, *supra* note 15, at 1533–36.

[196] *Id.* at 1535. Of course, insecurity can have reputational costs. A company that earns a reputation for easily compromised products might see customers defect to competitors. But it's not clear that consumers give much weight to product security when making their purchasing decisions; many buy on price and features rather than security. JOEL BRENNER, AMERICA THE VULNERABLE 225–26 (2011); Bambauer & Day, *supra* note 27, at 1063; Frye, *supra* note 28 at 367. *But see* Doug Lichtman & Eric P. Posner, *Holding Internet Service Providers Accountable*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 256 (Mark F. Grady & Francesco Parisi eds., 2006); *see also* Coyne & Leeson, *supra* note 33, at 486–87.

[197] Kesan & Hayes, *supra* note 16, at 789; *see also* Bambauer & Day, *supra* note 27, at 1054; Matwyshyn, *supra* note 16, at 827–28; Oriola, *supra* note 37, at 485.

Copyright Act (DMCA). Hackers who sell to government buyers face no such risks but receive implicit assurances of immunity. Perversely, it can be more dangerous to help a vendor patch a bug than to help the government exploit it, and many hackers react accordingly.[198]

Security research, by definition, involves breaking into computers and probing them for weaknesses. And that can be risky. Hackers might find themselves charged under the CFAA, a sweeping 1986 statute that criminalizes various forms of unauthorized access to any "protected computer,"[199] which is broadly defined to include essentially any system connected to the internet.[200] Moreover, a hacker who wants to sell a bug will need to demonstrate to prospective buyers that the vulnerability is legitimate. That often will require creating a working exploit—code that takes advantage of the flaw to compromise the system—as a proof of concept.[201] The fact that the hacker had benign intentions in probing the system is no excuse.

Consider Brett McDanel, a researcher at a now-defunct internet messaging company called Tornado Systems.[202] In 2003, McDanel was convicted of a CFAA violation after he sent customers an email alerting them to a vulnerability in Tornado's webmail system. The government's theory was that McDanel had "knowingly cause[d] the transmission of a program, information, code, or command" that "intentionally cause[d] damage without authorization, to a protected computer."[203] What sort of damage? The government successfully argued that McDanel had harmed Tornado's system merely by telling customers about the flaw.[204] McDanel was jailed for nearly a year and a half before his conviction was overturned on appeal.[205] Or consider Andrew Auernheimer and Daniel Spitler, who publicized a flaw in AT&T's website that allowed anyone to access the personal information of more than 100,000

[198] Fidler, *supra* note 16, at 426–27.

[199] 18 U.S.C. § 1030(a) (2012); *see, e.g.*, Granick, *supra* note 36, at 21–22; Kirsch, *supra* note 69, at 386–87, 392–94; Oriola, *supra* note 37, at 497–99.

[200] *See* 18 U.S.C. § 1030(e)(2); Orin S. Kerr, *Criminal Law in Virtual Worlds*, 2008 U. CHI. LEGAL F. 415, 423; Kirsch, *supra* note 69, at 392; Golabek-Goldman, *supra* note 25, at 51. Even if prosecutors decline to bring criminal charges under the CFAA, hackers might face civil liability. The CFAA's private right of action allows any person to bring a civil action for compensatory damages and equitable relief if he has been harmed by various CFAA violations to the tune of at least $5000 in a year. *See* 18 U.S.C. § 1030(g); *see also id.* § 1030(c)(4)(A)(i)(I).

[201] Kesan & Hayes, *supra* note 16, at 802; *see* Granick, *supra* note 36, at 7; Kuehn & Mueller, *supra* note 26, at 3.

[202] Granick, *supra* note 36, at 21.

[203] 18 U.S.C. § 1030(a)(5)(A).

[204] Granick, *supra* note 36, at 21.

[205] *See id.*

subscribers with iPads.[206] They were convicted of violating the CFAA and sentenced to three and a half years in prison; the conviction was vacated on appeal because of improper venue.[207] The fact that both convictions were eventually overturned offers cold comfort to other white hats, who presumably would rather avoid the ordeal of investigation and trial altogether.

Another potential source of liability is intellectual property law, especially the Digital Millennium Copyright Act. The DMCA makes it a crime for any person to "circumvent a technological measure that effectively controls access to a [protected] work,"[208] and a company injured by such a violation may bring a civil action for money damages and equitable relief.[209] To be sure, the DMCA contains safe harbors that might seem to protect well-intentioned hackers, such as exemptions for "reverse engineering"[210] and "security testing."[211] But these exemptions "are so narrow that they are effectively useless."[212] Of nearly 150 DMCA cases decided through 2011, "only one involved a claim of protection under the security testing safe harbor, and in it the safe harbor was held inapplicable."[213] The other exemptions have proven no more helpful.[214] As Derek Bambauer and Oliver Day argue, "IP law—like the software it protects—malfunctions here"; it "stifles the dissemination of critical research on software security vulnerabilities."[215]

Mike Lynn is a cautionary tale. In 2005 the security researcher found a flaw in Cisco's widely used internet routers.[216] He alerted Cisco, but, alarmed that the company wasn't doing enough to push users to implement the patch it had issued, he decided to give a talk about the problem at a hacker conference. Cisco fired back with an IP lawsuit, and the court issued a restraining order that blocked Lynn from presenting his findings. "The company also forced conference organizers to rip the printed version of Lynn's slides out of the

[206] Kirsch, *supra* note 69, at 386–87.

[207] Kim Zetter, *Appeals Court Overturns Conviction of AT&T Hacker 'Weev'*, WIRED (Apr. 11, 2014, 1:12 PM), https://www.wired.com/2014/04/att-hacker-conviction-vacated/ [https://perma.cc/22F2-82SS].

[208] 17 U.S.C. § 1201(a)(1)(A); *see also id.* § 1204(a) (establishing criminal penalties for "willful[]" violations of section 1201).

[209] *See id.* § 1203.

[210] *Id.* § 1201(f).

[211] *Id.* § 1201(j).

[212] Bambauer & Day, *supra* note 27, at 1083.

[213] *Id.*

[214] *See id.*; *see also* Oriola, *supra* note 37, at 510 (discussing a "limited" exemption for encryption research).

[215] Bambauer & Day, *supra* note 27, at 1054; *see also* Granick, *supra* note 36, at 9; Oriola, *supra* note 37, at 507–11.

[216] *See* Bambauer & Day, *supra* note 27, at 1053–54.

conference materials, and to turn over CDs containing a copy of his slideshow."[217] Mike Lynn is far from alone. Two years earlier, the educational software company Blackboard filed a DMCA suit and obtained a court order barring a researcher from giving a presentation about flaws in the company's products.[218] In 2001, the Recording Industry Association of America threatened Ed Felten, a computer science professor at Princeton University, with a DMCA lawsuit to stop him "from publishing information about security flaws in a technological protection scheme for digital music."[219] Around the same time, Felten's student discovered a bug that allowed users to disable a copy protection tool for music CDs; the vendor rewarded him by threatening a DMCA lawsuit and referring the case to law enforcement.[220]

Hackers who sell to government buyers face a substantially lower risk of liability. This is not because the CFAA contains an express grant of immunity for sales to the government. The statute does include a carve out for authorized law enforcement and intelligence activities[221] but this safe harbor seemingly applies only to the government's own conduct, not that of its private sector partners.[222] Instead, gray hats receive a tacit assurance that prosecutors will look the other way; the Justice Department is simply not going to file criminal charges against a hacker from whom the NSA has just bought a bug.[223] The DMCA is more explicit. Its safe harbor immunizes not just government actors but any private citizen "acting pursuant to a contract with the United States,"[224] which presumably includes hackers who sell to the government. The government's decision to buy a bug on the gray market thus operates as a grant of immunity for the hacker's antecedent acts of researching the bug and developing proof-of-concept code to exploit it.

Of course, certain bug bounty programs make promises that seem to resemble the immunity the government offers. Facebook says that "we will not bring any lawsuit against you or ask law enforcement to investigate you," so long as "you give us reasonable time to respond to your report before making any information public, and make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service

[217] *Id.*
[218] *See* Oriola, *supra* note 37, at 511.
[219] Granick, *supra* note 36, at 9.
[220] *See* Bambauer & Day, *supra* note 27, at 1081–82.
[221] *See* 18 U.S.C. § 1030(f) (2012).
[222] *See* Fidler, *supra* note 16, at 426–27.
[223] *See id.*; Kesan & Hayes, *supra* note 16, at 82–83.
[224] 17 U.S.C. § 1201(e).

during your research."[225] PayPal makes a similar pledge.[226] But there may be less to these assurances than meets the eye. Many companies don't have bug bounty programs at all, let alone ones that expressly immunize the researchers who participate in them. Nor is it obvious that hackers would enjoy the safe harbors if they sold to outsiders like ZDI or VCP. Worst of all, these promises often contain glaring ambiguities about exactly what hackers must do to stay out of trouble. Take that statement from Facebook. Just what kind of "efforts" are needed to demonstrate one's "good faith"? If a hacker doesn't do enough—measured by some unknown standard—to avoid harming Facebook's systems, the social media giant could press charges. Or consider Google's program. The rules state that researchers may access "any Google-operated web service," elaborating that "this includes virtually all of the content."[227] "Virtually all" is not the same as "all," and Google does not explain what remains off-limits. "Legitimate researchers are not comforted by this lack of legal clarity."[228] Even with vendors' promises, hackers may conclude that the safest move is still to sell to the NSA.

It amounts to something like a tragedy of the commons.[229] When a hacker discovers a critical flaw, the socially optimal move often will be to tell the vendor, so it can be patched, and users can be protected from attacks that target the vulnerability. Yet many researchers choose to sell to the government, which stockpiles the flaws for future offensive uses, because they stand to profit handsomely. The result is that society remains vulnerable; security tends to be underproduced. What is rational for individual hackers ends up being irrational for society as a whole.[230]

What about the government? Why does it so often prefer offense to defense? This is only conjecture, but it might be due to an asymmetry between benefits and costs: Officials might calculate that the upsides of using a bug to attack an adversary are greater than the downsides of allowing Americans to remain vulnerable to the same flaw. In addition, the preference for offense may be due to cognitive failures, as officials underestimate the probability that an enemy might independently find a flaw and use it to attack the U.S.

[225] Kuehn & Mueller, *supra* note 26, at 11.

[226] *See* Kirsch, *supra* note 69, at 398.

[227] *Id.* at 397.

[228] Granick, *supra* note 36, at 20.

[229] *See* Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243 (1968).

[230] Charlie Miller wonders, rhetorically, "[d]o I do the thing that's good for the most people and not going to get me any money at all"—i.e., write a patch—"or do I sell it to the U.S. government and make $50,000?" Ball, *supra* note 25.

As for cost-benefit asymmetry, imagine the NSA's calculus when deciding whether to exploit a bug or fix it. In a previous work, I argued that national security officials typically seek to maximize their influence—their clout relative to that of their interagency rivals—and autonomy—their ability to pursue their individual and institutional priorities.[231] If the NSA uses a bug to destroy Iran's nuclear centrifuges, agency officials will receive the lion's share of the credit, and hence more influence and autonomy. The benefit to NSA officials of a successful offensive use thus will be quite high. By contrast, the cost to the NSA of leaving Americans exposed normally will be quite low. Officials might conclude that hostile powers are unlikely to find the same flaw, and even if they did there's no guarantee they would use it against the United States. If adversaries did discover the vulnerability and attack, the resulting blame likely would be dispersed among a large number of players. Responsibility for defending the nation's computer networks is divided among several players, such as the NSA, which defends military systems, and DHS, which is responsible for civilian agencies' networks,[232] as well as the private companies that control over 85 percent of this country's critical infrastructure.[233] Indeed, barring a leak, the public may never learn that the government was aware of the flaw and allowed it to persist. In short, NSA officials may calculate that they have more to gain from playing offense than they stand to lose from failing to play defense, and that asymmetry may bias them systematically in favor of hoarding bugs for future exploitation.[234]

The gray market thus produces another tragedy of the commons, this time on the demand side.[235] The socially optimal move often will be for the government to tell vendors about flaws so they can be fixed and users protected against intrusions.[236] But the benefits of using a bug to attack an adversary are concentrated on NSA officials, while the costs of failing to defend American systems are widely distributed. The system therefore tends to overproduce offense and underproduce defense.

Another possible explanation for offense bias is bounded rationality. Bounded rationality refers to the "inescapable limitations" of human

[231] *See* Nathan Alexander Sales, *Self-Restraint and National Security*, 6 J. NAT'L SEC. L.& POL'Y 227, 234–36 (2012).

[232] *See* Jack Goldsmith, *The NSA's Growing Role in Domestic Cybersecurity*, LAWFARE (Oct. 21, 2010, 9:57 AM), https://www.lawfareblog.com/nsas-growing-role-domestic-cybersecurity [https://perma.cc/H2FA-B3SE].

[233] *See* Nojeim, *supra* note 57, at 135; *see also* ROSENZWEIG, *supra* note 33, at 2.

[234] *See* Anderson, *supra* note 38, at 5.

[235] *See supra* notes 229–230 and accompanying text.

[236] *See* Kesan & Hayes, *supra* note 16, at 820.

"knowledge and computational ability."[237] One common cognitive failure is overoptimism. We tend to underestimate the likelihood that we will experience an unfavorable result in a given situation.[238] A related problem is salience. We sometimes overestimate the probability of highly salient outcomes—those that, because of their vividness, are available to us—and we correspondingly discount the probability of less salient outcomes.[239] "When overoptimism is combined with salience, people may underestimate risks substantially."[240]

These sorts of cognitive shortcomings may help explain the government's preference for offense over defense. The highly salient Stuxnet episode might cause officials to overestimate the chances that an attack on enemy systems will succeed. On the other hand, overoptimism and availability might lead them to downplay the risks of allowing a known flaw to go unpatched. Officials certainly are aware of the catastrophic harms the nation could experience from a cyberattack; they've been hearing about "an electronic Pearl Harbor" for years.[241] But they may be underestimating the probability that a flaw they've acquired might be independently discovered by an adversary and exploited to devastating effect in the United States. That scenario may not be very salient because, as far as we know, it has never occurred, but the chances of rediscovery are in fact very far from nonexistent.[242] Or maybe officials are miscalculating the likelihood that they would be held responsible if an adversary exploited a flaw they knew about. Perhaps overoptimism leads them to conclude that the public is unlikely to ever learn of their decision to hoard a bug when, in an era of massive Snowden- and Manning-style leaks, such a revelation would be reasonably likely. In other words, offense may well be a worse choice than defense—not just for society as a whole, but for the officials themselves—yet cognitive constraints lead them to hoard bugs.[243]

[237] GRAHAM ALLISON & PHILIP ZELIKOW, ESSENCE OF DECISION: EXPLAINING THE CUBAN MISSILE CRISIS 20 (2d ed. 1999); *see* HERBERT A. SIMON, ADMINISTRATIVE BEHAVIOR 120–22 (4th ed. 1997).

[238] *See* Christine Jolls et al., *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471, 1524 (1998).

[239] *See id.* at 1519.

[240] *Id.* at 1542.

[241] Richard Clarke, *Threats to U.S. National Security: Proposed Partnership Initiatives Towards Preventing Cyber Terrorist Attacks*, 12 DEPAUL BUS. L.J. 33, 38 (1999).

[242] *See supra* note 55.

[243] *See* Sales, *supra* note 231, at 271 n.197.

2. Why It's a Problem

Why does it matter that so many hackers are selling to the government? For at least three reasons: First, the risk to ordinary users. When the NSA acquires a bug, Americans remain vulnerable to attacks by adversaries who might have discovered the same flaw. Second, proliferation. The government's participation in the gray market makes it more likely that bad actors will get their hands on dangerous cyberweapons. And third, brain drain. Highly capable hackers are migrating to the gray market, leaving less skilled counterparts responsible for the essential task of reporting bugs to vendors.

The first and most important problem is that ordinary users remain exposed to a given vulnerability for as long as the government holds it for offensive use. Governments that "sit[] on flaws" are effectively "exposing their own citizens to espionage."[244] Indeed, the government has a perverse interest in its people remaining vulnerable; if Americans fix their systems, chances are that our enemies will too.[245] In this respect, zero-days are unique. In realspace, offensive weapons normally coexist with defensive countermeasures; offense and defense are complements rather than substitutes. American M16s will still draw blood even if the soldiers who fire them are wearing body armor. Not so with zero-days. They are effective only because—and only insofar as—the civilian population remains vulnerable. Eliminating the vulnerability eliminates the weapon.[246]

Second, the thriving gray market creates opportunities for proliferation; potent cyberweapons could fall into the wrong hands. Some gray market players have no scruples about the buyers they work with and might sell directly to a hostile power. Recall the broker who sees no "good guys or bad guys. It's just business."[247] There may not be many companies willing to sell to the likes of China and Russia, but that silver cloud has its own dark lining. Because of the lack of suppliers, "those countries likely must pay a price premium for

[244] Gallagher, *supra* note 113 (quoting Chris Soghoian); *see also* Eichensehr, *supra* note 24, at 48; Fidler, *supra* note 16, at 410–11; Kesan & Hayes, *supra* note 16, at 757; Richard Clarke & Peter Swire, *The NSA Shouldn't Stockpile Web Glitches*, DAILY BEAST (Apr. 18, 2014, 5:45 AM) https://www.thedailybeast.com/the-nsa-shouldnt-stockpile-web-glitches [https://perma.cc/3V4U-G6QT].

[245] Menn, *supra* note 24; Schneier, *supra* note 55.

[246] Cybersecurity expert Rich Mogull argues that, with zero-days, "your offensive capability is predicated on keeping the population vulnerable. . . . I don't know of any other weapons that become worthless if the population becomes any better at defending themselves." Ball, *supra* note 25; *see also* Lemos, *supra* note 69.

[247] Gjelten, *supra* note 109.

access, making them attractive customers."[248] Other gray market players restrict themselves, to a greater or lesser extent, from doing business in shady countries,[249] but these self-imposed limits can be evaded fairly easily. A number of unsavory states remain eligible buyers under some brokers' policies. These states might serve as second-order brokers for outlaw regimes that can't participate in the market directly, like Iran, North Korea, or Syria.[250] Or blacklisted countries could buy bugs by commissioning seemingly legitimate private firms to serve as proxies.[251]

There are anecdotal reports that this proliferation is already happening. In 2011, the *Wall Street Journal* revealed that Syria was able to acquire thirteen internet filtering devices manufactured by a U.S. company, which it used to block or monitor thousands of "attempts to connect to websites run by opposition figures or devoted to covering the Syrian uprising," as well as visits to social networking sites like the "Syrian Revolution" page on Facebook.[252] The devices were sent to a Dubai-based distributor, which was supposed to deliver them to Iraq's Ministry of Communications. But the filters somehow ended up in Syria, even though the country has been subject to strict U.S. and international sanctions since 2004. In all, up to twenty-five such filters "have made their way into Syria since the mid–2000s, with most sold through Dubai-based middlemen."[253] The same thing easily could happen with exploit code.

The gray market also creates opportunities for the proliferation of sophisticated hacking techniques and technological capabilities. When the U.S. government introduces an exploit "into the wild," as the phrase goes, adversaries can study and learn from it.[254] They might use their newfound knowledge to better secure their systems against intrusion, making it harder for the U.S. to compromise them in the future. Even worse, they might develop sophisticated malware of their own and use it against the U.S. The danger is especially great for enemies that presently lack extensive cyber capabilities, like small states and terrorist groups.[255] In short, the government's active role in the

[248] Bambauer, *supra* note 23, at 1082.

[249] *See supra* notes 163–165 and accompanying text.

[250] *See* Bambauer, *supra* note 23, at 1082; Stockton & Golabek-Goldman, *supra* note 109, at 251.

[251] *See* Fidler, *supra* note 16, at 411–12; *see also* FREI & ARTES, *supra* note 41, at 8.

[252] Jennifer Valentino-DeVries et al., *U.S. Firm Acknowledges Syria Uses Its Gear to Block Web*, WALL ST. J. (Oct. 29, 2011), https://www.wsj.com/articles/SB10001424052970203687504577001911398596328.

[253] *Id.*

[254] Zetter, *supra* note 45.

[255] *See* Fidler, *supra* note 16, at 412; *cf.* Golabek-Goldman, *supra* note 25, at 10, 15 (noting that a particularly alarming aspect of this market is that it may enable terrorist organizations like al-Qaeda to make the requisite technological lead to wage "electronic jihad").

gray market is "bankrolling dangerous R&D" for criminals, terrorists, and rogue states.[256] We are effectively subsidizing our enemies.

Again, anecdotal evidence suggests that capability proliferation is already underway. In 2011, researchers discovered a new bug called "Duqu," which "tricked computers into installing malicious software disguised as a font to render type on the screen."[257] Apparently designed to steal sensitive information, Duqu had a number of similarities to Stuxnet and some observers speculated that it too might have been the handiwork of the U.S. government.[258] What's clear is that it taught black hats a great deal. "[C]riminal hackers copied Duqu's previously unheard-of method for breaking into computers and rolled it into 'exploit kits' . . . that were sold to hackers worldwide."[259] The vulnerability became the second most exploited known flaw in the last half of 2012, and attackers used it to infect computers with a wide range of malware including "Zeus, a notorious program for stealing financial login information that has been blamed for hundreds of millions of dollars in bank thefts."[260]

A third problem is brain drain. The gray market is luring hackers who otherwise might have shared their discoveries with software vendors.[261] This trend seems especially pronounced for the most capable hackers: The researchers whose skills enable them to uncover the most serious flaws are the ones who increasingly are demanding—and receiving—generous compensation.[262] The researchers who are left behind in the white market tend to be the ones with relatively modest skills. The result of this sorting is that the most severe flaws are increasingly likely to be found by gray hats and sold to the government for offense.

This is not to suggest that it's always bad for the government to exploit a vulnerability or that it should share every bug with vendors. Sometimes it will be appropriate to play offense—especially where a secretive zero-day can substitute for overt, lethal force. It's better to destroy Iran's nuclear centrifuges with a bug than a bomb. Moreover, prohibiting all offensive uses of zero-days would leave the U.S. at a disadvantage, as our adversaries are developing these

[256] *The Digital Arms Trade*, ECONOMIST (Mar. 30, 2013), https://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade [https://perma.cc/E3RB-NCKQ].

[257] Menn, *supra* note 24.

[258] *See id.*

[259] *Id.*

[260] *Id.*

[261] *See* Fidler, *supra* note 16, at 434; Menn, *supra* note 24.

[262] *See supra* notes 108–112 and accompanying text.

cyberweapons "on a massive scale."[263] Quitting the gray market altogether would amount to unilateral disarmament. The thorny question of how, for any given vulnerability, the government should balance its need for effective cyberweapons against its obligation to protect its citizens is beyond the scope of this Article. My more modest objective here is to fault the current bias in favor of offense while acknowledging that it may be appropriate in some (undefined) circumstances to acquire vulnerabilities for offensive operations.

III. WHY REGULATORY SOLUTIONS ARE INSUFFICIENT

Lawmakers and scholars alike have largely ignored the gray market. Bug sales to government agencies are essentially unregulated,[264] and the few scholars to address the issue have tended to propose the same sorts of regulatory solutions that are common to cybersecurity literature in general. One rare exception is the innovative proposal from Jay Kesan and Carol Hayes to use financial instruments such as derivatives to foster a legitimate vulnerabilities market.[265] But their market-based approach is very much an outlier. Regulation is indeed an essential part of the response to cyber insecurity, but regulatory solutions by themselves are insufficient. It's also necessary to get the incentives right.[266] Policymakers must correct the perverse incentives that lead hackers to sell flaws to government agencies that will exploit them instead of vendors that can patch them. In short, regulatory responses must be supplemented with market-based responses.[267]

This is not the place for an exhaustive review of the literature. But a few thoughts about the limits of the most prominent regulatory proposals are in order. Some scholars see bug sales as a problem for law enforcement. Paul Stockton and Michele Golabek-Goldman urge lawmakers to extend the CFAA's jurisdictional reach to vulnerability sales outside the United States.[268] Extraterritorial application of the CFAA would "enable prosecutions of vulnerability research firms located in the gray market abroad, such as the European-headquartered Vupen and ReVuln."[269] In a separate work, Golabek-Goldman argues that Congress should expand the CFAA's substantive scope by

[263] Greenberg, *supra* note 77.

[264] Gallagher, *supra* note 113; Oriola, *supra* note 37, at 512.

[265] *See* Kesan & Hayes, *supra* note 16.

[266] *See* Lawrence A. Gordon et al., *Sharing Information on Computer Systems Security: An Economic Analysis*, 22 J. ACCT. & PUB. POL'Y 461, 463–64 (2003).

[267] *See, e.g.*, Kesan & Hayes, *supra* note 16, at 759.

[268] *See* Stockton & Golabek-Goldman, *supra* note 109, at 260–64.

[269] *Id.* at 263.

"impos[ing] an affirmative duty on [zero-day] sellers to 'know their customers' or only sell to [approved] entities."[270] Hackers would be criminally liable if they could not "demonstrate that they 'reasonably investigated' the purchaser's background and had 'reasonable grounds to believe' that the purchaser would not exploit the [zero-day] for malicious cyber activities."[271]

Criminal law is certainly an important part of the conversation but overreliance on it could have a number of harmful effects. A new CFAA duty to investigate could chill legitimate research into cyber vulnerabilities.[272] White hats might decide that hunting for bugs is no longer worth the risk. A related concern is that ramping up prosecution could raise First Amendment problems.[273] White hats who report their discoveries to vendors or the public are engaging in constitutionally protected expression.[274] And while the First Amendment may not shield a hacker's antecedent research and testing—such steps probably would be deemed punishable conduct rather than protected speech—a prosecution for the disclosure itself would be much more problematic. Chilling this sort of "vulnerability speech" could be disastrous.[275]

Scholars also have proposed regulating bug exports. The gray market is global in scope, with hackers around the world partnering with intermediaries based in Europe (like Vupen in France and ReVuln in Malta) and Asia (such as the Grugq) to sell their discoveries to government agencies in the United States and elsewhere. Regulating the movement of bugs across borders therefore has intuitive appeal. So, for instance, Mailyn Fidler argues that the best international approach is "voluntary collective action to harmonize export controls on zero-days through the Wassenaar Arrangement."[276] Wassenaar, established in 1996, is a mechanism for participating countries—there are currently forty-one, mostly in North America and Europe[277]—to coordinate restrictions on the export of conventional weapons as well as dual-use goods.[278]

[270] Golabek-Goldman, *supra* note 25, at 52.

[271] *Id.*

[272] *See* Kesan & Hayes, *supra* note 16, at 771–72; Matwyshyn, *supra* note 16, at 840.

[273] Fidler, *supra* note 16, at 431–32; Kesan & Hayes, *supra* note 16, at 796–99. *See generally* Matwyshyn, *supra* note 16 (proposing a framework for evaluating when "vulnerability speech" by hackers should enjoy First Amendment protection).

[274] *See, e.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 445 (2d Cir. 2001).

[275] *See, e.g.*, Matwyshyn, *supra* note 16, at 817.

[276] Fidler, *supra* note 16, at 408; Golabek-Goldman, *supra* note 25, at 5–6; *see also* Stockton & Golabek-Goldman, *supra* note 109, at 243.

[277] *See The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, WASSENAR (May 8, 2017), http://www.wassenaar.org/ participating-states [https://perma.cc/8LBJ-VUVL].

[278] *See* Fidler, *supra* note 16, at 463.

Wassenaar is especially well suited to addressing bugs, Fidler argues, because "a wide swath of actors" already participate, it would not require "significant institutional change," and it is "a flexible mechanism" that would allow "international coordination without making unrealistic demands of participants."[279]

How likely is it that Wassenaar countries would agree to restrict exports of vulnerabilities and exploits? One readily can imagine them adopting common export controls on black market sales. But cracking down on the gray market would require them to crack down on their best friends—and themselves. The U.S. government reportedly buys bugs from suppliers in NATO countries and other allies that are part of the Wassenaar Arrangement—France and Malta, and perhaps others as well. Presumably the U.S. wants to maintain its access to those markets, and other Wassenaar countries that are active on the gray market seemingly would have the same interest. It is difficult to imagine these governments agreeing to export controls that would frustrate their shared interest in maintaining access to each others' markets.

Nor is it clear that restricting exports would be terribly effective. Even if Wassenaar countries did agree to harmonize their controls on exporting bugs, it may not make much difference. If France and Malta block the U.S. government from working with Vupen and ReVuln, the U.S. isn't going to stop acquiring bugs.[280] It will simply shift its purchases to domestic suppliers like Lockheed Martin, Raytheon, and other defense contractors that reportedly are rushing to enter the lucrative trade.[281] Or the U.S. will find new suppliers in countries that have not restricted exports—like the Grugq's home base of Thailand, which is not part of Wassenaar. Or the U.S. could stop outsourcing much of its vulnerabilities research and bring its R&D operations entirely in-house.[282] Bug hunters likewise might defeat any new export controls by relocating to countries with more permissive policies.

Even worse, if export controls were effective, they could end up harming the U.S. and its allies more than they help. These restrictions would disadvantage Western nations, which acquire many bugs from private researchers, including hackers located in other countries. But they would have no effect on unfriendly governments that do most of their vulnerabilities

[279] *Id.* at 471.

[280] *Cf. id.* at 437 ("[E]xport controls would not address concerns about U.S. government purchasing and use of zero-days.").

[281] *See supra* notes 157–161 and accompanying text.

[282] *Cf.* Kesan & Hayes, *supra* note 16, at 761 (noting that, with a smaller number of suppliers, "governments will have to move their vulnerability discovery operations in-house").

research internally or buy from domestic researchers. China, North Korea, and Russia come to mind. Export controls thus could impose asymmetric burdens. The U.S. and other Western states would find their access to bugs curtailed while their adversaries continued to develop advanced cyberweapons unimpeded.

A third approach favored by scholars—and by the government itself—is a more robust executive branch decisionmaking process, along with increased transparency and oversight. The President's Review Group on Intelligence and Communications Technologies, a team of scholars and intelligence experts, recommends that the government should stockpile vulnerabilities only in "rare" circumstances, "following senior, interagency review involving all appropriate departments."[283] Former White House official Richard Clarke and law professor Peter Swire, both members of the Review Group, similarly recommend an interagency process in which the White House is responsible for making the call to exploit or disclose "after having heard from all sides of the issue."[284] Fidler likewise argues that "increased executive branch oversight is the best domestic strategy" for preventing excessive offensive uses of zero-days.[285]

Policymakers apparently were listening. In 2014, the *New York Times* reported that "President Obama has decided that when the National Security Agency discovers major flaws in Internet security, it should—in most circumstances—reveal them to assure that they will be fixed, rather than keep mum so that the flaws can be used in espionage or cyberattacks."[286] The White House's Cybersecurity Coordinator later elaborated that the government weighs a number of factors when deciding whether to exploit a bug or tell vendors, including whether the vulnerability affects "core Internet infrastructure," how much harm an adversary could cause by exploiting it, the value of the intelligence the U.S. stands to gain, and so on.[287]

It remains to be seen, however, whether transparency and oversight will actually lead to more patches. The government's policy is riddled with loopholes that could preserve its ability to keep bugs for offensive use. First,

[283] RICHARD A. CLARKE ET AL., PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY & SECURITY IN A CHANGING WORLD 219 (2013).

[284] Clarke & Swire, *supra* note 244.

[285] Fidler, *supra* note 16, at 408.

[286] David E. Sanger, *Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say*, N.Y. TIMES (Apr. 12, 2014), https://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html.

[287] Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, WHITE HOUSE (Apr. 28, 2014, 3:00 PM), https://www.whitehouse.gov/blog/2014/04/28/ heartbleed-understanding-when-we-disclose-cyber-vulnerabilities [https://perma.cc/6RFB-MFQ4].

President Obama's decision applies to vulnerabilities that the NSA "discovers."[288] Presumably that means bugs the NSA has found in-house. No mention is made of vulnerabilities obtained from outside vendors, in which case the government would remain free to exploit bugs bought on the gray market, essentially without limit.[289] Second, the policy applies only to "major flaws in Internet security."[290] The implication is that, if a particular vulnerability is deemed to be minor, the default would be for the NSA to stockpile it.[291] The third loophole may be the most permissive of all: The government will disclose flaws to vendors "in most circumstances."[292] Thus, there will continue to be situations in which the government need not disclose even major vulnerabilities,[293] and officials seemingly will enjoy broad discretion when deciding whether offense is warranted. No wonder Microsoft's Scott Charney has characterized the government's new approach as "a policy of 'We'll share unless we don't.'"[294]

More fundamentally, transparency and oversight might not correct the internal dynamics that may naturally predispose officials to exploit flaws rather than fix them—cost-benefit asymmetries and cognitive shortcomings.[295] A more inclusive interagency process could in theory weaken this bias by diluting the voices of offense-minded players with the presence of defenders. The NSA traditionally has played the leading role when deciding whether to use a bug for attacking or defending. Clarke, a former cybersecurity czar, recalls that "[t]here is supposed to be some mechanism for deciding how they use the information, for offense or defense. But there isn't."[296] It's possible that other agencies might weigh the relative merits of offense and defense differently. DHS in particular comes to mind, as it has the Herculean responsibility of defending the government's civilian networks and also is the government's regulatory interface for many critical industries that might face cyberattacks. Officials at

[288] Sanger, *supra* note 286.

[289] *See* Fidler, *supra* note 16, at 448.

[290] Sanger, *supra* note 286.

[291] Jack Goldsmith, *More on USG Policy on Cyber Vulnerabilities*, LAWFARE (Apr. 12, 2014, 9:04 PM), https://www.lawfareblog.com/more-usg-policy-cyber-vulnerabilities [https://perma.cc/7U7P-X8SN].

[292] Sanger, *supra* note 286.

[293] *See* Goldsmith, *supra* note 291.

[294] Fidler, *supra* note 16, at 449; *see also* Schwartz, *supra* note 143.

[295] *See supra* notes 231–243 and accompanying text.

[296] Andrea Peterson, *Why Everyone Is Left Less Secure When the NSA Doesn't Help Fix Security Flaws*, WASH. POST (Oct. 4, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws/?utm_term=.b9ea732288ce [https://perma.cc/VVA2-B5RG].

DHS might calculate that they would bear a disproportionate share of the blame if foreign powers independently discovered a flaw and used it to attack the U.S. Giving defenders a seat at the decisionmaking table would enable contrarian perspectives to be aired, though it's hard to say how clearly their voice would register amid the din from the many offense-minded agencies like the NSA, CIA, FBI, and so on. Offense may continue to trump defense.

IV. TOWARD A MORE ROBUST WHITE MARKET

None of this is to suggest that regulatory approaches are useless. Criminal law, export controls, and oversight are important tools in the overall kit of responses to software vulnerabilities. But regulation by itself is insufficient. Complementary market-oriented solutions are needed to incentivize hackers to sell bugs on the white market to vendors who will patch them rather than to governments and criminals who plan to exploit them.[297] In particular, policymakers should establish legitimate vulnerability brokers and increase the payouts offered to white hat hackers; the former will reduce transaction costs, enabling more legitimate sales to take place, while the latter will lure researchers away from the internet's shadier corners.

A credible white market thus can trigger a virtuous cycle that improves product security and helps shrink its shadier counterparts. More hackers selling to vendors increases the chances that dangerous flaws will be found and patched.[298] That will tend to depress the prices on the gray and black markets, because vulnerabilities are highly perishable.[299] From an attacker's perspective, a vulnerability is only useful if targets haven't patched it, and as the odds increase that white hats will find a given flaw, its value will decline—and so will the price the attacker is willing to pay.[300] Price drops will make the white market still more attractive relative to the gray and the black, drawing even more researchers, which in turn further increases the chances that bugs will be found and fixed before they can be exploited. And so on.

[297] *See* Böhme, *supra* note 22, at 306–09; Kesan & Hayes, *supra* note 16, at 759, 805; Radianti, *supra* note 115, at 3.

[298] *See* FREI & ARTES, *supra* note 41, at 14; Ozment, *supra* note 17, at 19.

[299] *See* Bambauer & Day, *supra* note 27, at 1101; Kesan & Hayes, *supra* note 16, at 760–61; *see also* MILLER, *supra* note 101, at 2–3.

[300] *See* Kesan & Hayes, *supra* note 16, at 794–95.

A. Establishing White Market Brokers

The need for a vulnerabilities broker is not an original idea. Many scholars have called for a "trusted third party" to facilitate exchanges of cybersecurity information,[301] and the gray and black markets already have functioning go-betweens. Yet there is almost no sustained analysis in the academic literature of how white market go-betweens would operate or the benefits they would produce.[302] This Article begins to fill that gap. In short, brokers would perform the vital functions of connecting buyers with sellers, verifying the parties' good faith, overcoming information asymmetries, assisting the parties in negotiating a sale price, and publicizing information about completed transactions. Brokers thus would help reduce the cripplingly high transaction costs that plague white market sales, enabling more transactions to take place and more flaws to be patched.

1. The Basics

A cybersecurity broker's most basic function would be to connect sellers with buyers. The process would begin on the hacker's side. At least initially, most white hats probably will be individuals, as is currently the case. But as the market matures, white hats might organize themselves into firms to take advantage of economies of scale. (Similar consolidation reportedly is taking place in the black market.[303]) When a researcher finds a new vulnerability, he would alert a broker, which likewise could be an individual or a firm. Presumably he will want to begin the process as soon as the flaw is discovered, rather than sitting on it in hope of a higher price in the future. There is always a risk that someone else will find the same bug and sell it first, in which case one's discovery will become worthless.[304]

The broker would then verify the hacker's bona fides, ensuring that he isn't an extortionist or otherwise unreliable. Repeat players with established reputations will require only perfunctory screening. But for unknown hackers, brokers will have strong incentives to develop reliable mechanisms to screen out illegitimate sellers. This is a matter of self-preservation. A broker that approaches a buyer is effectively vouching for the hacker's good faith, and if too

[301] *See, e.g.*, Bambauer & Day, *supra* note 27, at 1056; Ozment, *supra* note 17, at 4; *see also, e.g.*, ROSENZWEIG, *supra* note 33, at 18–19; Kannan & Telang, *supra* note 73, at 1.

[302] *But see* Bambauer & Day, *supra* note 27, at 1101–03.

[303] ABLON ET AL., *supra* note 23, at 4–5.

[304] *See supra* notes 55, 299.

many turn out to be scammers, then vendors will stop working with it. Any number of measures could be used to identify bad apples. Perhaps hackers could undergo background checks. Or perhaps brokers could require them to pay something like an earnest money deposit that they would forfeit if they turn out to be scammers. At the same time, the broker would assess the flaw's severity and thus its likely market value.[305] Again, this quality control is a matter of self-preservation. If a broker repeatedly offers low-quality goods—if it characterizes flaws as critical but they turn out to be minor—it will develop a poor reputation and buyers will stop working with it. Brokers therefore will have a strong incentive to make accurate assessments, which means they will need to develop the technical expertise those assessments require.

After completing its review, the broker would reach out to potential buyers. Of course, the vendor of the flawed product will be the obvious candidate, but as described below, independent security companies might bid too.[306] This will help mitigate substantial transaction costs on both sides of the ledger,[307] including seller search costs. Rookie hackers who are trying to sell for the first time may not know whom at a particular company to contact—especially when the vendor has no bug bounty program. By contrast, brokers will be veterans of numerous deals and can route a seller's offer to the appropriate decisionmakers.[308] Brokers also would reduce buyers' verification costs. Because the broker would be a known quantity from previous transactions—in which it presumably cultivated a reputation for reliability and fair dealing—there will be less need for buyers to exhaustively verify that the hacker is acting in good faith.[309]

Second, brokers would help negotiate a sale price that reflects the bug's importance—taking into account, among other factors, the probability that an adversary would discover the flaw, the degree of control that could be gained over a compromised system, the harm that could be done if the vulnerability is exploited, the cost of patching the flaw or remediating the damage, and so on.[310] A broker's status as a trusted player and its experience with past deals will help the parties come closer to a shared understanding of the flaw's severity and hence its fair market value.[311]

[305] Kesan & Hayes, *supra* note 16, at 826; Ozment, *supra* note 17, at 4.

[306] *See infra* Part IV.A.3.

[307] *See supra* notes 169–174 and accompanying text.

[308] Bambauer & Day, *supra* note 27, at 1102; *see also* MILLER, *supra* note 101, at 7.

[309] Bambauer & Day, *supra* note 27, at 1102.

[310] *See* BÖHME, *supra* note 18, at 3; Camp & Wolfram, *supra* note 19, at 25; Kesan & Hayes, *supra* note 16, at 810.

[311] Kesan & Hayes, *supra* note 16, at 59.

Even more importantly, brokers can overcome the significant pricing problems that result from information asymmetries between hackers and vendors. Akerlof's lemon market suggests that, because the hacker will know more about the flaw, the vendor will bid the sale price down to reflect the risk that the report is fraudulent.[312] But a broker can credibly assure the buyer that the information is indeed valuable—that the vendor isn't buying a lemon. Similarly, under the Arrow information paradox, a hacker must choose saying very little about the find, in which case the buyer might not believe that the flaw is legitimate, or revealing a great deal, in which case the buyer would obtain the information without payment.[313] But because the hacker would demonstrate his discovery to the broker, the broker would be able to verify quality and then vouch for the flaw in a way that would not destroy its economic value.[314] Brokers thus would not only reduce transaction costs, they also would bolster white market prices, helping to lure researchers away from selling to governments and criminals.

Third, at some point after the parties reach an agreement, brokers would publicize the sale price and other details about the transaction.[315] The vulnerabilities market lacks price transparency.[316] Buyers typically decline to reveal the bounties they've paid for particular discoveries and many require hackers to sign nondisclosure agreements. Today's buyers and sellers thus lack information about yesterday's deals that could shed light on the fair market value of a newly discovered flaw.[317] Revealing information about bug sales would inform future negotiations between buyers and sellers. The specific information to be made public will vary from bug to bug. At a minimum, brokers should announce the sale price as well as a general summary of the flaw, including the affected product and what an intruder could do to a compromised system. In some circumstances, it might also be advisable to reveal technical details, so other vendors and users can be on the lookout for similar flaws in their own products. But complete transparency could help malicious hackers, who

[312] *See supra* notes 179–181 and accompanying text.

[313] *See supra* notes 182–188 and accompanying text.

[314] Bambauer & Day, *supra* note 27, at 1101–02; Kesan & Hayes, *supra* note 16, at 59.

[315] *Cf.* Bambauer, *supra* note 23, at 1084 (arguing that policymakers should mandate "confidential reporting on transactions by firms in [vulnerability] markets").

[316] *See* Anderson & Moore, *supra* note 55, at 612; *see also* MILLER, *supra* note 101, at 3.

[317] Vendors may well object to brokers publicizing information about bug sales that currently is kept under wraps. But their heartburn might be lessened if the government supplements the rewards offered by vendors with bounty payments of its own. A portion of these payments would amount to a government subsidy for the vendor's efforts to test for flaws in its own products. *See infra* notes 372–373 and accompanying text.

might use it to create even more damaging malware. It could be Duqu redux.[318] In those situations, the price and a basic summary will have to suffice, though the complete technical details might be shared with a preapproved group of vendors that could be trusted not to give the information to bad actors.

2. Complications

While brokers would bolster the white market, there remain a number of complicated questions about whether cybersecurity brokers should be profit-seeking companies or nonprofits, whether there should be a single intermediary or multiples, and practical matters such as how to create and fund brokers.

My sense is that brokers should operate as for-profit entities, which cuts against the conventional wisdom. Most scholars favor an intermediary that is either operated by the government or organized as a government-backed nonprofit. Paul Rosenzweig proposes "a Congressionally chartered, non-profit corporation" that would "administer the creation and use of . . . information about cyber threats."[319] Karthik Kannan and Rahul Telang likewise argue that a "Federally-Funded Social Planner" is preferable because of the risk that a private company might leak information about bugs to make its products more attractive.[320] Yet these perspectives discount the important work of the profit motive. Companies have strong incentives to satisfy their customers. If they don't, they go out of business.[321] The profit motive thus functions as a sort of accountability mechanism—a mechanism to which the public sector is not subject. Government entities don't face the same existential risk. If they fail, Congress isn't going to abolish them; it may not even cut their budgets.

In the specific context of bug sales, the profit motive would incentivize brokers to accurately assess the value of flaws and develop the technical expertise required to do so. If a broker consistently overestimates severity, it will lose credibility and vendors will stop working with it. If a broker consistently underestimates severity, hackers will be disappointed in their payouts and seek out rivals capable of getting better deals. Similarly, private go-betweens will have strong incentives to secure their systems against

[318] *See supra* notes 257–260 and accompanying text.

[319] ROSENZWEIG, *supra* note 33, at 18; *see also* L. Jean Camp, *The State of Economics of Information Security*, 2 ISJLP 189, 194 (2006); Kesan & Hayes, *supra* note 16, at 821.

[320] Kannan & Telang, *supra* note 73, at 1, 10–11. I respond to this concern *infra* Part IV.A.3.

[321] *See* Calkins, *supra* note 27, at 198; Powell, *supra* note 58, at 505.

intruders. Brokers will "present attractive targets for hacking and espionage."[322] Individuals might steal bugs from their databases and sell them, while criminals might hack them in search of new flaws to target. These sorts of intrusions would devastate a broker's reputation—and therefore profits. White hats won't work with an intermediary that can't guarantee the security of the flaws they've brought to it; breaches would allow others to profit from their discoveries. Private brokers thus are subject to a feedback mechanism in the form of profits and losses that will spur them to take appropriate precautions against cyberattacks. Nonprofits lack the same incentives.

The next feature of the market has already been telegraphed: There should be multiple brokers competing against one another, not just a single intermediary. This too is counter to the scholarly consensus, as commentators generally favor a centralized storehouse for cybersecurity information.[323] For instance, Bambauer and Day propose "a voluntary intermediary" that would connect hackers with vendors,[324] and Kesan and Hayes call for a single "Information Security Clearinghouse" that would replace existing quasi-brokers like ZDI and VCP.[325] Yet a market with rival brokers offers a number of distinct advantages.

The most basic reason to prefer multiple firms over a single intermediary is competition, which incentivizes brokers to accurately assess bug severity, protect their systems, and otherwise perform well on pain of bankruptcy. Competition also can increase the size of the bounties hackers receive. Researchers will be able to shop their discoveries around, choosing the intermediary that seems most likely to get them the biggest payout. For their part, brokers will want to deliver the highest possible bounties for fear of their clients defecting to rivals with better track records. In addition, competing brokers would allow for specialization. Some might specialize in deals involving Microsoft Windows, others might focus on vulnerabilities in Google products, and so on. If a broker develops a comparative advantage at

[322] Bambauer, *supra* note 23, at 1083.

[323] One exception is Frei and Artes's proposal for an "International Vulnerability Purchase Program" that would "employ[] an organizational structure with multiple entities at each tier." FREI & ARTES, *supra* note 41, at 17.

[324] Bambauer & Day, *supra* note 27, at 1056. *But see id.* at 1101–02 (summarizing the existing entities that could serve as "intermediaries," plural).

[325] Kesan & Hayes, *supra* note 16, at 760–62, 817–18; *see also* Antone Gonsalves, *Good Guys Should Compete With Criminals in Buying Zero-Day Vulnerabilities, Report Says*, CSO ONLINE (Dec. 17, 2013, 7:00 AM), https://www.csoonline.com/article/2134242/malware-cybercrime/good-guys-should-compete-with-criminals-in-buying-zero-day-vulnerabilities—repor.html [https://perma.cc/7R5C-AHXC] (touting "a centralized vulnerability purchasing program").

assessing flaws in particular products, it will be able to facilitate deals involving those products more cheaply than its rivals. Broker specialization thus can further decrease the market's transaction costs. The resulting savings might be passed on to hackers in the form of larger payments, helping to make the white market more attractive. Lower transaction costs also would make the overall system more efficient—more bugs will be found and patched at a lower cost.

Another advantage is that multiple brokers would avoid the "Fort Knox" problem. Rosenzweig warns that "by creating a single focal point for cybersecurity efforts we risk creating a cyber Fort Knox: an attractive, high-value target of opportunity whose compromise would be catastrophic."[326] If there is a single intermediary and hackers manage to compromise it, the entire system could come crashing down. A system with multiple brokers would be far more resilient.[327] If one intermediary is taken down, others would pick up the slack. Indeed, that risk of losing business to one's competitors is a feature, not a bug—it will further incentivize brokers to secure their own systems.

Finally, there are a several practical considerations. Lawmakers may not need to do anything at all to encourage the creation of white market brokers. Part of the reason brokers haven't yet emerged is because prices aren't very high. If legitimate vulnerability sales become sufficiently lucrative, brokers should form on their own, drawn by the prospect of sharing hackers' large payouts. Brokers would operate, in effect, as pilot fish. This has already happened in the gray and black markets, where brokers appeared without any specific government encouragement (and, in the latter case, notwithstanding efforts to suppress the trade).[328] Somewhat more complicated is how to ensure that white market brokers will have the desired attributes that are described in this Subpart. Some of these characteristics should emerge naturally as a result of government nonintervention. For example, we want white market brokers to be for-profit entities. That should happen on its own, just as it has in the gray and black markets, and the government need only refrain from backing nonprofit competitors with subsidies that could drive their rivals out of business. In the same way, multiple brokers will probably appear naturally, again as in the gray and black markets. All that's needed is for the government to refrain from picking a favored intermediary or encouraging industry

[326] ROSENZWEIG, *supra* note 33, at 19.

[327] *Cf.* Bambauer, *supra* note 23, at 1054–57 (arguing that disaggregated systems are more resilient to attack).

[328] *Cf.* Sutton & Nagle, *supra* note 126, at 15 (noting that if underground methods "successfully generated revenue, they would be used more often").

consolidation.[329] Other desirable characteristics may require an affirmative government push. For instance, we want hackers and brokers to be able to sell bugs to independent security companies, not just the vendors who made the flawed products. But that carries a risk of legal liability, so authorities would need to offer immunity or adopt a policy of nonenforcement.

As for funding, some scholars argue that brokers should be financed through taxes[330] or user fees.[331] But perhaps the most straightforward approach would be for them to charge commissions. In return for facilitating a successful deal, a hacker might pay a certain percentage of the sale price—say 10 or 15 percent. The numbers needn't necessarily be fixed. A broker's exact cut from a given sale could vary depending on the product concerned or the bug's severity.

Commissions have the advantage of being easy to administer. Using commissions to fund white market brokers also would be consistent with practices on the gray and black markets, where intermediaries commonly receive a cut of the sales they facilitate. (TheRealDeal's commission is 3 percent, while the Grugq takes 15.[332]) Additionally, commissions would bring an element of progressivity. The researchers who derive the most benefit from the system—those who sell high severity and therefore high-priced bugs—would be responsible for shouldering most of the system's administrative costs. Just as importantly, commissions would align the interests of hackers and brokers during negotiations with vendors—both would have an interest in maximizing sale price. A broker's interest in maximizing payouts will help counteract the downward price pressures that are endemic to the white market and thus make legitimate sales to vendors more alluring.

3. Sales to Third Parties

The thorniest question about white market brokers is whether white hats should be limited to selling bugs to the vendors of the affected products or should also be allowed to work with independent security companies. Most scholars argue the former. Kannan and Telang worry that a subscription-based security firm "always has an incentive to 'leak' vulnerability information" to hackers who might exploit it, thereby making its services more valuable and in

[329] *But see* Kannan & Telang, *supra* note 73, at 3 (predicting that the white market "is likely to yield to natural monopoly").

[330] *See, e.g.*, FREI & ARTES, *supra* note 41, at 15.

[331] *See* Ozment, *supra* note 17, at 4; *see also* Kesan & Hayes, *supra* note 16, at 821.

[332] *See supra* notes 121, 144 and accompanying text.

the process "threaten[ing] non-subscribers who may be subjected to attacks."[333] Yet allowing sales to independent security companies would offer a number of benefits, and any risk of leaks can be managed with a combination of criminal law and market-based sanctions.

A vendor-issued patch normally will be the best solution to a flaw, but independent security companies can provide subscribers with temporary, second-best options. Subscription-based security services like TippingPoint, which runs the Zero Day Initiative, and iDefense, which runs the Vulnerability Contributor Program, offer "ahead of the threat" stopgaps that provide a modicum of protection until vendors get around to fixing the problems.[334] These include intrusion detection systems, which "filter suspicious traffic based on signature-based attack detection," and other services.[335] In addition, independents can fill gaps in existing bug bounty programs. Many vendors don't buy bugs at all, and a sale to an independent company may be the only way to address flaws in products unsupported by bounties.[336] Similarly, some vendors might not issue patches for obsolete software—why keep updating Windows XP when you're trying to move everyone to Windows 10? Users with older, unsupported versions of software can't count on vendor-issued patches so their only option may be to rely on independent companies that still service outdated products. There's also the problem of multivendor vulnerabilities. If there's a flaw in a popular software library or a protocol, as opposed to a proprietary piece of software, the most efficient way of remedying the bug may be to sell to an independent company rather than negotiating separately with each vendor whose products were affected.[337]

Allowing independent security companies to buy bugs also introduces competition to the buyer's side, helping inflate prices and correct distortions in the marketplace. When it comes to software flaws, a vendor is more or less a monopsonist. It is essentially the only buyer for information about flaws in its

[333] Kannan & Telang, *supra* note 73, at 4. The authors raise this concern about "market-based informediar[ies]"—namely, brokers. *Id.* at 4. But because the brokers they envision would sell security services in addition to facilitating deals, their concern about leaks would arise here too. *See id.* at 2; *see, e.g.*, Anderson & Moore, *supra* note 55, at 612; Camp, *supra* note 319, at 194; Li & Rao, *supra* note 73, at 532.

[334] *See* FREI & ARTES, *supra* note 41, at 7; *see also* Ransbotham et al., *supra* note 55, at 45, 46.

[335] Ransbotham et al., *supra* note 55, at 45; *see also* Sam Ransbotham & Sabyasachi Mitra, *Choice and Chance: A Conceptual Model of Paths to Information Security Compromise*, 20 INFO. SYS. RES. 121, 129–30 (2009) (describing possible countermeasures).

[336] *See, e.g.*, Egelman et al., *supra* note 106, at 44 (explaining that "markets independent of a software vendor" are necessary when there is "no vendor willing to pay for vulnerability information").

[337] *See, e.g.*, FREI & ARTES, *supra* note 41, at 15.

products, at least on the white market, and this concentration on the buyer's side tends to depress prices.[338] Allowing hackers to sell to third parties dilutes the monopsony. If McAfee can bid against Microsoft, that means higher prices.[339] A related benefit is that third-party sales can reduce buyer holdouts. If a vendor makes a lowball offer and refuses to budge, a hacker can pull out and strike a deal with Symantec. Finally, the existence of multiple bidders helps facilitate price discovery. The price a given flaw ultimately commands is more likely to reflect its true market value when multiple parties are bidding on it than when a single buyer makes a take-it-or-leave-it offer.

What about leaks? Independent security companies seemingly have an incentive to share vulnerability information with malicious hackers to drum up business—the digital equivalent of a home security company hiring neighborhood toughs to burglarize houses. But the risk of leaks seems more theoretical than real. Antivirus companies have been around for decades, and VCP and ZDI have been buying bugs since the early 2000s. Yet there appear to be no reported instances of any of these firms leaking, notwithstanding the apparent financial incentive to do so.[340] That may be because the threat of criminal punishment and reputational sanctions seem capable of managing the problem.

A company that divulges vulnerabilities on the sly could well face liability under the CFAA.[341] Prosecutors have successfully brought CFAA charges against defendants who either aided and abetted or conspired with others who violated the statute.[342] Deliberately revealing vulnerabilities to known hackers with the intent that they compromise the affected systems certainly sounds like a clear case of complicity, and the prospect of criminal charges may be enough to suppress this sort of self-dealing. Market-based sanctions likewise may discourage leaks. Companies that are known to cooperate with malicious hackers likely would be punished in the marketplace; they would earn justifiably bad reputations for facilitating cyberattacks, and subscribers likely

[338] *See supra* note 177 and accompanying text.

[339] *See, e.g.*, Bambauer, *supra* note 23, at 1088; Ransbotham et al., *supra* note 55, at 61.

[340] *See* Li & Rao, *supra* note 73, at 538 (reporting that "[e]xtensive" research "uncovered no previous instances of information leakage from iDefense").

[341] 18 U.S.C. § 1030(a) (2012); *see, e.g.*, Granick, *supra* note 36, at 19–20; Kirsch, *supra* note 69, at 386–87, 392–94; Oriola, *supra* note 37, at 497–99.

[342] *See* OFFICE OF LEGAL EDUC., PROSECUTING COMPUTER CRIMES MANUAL 17 (2010); *see, e.g.*, United States v. Willis, 476 F.3d 1121 (10th Cir. 2007) (upholding an aiding-and-abetting conviction under the CFAA); *cf.* United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc) (affirming the dismissal of an aiding and abetting conviction because the people with whom the defendant cooperated had not "exceed[ed] authorized access" in violation of the CFAA).

would flee to competitors that are committed to preventing, rather than facilitating, intrusions. Kannan and Telang themselves emphasize the risk of leaks from a "monopolistic" firm "in an unregulated framework,"[343] perhaps recognizing that companies that are subject to competitive forces and regulations, such as criminal laws, are less likely to do so.[344]

B. Increasing White Market Payouts

Brokers can make white market transactions somewhat more attractive by correcting power imbalances and redressing information asymmetries. But this probably won't overcome the substantial pricing disparities that lead so many researchers to sell on the gray market, where paydays are substantially larger.[345] Overt government assistance like liability protections, tax benefits, and outright subsidies likely will be needed.[346] These measures should not only lure hackers into the market, they should also produce a pilot fish effect as brokers naturally emerge to claim a share of the white hats' substantial rewards.

One straightforward way to increase payouts is to grant hackers immunity.[347] Unlike the gray market, where government buyers give researchers an implicit assurance of immunity, sales to vendors carry a substantial risk of criminal and civil liability.[348] Removing that threat would increase white hats' expected benefits—they no longer would need to discount the bounties they stand to receive to reflect the risk of criminal charges or civil lawsuits. For instance, Bambauer and Day argue that hackers should be immune to civil IP lawsuits as long as they follow certain best practices, such as telling vendors first about their finds, testing on their own systems, and not weaponizing the bugs.[349]

White hats should enjoy both civil and criminal immunity, provided they comply with these or similar best practices and thereby demonstrate that

[343] Kannan & Telang, *supra* note 73, at 9.

[344] The same legal and reputational constraints seemingly would dissuade a hacker or broker from offering a newly discovered flaw to black market buyers in an effort to drive up prices on the white market.

[345] *See, e.g.*, MILLER, *supra* note 101, at 5.

[346] *See, e.g.*, Bambauer, *supra* note 23, at 1060; Esther Gal-Or & Anindya Ghose, *The Economic Incentives for Sharing Security Information*, 16 INFO. SYS. RES. 186 (2005).

[347] *Cf.* Kesan & Hayes, *supra* note 16, at 821 (explaining that the risk of a "federal prosecution" is a "substantial barrier to entry").

[348] *See supra* notes 197–228 and accompanying text.

[349] Bambauer & Day, *supra* note 27, at 1088–94; Calkins, *supra* note 27, at 203; Kesan & Hayes, *supra* note 16, at 821, 826–27; Kirsch, *supra* note 69, at 400; *see also* ROSENZWEIG, *supra* note 33, at 17.

they're operating in good faith. Bambauer and Day favor civil immunity but argue that the CFAA and other criminal laws should remain in play to "deter strategic behavior by black hat hackers, who may try to fit their activities within the contours of the safe harbor."[350] That is certainly a danger, but leaving well-intentioned hackers exposed to criminal sanctions seems ill-advised. Civil immunity without criminal immunity might not be very effective. Eliminating the relatively modest sanctions threatened by civil lawsuits may not foster legitimate research if white hats remain subject to the more severe penalties promised by criminal law. In addition, criminal liability would maintain existing incentivizes to sell to the NSA and other government buyers. Why work in the white market, where you are safe from civil suits but exposed to criminal prosecutions, when you can go gray and avoid both?

A second option is tax breaks.[351] Lawmakers might exclude from hackers' taxable income any bounties from software vendors or independent security companies. Exempting such payments from taxation would effectively increase their value anywhere from 10 to nearly 40 percent, depending on one's bracket. Tax exemptions are a fairly common tactic for encouraging a wide variety of desired conduct, such as providing health care (health insurance paid for by one's employer is tax exempt) and geographic mobility (certain proceeds from the sale of one's primary residence are not taxed). Policymakers might take a similar approach for vulnerability research. Letting white hats shield a portion of their income from Uncle Sam would be a powerful enticement—especially for hackers who treat freelance bug hunting as a full-time job. An experienced researcher named Mark Litchfield made $500,000 in two years submitting flaws to HackerOne.[352]

Third, the government might directly subsidize white hats by matching the bounties they receive from vendors.[353] In the mid–2000s, entrepreneur and philanthropist Mark Shuttleworth matched donations to a fund that the nonprofit software developer Mozilla used to reward hackers who found critical flaws in its products.[354] More recently, Dan Geer of In-Q-Tel—"the CIA's venture capital arm"—has urged the government to pay hackers ten times the amount of the bounties offered by vendors.[355] (To be precise, Greer is

[350] Bambauer & Day, *supra* note 27, at 1104.

[351] *See* Bambauer, *supra* note 23, at 1060; *see also* ROSENZWEIG, *supra* note 33, at 24–25.

[352] Weinberger, *supra* note 93.

[353] Eichensehr, *supra* note 24, at 527.

[354] *See* Sutton & Nagle, *supra* note 126, at 12.

[355] *See* Kim Zetter, *CIA Insider: U.S. Should Buy All Security Exploits, Then Disclose Them*, WIRED (Aug. 6, 2014, 4:28 PM), https://www.wired.com/2014/08/cia-0day-bounty/ [https://perma.cc/N86J-BYVW].

not proposing supplemental bounties; he envisions that the government would outbid the vendor, acquire the bug itself, then publicly disclose the information.) Whether the government would need to boost a payment by a factor of ten or whether some smaller multiplier would suffice—doubling or tripling it, say—the basic insight remains the same: Increasing payments to white hats would cause more hackers to abandon the black and gray markets and sell flaws to vendors who can patch them.

The annual cost of these supplemental bounties could range anywhere from $8 million to $36 million on up. (Those numbers are in the same ballpark as the $25 million the NSA paid for bugs on the gray market in 2013.[356]) Here are a few rough, back of the envelope calculations. Google reportedly paid white hats some $2 million between 2010 and 2013, and Facebook's bounties totaled about $1 million from 2011 to 2013.[357] Let's assume that those numbers—between $333,000 and $500,000 per company per year—are representative of payouts throughout the industry. Let's also assume that there are two dozen major vendors that would pay bounties in that range.[358] If the feds matched these bounties dollar for dollar, it would cost taxpayers between $8 and $12 million a year. Doubling the bounties would run $16 to $24 million, tripling them would be $24 to $36 million, and so on.

That's not nothing, but it's small beer as far as subsidies go. Private firms in the energy, financial, and manufacturing sectors routinely are subsidized by the federal government to the tune of tens of millions and even billions of dollars each year. To wit:

- Boeing: $32 million in grants and tax credits, along with $4.6 billion in loans and loan guarantees.[359]
- General Motors: $38 million in grants and tax credits, $3.6 billion in loans and guarantees.[360]

[356] Gellman & Nakashima, *supra* note 129; *see also* Stockton & Golabek-Goldman, *supra* note 109, at 249.

[357] *See supra* notes 80, 83 and accompanying text.

[358] That assumption might be too generous. Frei and Artes emphasize that "most" critical vulnerabilities are in products offered by a small handful of dominant firms; the authors put the number at ten leading companies. FREI & ARTES, *supra* note 41, at 16. For unexplained reasons, the authors estimate that vendors would pay an average of $150,000 per bug. That's why their overall estimate of $262.1 million a year is considerably higher. *Id.*

[359] Between 2000 and 2014, Boeing received $457 million in federal grants and tax credits as well as $64 billion in federal loans, loan guarantees, and bailout assistance. PHILIP MATTERA & KASIA TARCZYNSKA, UNCLE SAM'S FAVORITE CORPORATIONS: IDENTIFYING THE LARGE COMPANIES THAT DOMINATE FEDERAL SUBSIDIES 12–13 (2015).

[360] Between 2000 and 2014, GM received $529 million in federal grants and tax credits as well as $50 billion in federal loans, loan guarantees, and bailout assistance. *Id.* at 13.

- JPMorgan Chase: $32 million in grants and tax credits, $92.8 billion in loans and guarantees.[361]
- NextEra Energy (an owner of renewable energy properties): $285 million in grants and tax credits.[362]

Again, those are average annual subsidies, not total amounts. Matching vendor bounties would be costly, to be sure. But the expenditures would be several orders of magnitude smaller than what other companies receive from taxpayers every year. And these defensive payments would not be appreciably larger than what the NSA currently spends on bugs for offensive purposes.

Candidly, supplemental bounties could produce unhelpful price inflation on the gray market.[363] In response to larger white market payments, government buyers could simply hike their own prices and restore hackers' prior preference for gray market deals. This risk, though meaningful, can be managed in a number of ways. The NSA does not have unlimited resources, and Congress could use its power of the purse to stave off the threatened inflation. It could appropriate a sum large enough for the NSA to acquire a sufficient (whatever that means) number of bugs but not so large that the agency could systematically bid up prices. Another option is to foster intragovernmental price transparency.[364] If the NSA knows that the CIA is offering only $10,000 for a bug, it's not likely to bid $80,000.[365] A more extreme measure would be for the government to designate a single gray market buyer—perhaps the Office of the Director of National Intelligence, which oversees the entire intelligence community—and then, after purchase, allocate a given bug to whichever agency demonstrates the greatest need. This would effectively establish a gray market monopsony, depressing prices.[366] These measures may be worth adopting in their own right, but they seem especially appropriate responses to gray market inflation negating the benefits of higher white market bounties.

It may seem odd for the government to fund defensive bounties at the same time it is paying top dollar for bugs it plans to exploit. There is, in other

[361] Between 2000 and 2014, JPMorgan Chase received nearly $450 million in federal grants and tax credits as well as $1.3 trillion in federal loans, loan guarantees, and bailout assistance. *Id.* at 13.

[362] Between 2000 and 2014, NextEra received $1.9 trillion in federal grants and tax credits. About ninety percent of those subsidies were paid between 2009 and 2014 for renewable energy projects. *Id.* at 7, 8.

[363] *Cf.* Fidler, *supra* note 16, at 451 (worrying that competition among government buyers drives up prices, luring hackers into the gray market).

[364] *Id.*

[365] *Cf.* MILLER, *supra* note 101, at 8.

[366] *See supra* notes 177–178 and accompanying text.

words, a Janus problem. But this dynamic is already present. On the offensive side of the ledger, the NSA competes against the FBI, CIA, and other agencies that want bugs for law enforcement, military, and intelligence operations.[367] Competition also exists between offensive and defensive players.[368] The government funds a number of defensive initiatives—including grants to study bugs in automobiles and other products,[369] as well as funding for CERT, a nonprofit vulnerabilities clearinghouse[370]—while simultaneously buying zero-days of the utmost destructive potential. Indeed, the NSA itself is torn between offense and defense. Fort Meade conducts offensive cyber operations against the nation's adversaries, but it is also charged with protecting much of the nation's digital infrastructure.[371] Intragovernmental competition would be nothing new.

It also may seem incongruous for a market-based approach to propose government subsidies. At least some of these outlays, however, are payments for services rendered to the government rather than true subsidies. To be precise, my proposal involves two sets of payouts. The payments to hacker are overt: The government would reward researchers who uncover flaws with cash and other benefits. The payments to vendors are implicit: The supplemental bounties offered to hackers amount to taxpayers bearing some of the companies' costs of ensuring that their products are relatively free of bugs. But only part of these implicit payments would represent subsidies. As described above, brokers would publicize certain details about the completed transactions, including the prices at which the bugs were sold.[372] The government would be paying vendors for information about the transactions along with the right to reveal that information to the public.[373] As for the expenditures that are properly characterized as subsidies, they seem justified because bug hunting generates substantial positive externalities. When hackers find flaws and vendors repair them, security is improved for all users of the affected products. Users experience a positive externality—they receive a benefit but need not compensate those who provided it.[374] Because

[367] *See* Fidler, *supra* note 20, at 40–41; *see also* Strohm & Riley, *supra* note 125.

[368] Eichensehr, *supra* note 24, at 498 n.154.

[369] *See, e.g.*, Greenberg, *supra* note 50.

[370] Granick, *supra* note 36, at 5; *see supra* note 73.

[371] Derek E. Bambauer, *Sharing Shortcomings*, 47 LOY. U. CHI. L.J. 465, 476–77 (2015); *cf.* Nojeim, *supra* note 57, at 136.

[372] *See supra* notes 315–318 and accompanying text.

[373] *Cf.* Bambauer, *supra* note 23, at 1086 (arguing that Congress should pay firms that inform the government about their zero-day sales).

[374] *See* ROSENZWEIG, *supra* note 33, at 9.

white hats don't capture all the benefits of their discoveries, vulnerability reports are undersupplied on the white market.[375] A common strategy is to encourage positive externalities through government subsidies and other incentives.[376]

Of course, the implicit payments to vendors threaten moral hazard. Companies are more likely to engage in risky behavior (failing to make adequate efforts to find flaws in their products during development) if others bear the associated costs—specifically taxpayers, in the form of payments to outside researchers after the products are released. Vendor subsidies thus could lead to an especially perverse outcome: Bounties that are intended to improve product security could result in software that's plagued with even more flaws.

This is a significant problem, but it can be managed with a combination of governmental and market-based responses. Many scholars have proposed subjecting software developers to tort liability for injuries caused by flaws in their products,[377] thereby internalizing some of the costs of insecure software.[378] Another way to address moral hazard is reputational sanctions—a method that requires little, if any, government intervention. If a company's products are regarded as insecure, users may take their business to competitors. Vulnerability brokers can play an instrumental role in that process. Brokers normally will publicize information about the transactions they have mediated—including vendor, product, and price. If consumers notice that a large number of reported transactions concern iOS, Apple's reputation may suffer, and some may switch to Android smartphones. Apple therefore will have an incentive to keep testing its products for flaws notwithstanding the implicit subsidies.

Kesan and Hayes recently proposed a novel method of funding a legitimate vulnerabilities market that would not require overt government subsidies: tradeable derivatives.[379] (Rainer Bohme described a similar "exploit derivatives market" a decade earlier.[380]) Under this innovative proposal, investors would buy and sell contracts "based on whether they think the value of a particular vulnerability tier will go up or down," with flaws grouped into tiers of high, medium, and low severity.[381] Because bug bounty programs

[375] *See* Coyne & Leeson, *supra* note 33, at 479–81.

[376] Bambauer, *supra* note 23, at 1060; Coyne & Leeson, *supra* note 33, at 479; *see also* ROSENZWEIG, *supra* note 33, at 10.

[377] *See* Coyne & Leeson, *supra* note 33, at 492; Lichtman & Posner, *supra* note 196, at 232–39; *see also* ROSENZWEIG, *supra* note 33, at 23.

[378] Sales, *supra* note 15, at 1557.

[379] Kesan & Hayes, *supra* note 16, at 821–28.

[380] BÖHME, *supra* note 18, at 3.

[381] Kesan & Hayes, *supra* note 16, at 821.

usually pay less than gray market buyers, the authors propose to subsidize vendors' rewards with the proceeds from futures contracts.[382] Such an arrangement would harness "the collective knowledge of investors, security researchers, and vendors to establish a fair market price" for software flaws and thus make the vulnerabilities market "much more transparent."[383]

Vulnerability derivatives, however, may not be politically viable, as they could prompt concerns that investors are somehow profiting from cyberattacks. Similar objections arose in 2003,[384] when word got out that the Pentagon's Defense Advanced Research Projects Agency was considering what critics dubbed a "terrorism futures market."[385] The basic idea was to allow people to trade contracts that paid out if various calamities like terrorist attacks or assassinations took place. The price of the contracts would enable policymakers to infer the probability that the events would occur. Justified or not,[386] the idea was met with widespread public outrage.[387] The Pentagon quickly backtracked, announcing within a day that the program was being canceled.[388] Vulnerability derivatives might trigger the same objections. Kesan and Hayes emphasize that contracts in their market would not be based on specific "security events" but rather on general "tiers of security risks."[389] But presumably the former will influence the latter. If malicious hackers exploit lots of "high severity" flaws, that will affect the price at which contracts for the "high severity" tier are traded, and therefore the size of the resulting payouts.[390] Investors thus would be paid based on the extent to which bad actors have successfully compromised systems. And that could provoke concern about the seemliness of the resulting profits.

[382] *Id.* at 826.

[383] *Id.* at 824.

[384] *Id.* at 811–12.

[385] *See* Carl Hulse, *Threats and Responses: Plans and Criticisms; Pentagon Prepares a Futures Market on Terror Attacks*, N.Y. TIMES (July 29, 2003), http://www.nytimes.com/2003/07/29/us/threats-responses-plans-criticisms-pentagon-prepares-futures-market-terror.html.

[386] For a defense of the DARPA program, see Justin Wolfers & Eric Zitzewitz, *The Furor Over "Terrorism Futures,"* WASH. POST. (July 31, 2003), https://www.washingtonpost.com/archive/opinions/2003/07/31/the-furor-over-terrorism-futures/af3569b4-479e-4100-97f4-c929a3f43922/?utm_term=.6bbad764f0d4 [https://perma.cc/7Y7U-LCUE].

[387] Paul Courson & Steve Turnham, *Amid Furor, Pentagon Kills Terrorism Futures Market*, CNN (July 30, 2003, 1:37 PM), http://www.cnn.com/2003/ALLPOLITICS/ 07/29/terror.market [https://perma.cc/J3ZW-SL9F].

[388] Carl Hulse, *Swiftly, Plan for Terrorism Futures Market Slips Into Dustbin of Idea Without a Future*, N.Y. TIMES (July 30, 2003), http://www.nytimes.com/2003/07/30/us/threats-responses-plans-criticisms-swiftly-plan-for-terrorism-futures-market.html.

[389] Kesan & Hayes, *supra* note 16, at 55.

[390] *Id.*

There's also the question of administrative cost. Regulating a complex, new market for vulnerability derivatives could prove expensive, and it's not obvious that doing so would be cheaper than supplementing vendors' bounty payments. Recall that these payouts could run anywhere from $8 million to $36 million a year.[391] The cost of staffing up an administrative agency to oversee the market could easily approach or even exceed those numbers. It may be cheaper to simply match vendor bounties.

A few final observations about making the white market more attractive to hackers: First, white market payouts need not necessarily be identical to those offered by governments and criminals to draw sales from the gray and black markets. Many researchers have moral and reputational motivations to go along with their pecuniary concerns.[392] All things being equal, or nearly so, they might prefer to contribute to the internet's security than to help facilitate cyberattacks. These hackers might be willing to accept payouts that, while larger than the modest sums vendors currently offer, are somewhat less generous than the prevailing gray and black market rates.[393] In addition, some hackers might be induced to accept slightly less lucrative offers from software vendors due to the high transaction costs on the black market.[394] Even if the white market sticker price is lower, the value of the payment actually received may be comparable (or even larger) because the hacker need not apply a discount rate to reflect the possibility of being caught by law enforcement or the risk of scams. Finally, the promise of immunity might persuade some researchers to accept smaller sums on the white market than they could obtain on the black market. (Gray market sales already receive that assurance.[395]) Again, a somewhat lower sticker price might be sufficiently attractive because there would be no risk of criminal sanctions. To entice hackers into the white market, it may not be necessary to match governments and criminals dollar for dollar.

C. Why Not Have the Government Do It?

Wouldn't it be easier for the government to simply buy bugs and hand them over to vendors, as several scholars have urged?[396] The government

[391] *See supra* notes 356–358 and accompanying text.

[392] *See supra* notes 104–106 and accompanying text.

[393] FREI, *supra* note 99, at 8; Egelman et al., *supra* note 106, at 44.

[394] ABLON ET AL., *supra* note 23, at 25; *see supra* notes 116–120 and accompanying text.

[395] *See supra* notes 221–224 and accompanying text.

[396] *See* Bambauer, *supra* note 23, at 1019, 1087–88; Camp, *supra* note 319, at 194; Eichensehr, *supra* note 24, at 525–27; Fidler, *supra* note 16, at 453–54; *see also* FREI & ARTES, *supra* note

option does have the seeming advantage of simplicity. But on closer inspection, the more complex system of brokers and subsidies I've proposed has a number of decisive advantages.

First, a market-based approach likely would have lower transaction and administrative costs.[397] A bug sale in the private sector would involve three distinct steps: discovery by a hacker, mediation by a broker, and transfer to a vendor. The government option would add a fourth step to this process: discovery by a hacker, mediation by a broker, transfer to the government, and transfer to a vendor. A government buyer would not obviate the need for a broker, as the power imbalances and information asymmetries that plague white market sales would persist. The fact that brokers remain integral to the gray market, which is dominated by government buyers, is strong evidence that they would be just as essential on a government-dominated white market. Indeed, some scholars who favor the government option acknowledge that it would require intermediaries.[398] Adding a fourth step would increase the system's operating costs; resources that could have been devoted to buying bugs will instead be consumed by the government. In short, the market-based approach would produce more patches at a lower cost than the government-run alternative.

Second, a monopsonistic buyer would depress prices. The white market is already a quasi-monopsony—for example, Microsoft is essentially the only buyer for flaws in Microsoft products[399]—and creating a bona fide monopsony could drive down prices even further.[400] (These harms are unlikely to materialize, of course, if the government offered lavish payouts along the lines proposed by Dan Geer: "[S]how us a competing bid, and we'll give you 10 times."[401]) Monopsony may well be desirable in the gray market,[402] as reducing the prices paid by offense-minded government buyers is a key way of encouraging hackers to sell to vendors instead. But monopsony would be devastating in the white market, where it would exacerbate existing downward

41, at 1; *cf.* Stockton & Golabek-Goldman, *supra* note 109, at 265 (proposing that government buyers "curb the demand side" by publicly revealing their zero-day purchases).

[397] *Cf.* Hahn & Layne-Farrar, *supra* note 33, at 300 (arguing that cybersecurity regulation should "seek to minimize," among other things, "administrative costs").

[398] FREI & ARTES, *supra* note 41, at 17 (describing a government-run vulnerability purchasing program that would use intermediaries known as "technical qualification centers" to assess flaws submitted by hackers and interface with vendors).

[399] *See supra* note 177 and accompanying text.

[400] *See supra* notes 177–178 and accompanying text.

[401] Zetter, *supra* note 355.

[402] *See supra* note 366 and accompanying text.

price pressures. In the white market, price-inflating competition is what's needed.

Third, the government might not consistently turn the bugs over to vendors. It might succumb to the persistent temptation to use them in offensive military or intelligence operations. The same institutional dynamics that today lead officials systematically to prefer offense over defense may well resurface in a government-run purchase program. In particular, cost-benefit asymmetries and cognitive failures might continue to bias the government in favor of offense.[403] Policymakers might have a change of heart after acquiring a vulnerability on the white market and reallocate it to the NSA.

Fourth, and relatedly, hackers who are willing to sell to private firms might balk at working with the government. Certain ideologically motivated researchers will "refuse to sell to the U.S. government on principle, no matter the price,"[404] especially after Edward Snowden's leaks about NSA surveillance programs. Establishing the government as the sole white market buyer might drive ideological hackers to sell elsewhere—to penetration-testing firms on the gray market or, even worse, to criminals or hostile states on the black market. This outcome seems even more likely if hackers suspect that the bugs they sell the government for defensive uses will end up being used by the NSA in offensive operations.

Fifth, a government-run purchasing program could exacerbate the moral hazard problem. Software developers might take shortcuts when testing their products for flaws because the government will bear the resulting costs. Why spend millions of dollars to purge vulnerabilities during the development phase when taxpayers will pick up the tab for outside hackers who uncover the problems after release?[405] Candidly, this problem arises with any proposal to effectively subsidize vendors by paying outside researchers, including my own. But a direct government purchasing program would involve larger subsidies than merely supplementing vendor bounties. In the latter, the vendor would bear at least some of the costs; in the former, all costs would fall on the government. Direct government purchases thus would create an even stronger perverse incentive to release inadequately tested products with critical vulnerabilities.

[403] *See supra* notes 231–243 and accompanying text.

[404] Zetter, *supra* note 355.

[405] *But see* FREI & ARTES, *supra* note 41, at 14 (speculating that a remunerative purchasing program run by the government will "motivate vendors to discover vulnerabilities during the development phase").

Finally, the same Fort Knox concerns that counsel against one broker also counsel against one buyer.[406] A single buyer of vulnerability information—with a single database of all flaws that are awaiting patches—would be an attractive target, and its compromise would be catastrophic. True, it would be a government entity, but it could still be breached. Military and intelligence networks are generally regarded as more secure than the government's civilian systems—take a bow, Office of Personnel Management[407]—and most private-sector networks. But they are not impregnable, certainly not to insiders; a future Manning or Snowden might leak, whether because of well-intentioned concerns that vendors are not patching the flaws quickly enough or for more malicious reasons. A system with multiple buyers would be more resilient. If one is compromised, only a portion of the universe of data will be affected, and other buyers would continue to operate.[408]

D. Ancillary Benefits

The primary reason to foster a more robust white market is, of course, to encourage hackers to sell the bugs they've discovered to vendors that will patch them instead of government agencies that will exploit them. But such a market would have a number of ancillary benefits as well. This Article attempts only a thumbnail sketch of these benefits; a more comprehensive analysis would be a fruitful topic for future research.

First, white market sales would generate price signals that would allow key players to optimize their investments in cyber defense. F.A. Hayek recognized that prices communicate valuable information about market conditions. If the price of, say, tin increases, that tells users that "some of the tin they used to consume is now more profitably employed elsewhere, and that in consequence they must economize tin."[409] Prices transmit this information far more efficiently than centralized mechanisms ever could. "The most significant fact about this system is the economy of knowledge with which it operates, or how little the individual participants need to know in order to be able to take the right action."[410] The price system thus operates as "a kind of machinery for

[406] *See supra* notes 326–327 and accompanying text.

[407] *See* Brendan I. Koerner, *Inside the Cyberattack That Shocked the US Government*, WIRED (Oct. 23, 2016, 5:00 PM), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government [https://perma.cc/LAR5-J3S5].

[408] *Cf.* Bambauer, *supra* note 23, at 1054–57 (arguing that disaggregated systems are more resilient to attack).

[409] Hayek, *supra* note 56, at 526.

[410] *Id.* at 526–27.

registering change, or a system of telecommunications which enables individual producers . . . to adjust their activities to changes of which they may never know more than is reflected in the price movement."[411] Whether or not one is sympathetic to Hayek's broader agenda—demonstrating the impossibility of a centrally planned economy[412]—one can certainly recognize that prices are a uniquely powerful way of conveying information.

That is certainly true when it comes to cybersecurity. The frequency and prices at which vulnerabilities are sold communicate valuable information to consumers, researchers, and policymakers alike.[413] Prices tell us about the security of a given product.[414] A bug's price likewise reveals its severity—the probability that attackers will discover and exploit it, the degree of control an intruder can attain over a compromised system, the harms an attacker can inflict, the number of machines that are vulnerable, and the costs of remediation. This sort of information can be enormously valuable to users. A large number of high-priced bugs signals that the product is insecure; users might respond by switching to a competitor's product. Small numbers and low prices send the opposite signal and may cement customer loyalty. Price data also helps hackers decide how much effort to devote to bug hunting and which products to focus on. A large number of expensive flaws will draw researchers to that particular product, increasing the chances that vulnerabilities will be found and patched. With small numbers and low prices, white hats will focus on other products or abandon bug hunting altogether. A broader advantage of price signals is that they can help society as a whole calibrate its investments in cyber defense. In the absence of pricing data, policymakers "have no way to know the optimal level of security" and, if they get it wrong, they "lack the feedback mechanism to force them to revise their judgments."[415] Prices aggregate the judgments of countless players into an easily understood assessment, increasing the odds that "the 'right' amount of cyber security can be produced."[416]

Second, bug sales can foster a more robust market for cyber insurance by generating data that insurers could use to predict the incidence and

[411] *Id.* at 527.

[412] *Id.* at 524.

[413] *See* Böhme, *supra* note 22, at 306; Coyne & Leeson, *supra* note 33, at 478–79; Kuehn & Mueller, *supra* note 26, at 10–11.

[414] Anderson & Moore, *supra* note 55, at 612; Böhme, *supra* note 22, at 301; *see also* BÖHME, *supra* note 18, at 3; *cf.* Egelman et al., *supra* note 106, at 44 ("[M]arket prices should reveal or reflect something about the security of the underlying products, extracting hidden information.").

[415] Powell, *supra* note 58, at 507; *see also* Coyne & Leeson, *supra* note 33, at 488.

[416] Coyne & Leeson, *supra* note 33, at 490.

consequences of intrusions. This market is still in its "infancy."[417] According to a 2014 study by the *Wall Street Journal*, just 31 percent of companies carry some sort of cybersecurity insurance.[418] Part of the reason the industry remains in this embryonic state is because of the absence of actuarial data.[419] To insure against a given risk one needs to know, among other things, the probability that the threatened harm will come to pass as well as the magnitude of the losses the insured stands to incur.[420] That's a fairly straightforward task for commonplace risks like car crashes or residential fires. Insurers have extensive data sets on these kinds of incidents stretching back many decades, so it is relatively simple to predict the likelihood that they will occur in the future and set premiums and coverage levels accordingly.[421] The process is much more complicated when it comes to cyber. Cyber intrusions are still relatively novel, and many incidents go unreported (or even undiscovered), so the data that insurers rely on to calculate risk simply doesn't exist.[422] Given that uncertainty, it is quite difficult to price insurance products.[423] The pricing data generated by a white market isn't a perfect substitute, but it can help insurers estimate risk more accurately.

Cyber insurance is desirable for a number of reasons, not least of which is that the pooling of risk can substantially reduce the social losses from

[417] *See* Aviva Abramovsky & Peter Kochenburger, *Insurance Online: Regulation and Consumer Protection in a Cyber World*, *in* THE "DEMATERIALIZED" INSURANCE: DISTANCE SELLING AND CYBER RISKS FROM AN INTERNATIONAL PERSPECTIVE 117, 135 (Pierpaolo Marano et al. eds., 2016); *see also* Anderson & Moore, *supra* note 55, at 610; Rainer Böhme, *Cyber-Insurance Revisited*, 2005 WORKSHOP ON ECON. INFO SEC. 1, 5; Hahn & Layne-Farrar, *supra* note 33, at 338; William Yurcik & David Doss, *CyberInsurance: A Market Solution to the Internet Security Market Failure*, 2002 WORKSHOP ON ECON. INFO. SEC. 1, 1.

[418] Anderson, *supra* note 38, at 533.

[419] Lack of actuarial data is only part of the problem; there are plenty of other reasons for the market's immaturity. On the supply side, insurers are reluctant to offer coverage because of "cyber hurricanes": An attack on a widely used product could produce highly correlated losses that would be financially ruinous to the insurer. *See* Anderson & Moore, *supra* note 55, at 612; Böhme, *supra* note 22, at 306. Reinsurance, a common technique for managing concentrations of risk, may not be possible here as the losses from a massive cyberattack likely would not be limited to a particular geographic area but would be felt worldwide. *See* Böhme, *supra* note 417, at 5. On the demand side, many companies see little need for cyber insurance because they are effectively immune to lawsuits by third parties. Insurance requires the prospect of civil liability; why insure against harms to those who can't sue you? *See* ROSENZWEIG, *supra* note 33, at 23–24.

[420] *See* Abramovsky & Kochenburger, *supra* note 417, at 139–40; Anderson & Moore, *supra* note 55, at 612; Frye, *supra* note 28, at 366.

[421] *See* Lawrence A. Gordon et al., *A Framework for Using Insurance for Cyber-Risk Management*, 46 COMMS. ACM 81, 82 (2003).

[422] *See* Abramovsky & Kochenburger, *supra* note 417, at 141; Michelle E. Boardman, *Known Unknowns: The Illusion of Terrorism Insurance*, 93 GEO. L.J. 783, 784 (2005); Böhme, *supra* note 417, at 4; Gordon et al., *supra* note 421, at 82; Yurcik & Doss, *supra* note 417, at 1.

[423] *See* Gordon et al., *supra* note 421, at 85; Kesan & Hayes, *supra* note 16, at 805–06.

intrusions. Kesan et al. estimate that "the welfare gains associated with insuring worldwide security breaches and virus attacks in 2000 could have approached $13.16 billion."[424] Another advantage is that insurers can insist that their insureds take various steps to protect their systems from attackers, leading to better security.[425] If a policyholder balked, the insurer could increase its premiums to reflect the greater likelihood of losses (a form of price discrimination) or decline to provide coverage at all.[426] Rosenzweig points out that the same dynamic was at work in the late 1800s, when insurers drove the development of building and fire codes.[427] Insurance thus would function as a second-order form of regulation.[428]

These insurer-driven mandates may be even more effective than traditional regulations adopted by lawmakers.[429] Because of their need to turn a profit, insurance companies are better positioned to select security requirements whose severity is properly calibrated to the magnitude of the threats their insureds face.[430] They also have strong incentives to develop the expertise and gather the information that will allow them to determine what those risks are and the most effective way to counter them.[431] If their rules are too lenient, policyholders may suffer more attacks and they will have to pay more claims. If the rules are too strict, policyholders may flee to rival insurers with less costly mandates. In either case, the profit/loss mechanism enables insurance companies to correct any misalignment between threats and countermeasures. No comparable feedback mechanism exists for government regulators.[432]

Third, the white market could produce a more efficient industry structure as vendors replace their current firm-based approaches to bug hunting with contract-based approaches. In his seminal 1937 article "The Nature of the Firm," Ronald Coase posed a fundamental question: Why do firms emerge?[433] That is, why do entrepreneurs sometimes form organizations when they could

[424] Jay P. Kesan et al., *Three Economic Arguments for Cyberinsurance*, *in* SECURING PRIVACY IN THE INTERNET AGE 345, 357 (Anupam Chandler et al. eds., 2008).

[425] *See* Kesan et al., *supra* note 424, at 348; *see also* Coyne & Leeson, *supra* note 33, at 491; Hahn & Layne-Farrar, *supra* note 33, at 350; Hal R. Varian, *System Reliability and Free Riding* 10 (Nov. 30, 2004) (unpublished manuscript), https://pdfs.semanticscholar.org/78b3/bd3eba002da991a30e75a205524c118b89c8.pdf [https://perma.cc/8NT5-DR27].

[426] *See* Böhme, *supra* note 22, at 305; Gordon et al., *supra* note 421, at 82–83.

[427] ROSENZWEIG, *supra* note 33, at 24.

[428] *See* Sales, *supra* note 15, at 1558; *see also* Abramovsky & Kochenburger, *supra* note 417, at 140.

[429] *See* Kesan et al., *supra* note 424, at 353–54; *see also* ROSENZWEIG, *supra* note 33, at 24.

[430] *See* Coyne & Leeson, *supra* note 33, at 490; Powell, *supra* note 58, at 505.

[431] *See* Böhme, *supra* note 417, at 2.

[432] *See* Powell, *supra* note 58, at 505.

[433] R. H. Coase, *The Nature of the Firm*, 4 ECONOMICA 386 (1937); *see also* Benkler, *supra* note 106, at 372.

coordinate production by entering contracts with outsiders? The answer, Coase proposed, has to do with transaction costs. When the transaction costs associated with market exchanges are high, firms will emerge to manage production internally. Where transaction costs are low, entrepreneurs may prefer to coordinate via contracts. We can use this framework to understand bug hunting. In Coasean terms, vendors that employ full-time software engineers to search for flaws in their products are engaged in firm-based production of vulnerability data. Vendors that pay bug bounties to outside hackers are using a contract-based mechanism.

Vendors rely heavily on the efforts of in-house employees to find flaws in their products. These companies rely exclusively—or nearly so—on firm-based production. Even vendors with bug bounty programs seem to prioritize firm-based over contract-based production. No hard data is readily available, but vendors probably spend much more on employees who look for flaws during the product-development phase than on bounties paid to outside hackers who find flaws after release. Take, for instance, Google and Facebook. In recent years each reportedly spent between $333,000 and $500,000 on bounty payments annually.[434] The average software engineer at Google makes around $125,000 in base salary (not including benefits, stock options, and other compensation), and Facebook isn't far behind at approximately $120,000 a year.[435] At those rates, the companies would need at most the equivalent of three to four full-time employees devoted to bug hunting before they outran the amounts paid to outside researchers.

Part of the reason for this emphasis on firm-based production may be the high transaction costs of contracting with outside hackers.[436] If so, brokers could make contract-based production more attractive. In practice that would mean vendors would have less need for extensive teams of in-house employees responsible for bug hunting. Some could be replaced with outside hackers who would perform the same quality control functions on a contractual basis, both after products are released (as hackers currently do) and during the development phase (as employees currently do). In other words, outsourcing.[437]

[434] *See supra* notes 357–358 and accompanying text.

[435] Alyson Shontell, *The 25 Best-Paying Companies for Software Engineers*, BUS. INSIDER (Apr. 2, 2013, 9:10 PM), http://www.businessinsider.com/the-worlds-highest-paid-software-engineers-work-for-these-25-companies-2013-4 [https://perma.cc/UV92-J8D5].

[436] *Cf.* Kuehn & Mueller, *supra* note 26, at 7.

[437] *See* Egelman et al., *supra* note 106, at 43.

Candidly, that wouldn't be such a great deal for vendors' current employees, some of whom could see pay cuts or lose their jobs.[438] But those losses would be more than offset by the substantial gains to society at large. Matthew Finifter and his coauthors estimate that paying bounties to outside hackers is up to one hundred times more cost effective than hiring full-time employees to do the same job.[439] Contract-based bug hunting would dramatically lower vendors' costs of finding flaws.[440] "No matter how large a vendor's security team, it cannot compete with the combined experiences of a global group of individual specialists or organizations with diverse backgrounds, education, culture, and skills."[441] In short, a white market that allows more outsourcing to independent researchers would result in more efficient vulnerability discovery. Software vendors could achieve better security at a lower cost.

CONCLUSION

There's no question that the government has a critical role to play—indeed, the leading role—in securing cyberspace, whether through traditional means like law enforcement or through less conventional regulatory approaches. But it would be a mistake to neglect the private sector.

Individual hackers and other private entities have a wealth of cybersecurity expertise, and nowhere is this more true than the vital task of bug hunting. The more flaws that are found and reported to vendors, the better protected users will be against devastating cyberattacks. Yet because of excessive transaction costs on the white market, and because offense-minded government buyers offer such lavish payouts, many researchers choose to sell their discoveries to military and intelligence agencies, prolonging the window of vulnerability.

[438] It is still possible to make a comfortable living as a freelance security researcher. Mark Litchfield made $250,000 a year working with HackerOne, and in 2010 a Canadian named Abdul-Aziz Hariri earned more than $50,000 submitting bugs to the Zero Day Initiative. *See* Weinberger, *supra* note 93; Kim Zetter, *Portrait of a Full-Time Bug Hunter–Abdul-Aziz Hariri*, WIRED (Nov. 8, 2012, 6:30 AM), https://www.wired.com/2012/11/bug-hunting [https://perma.cc/9BLE-MNZH]. That may not be much money in Silicon Valley, but it undoubtedly would be attractive to hackers in developing economies like, say, India and Malaysia. *See* Zetter, *supra* note 55. So a switch from firm-based to contract-based production could have distributive consequences; it could redirect resources away from relatively prosperous jurisdictions toward less developed parts of the world.

[439] Finifter et al., *supra* note 55, at 273, 286. *But see* Granick, *supra* note 36, at 3 (arguing that patching already released products "is an expensive and inefficient way to fix flaws").

[440] *See* Egelman et al., *supra* note 106, at 42; Sutton & Nagle, *supra* note 126, at 9.

[441] FREI & ARTES, *supra* note 41, at 8.

Regulation is ill-suited to addressing this problem. What's needed are market-based solutions that can incentivize gray and black hats to shed their shadowy headwear and enter the white market instead.

Policymakers seeking to foster a legitimate vulnerabilities market needn't start with a blank canvas. They should look to the measures that have contributed to the thriving black and gray markets. In particular, brokers could minimize the often crippling transaction costs by connecting sellers with buyers, verifying the players' bona fides, overcoming information asymmetries, and counteracting severe power imbalances. In addition, a combination of liability protections, favorable tax treatment, and direct subsidies could make legitimate sales more attractive, luring hackers into the white market. These sorts of measures will help the private sector fulfill its promise as a worthy partner of the government in protecting cyberspace.