BUGS IN THE MARKET: CREATING A LEGITIMATE, TRANSPARENT, AND VENDOR-FOCUSED MARKET FOR SOFTWARE VULNERABILITIES

Jay P. Kesan* & Carol M. Hayes**

Ukraine, December 23, 2015. Hundreds of thousands of homes lost power. Call center communications were blocked. Authorities reported that 103 cities experienced a total blackout. The alleged cause? BlackEnergy malware. With so much of our daily lives reliant on computers, is modern civilization just a stream of ones and zeroes away from disaster?

Malware like BlackEnergy relies on uncorrected security flaws in computer systems. Sometimes, the system owner fails to install a patch. Other times, there is no patch because the software vendor either did not know about or did not correct a critical security flaw. Meanwhile, the victim country's government or its allies may have knowledge of the same flaw, but kept the information secret so that it could be used against its enemies.

There is an urgent need for a new legal and economic approach to cybersecurity that will curtail socially harmful behavior by security researchers and governments. Laws aimed at curbing cyberattacks typically focus on punishment, with little to no wiggle room provided for socially beneficial hacking behavior. Around the world, governments hoard zero-day vulnerabilities while permitting software vendors to sue security researchers who plan to demonstrate critical security flaws at industry conferences. There is also a growing market for buying and selling security flaws, and the buyers do not always have society's best interests in mind.

This Article delves into the world of cybersecurity and software and provides an interdisciplinary analysis of the current crisis, contributing to the limited but growing literature addressing these new threats that cannot be contained by traditional philosophies of war and weaponry. First, the Article presents an economic model to explore incentives for selling vulnerability information in

---

* Professor and H. Ross & Helen Workman Research Scholar, University of Illinois at Urbana-Champaign.

** Research Associate, University of Illinois at Urbana-Champaign. The authors wish to thank the members of the software and security communities who helped in the shaping of the proposal, including Chris Kuethe, Eduardo A. Vela Nava, and Don Hayes.

different types of markets. Then, it proposes and designs a revolutionary market for vulnerabilities aimed at facilitating legitimate, transparent, and vendor-focused transactions of critical security information at a fair market price. The proposal combines insights from economics, security, and law, and draws inspiration from around the world; from commodity futures markets in New York to archaeological sites in Iraq. The Article applies the marketplace proposal to several examples, demonstrating that it is a practical and achievable approach that will support socially desirable cybersecurity practices.

TABLE OF CONTENTS

INTRODUCTION

The Internet is a game changer, connecting people, businesses, and countries like never before in world history. Educational videos from the 1990s painted the Internet as a great tool to help Lisa with her homework and let Dad check the stock reports.[1] In the decades since, the Internet has proven to be much more than a useful tool. It is a new road that connects businesses to consumers and governments to citizens. It has dramatically reduced transaction costs to enable outstanding economic growth.[2] But new roads can be used by anyone with access to them. As former FBI Director Robert Mueller noted, the same roads that enabled the spread of Roman civilization also led invaders to Roman doorsteps.[3] This also applies in the arena of cybersecurity threats. General Keith Alexander, Director of the National Security Agency ("NSA"), declared that ongoing cyber thefts "represent the greatest transfer of wealth in human history."[4] The global nature of cybercrime complicates the enforcement of laws and rights, because investigators are much more constrained by borders than criminals.[5]

In 2014, experts estimated that cybercrime costs the global economy more than $400 billion every year.[6] The United States alone reportedly accounts for $100 billion of that total.[7] Harm from cybercrime includes the destruction and theft of information, but the harm can also be reputational or even physical. One careless network user who clicks on a phishing link in an email is sometimes all it takes.[8] The defender must simultaneously defend everywhere against everything, but all an attacker needs is one good day.[9]

---

1. *See, e.g.*, Eric Mack, *Revisit the Amazing Internet the Cool Kids Used in 1997*, CNET (Aug. 18, 2013, 12:43 PM), http://www.cnet.com/news/revisit-the-amazing-internet-the-cool-kids-used-in-1997/.

2. *See* Miriam A. Cherry, *Cyber Commodification*, 72 MD. L. REV. 381, 407 (2013).

3. Omer Tene, *A New Harm Matrix for Cybersecurity Surveillance*, 12 COLO. TECH. L.J. 391, 392 (2014).

4. Keith B. Alexander, *An Introduction by General Alexander*, 19 NEXT WAVE, no. 4, 2012, at 2.

5. Cassandra Kirsch, *The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law*, 41 N. KY. L. REV. 383, 383 (2014).

6. MCAFEE CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME 2 (June 2014), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

7. Dan Zureich & William Graebe, *Cybersecurity: The Continuing Evolution of Insurance and Ethics*, 82 DEF. COUNS. J. 192, 192 (2015).

8. *See* Taiwo A. Oriola, *Bugs for Sale: Legal and Ethical Proprieties of the Market in Software Vulnerabilities*, 28 J. MARSHALL J. COMPUTER & INFO. L. 451, 465 (2011) ("[T]he human link remains . . . a potent source of vulnerability in the computing and network systems security chain.").

9. *See* Rachel Rue & Shari Lawrence Pfleeger, *Making the Best Use of Cybersecurity Economic Models*, IEEE SECURITY & PRIVACY, July–Aug. 2009, at 52, 53 (discussing the Clark and Konrad cybersecurity model, and stating that "the defender [against a cyberattack] must defend every front, but the attacker need be successful on only one").

Those with cybersecurity knowledge have engaged in research efforts to limit the harmful use of this new road. The information security market has been thriving since the beginning of the millennium. In 2004, experts estimated the computer security market's value at $27 billion.[10] By 2014, estimated worldwide spending on information security products had jumped to over $70 billion.[11]

Even with this increase in investments, network security remains fragile. Invaders are always looking for new vulnerabilities to exploit, which may be human or technological in nature.[12] Security breaches have led to the theft of sensitive information from health insurance companies, retailers, banks, hotels, and more.[13] Hackers have exploited security vulnerabilities in operating systems, encryption software, firmware, and countless numbers of other software products.[14] Noah Susskind notes that over a billion data records have been compromised in data breaches, causing significant financial harm to U.S. companies.[15] Yet many companies fail to take basic steps to secure information in their systems. One study estimates that over 63% of businesses store customer credit card information in an unencrypted format, and that 7% of companies keep records of all of the information contained in the magnetic bar on the back of each

---

10. Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 308 (2006).

11. *Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware*, GARTNER: NEWSROOM (Aug. 22, 2014), http://www.gartner.com/newsroom/id/2828722.

12. *See* U.S. DEP'T HOMELAND SEC., COMMON CYBERSECURITY VULNERABILITIES IN INDUSTRIAL CONTROL SYSTEMS vii (2011), https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf ("[A]ttack strategies are constantly evolving to compensate for increasing defense mechanisms."). The DHS report addresses several categories of vulnerabilities, including improper input validation and network weaknesses. *Id.* at ix–xi.

13. Keith Collins, *A Quick Guide to the Worst Corporate Hack Attacks*, BLOOMBERG (Mar. 18, 2015), http://www.bloomberg.com/graphics/2014-data-breaches/; Andrea Peterson, *Wyndham Agrees to Settle with FTC in Case That Challenged Agency's Data Security Enforcement Powers*, WASH. POST: THE SWITCH (Dec. 9, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/12/09/wyndham-agrees-to-settle-with-ftc-in-case-that-challenged-agencys-data-security-enforcement-powers/.

14. *E.g.*, Andy Greenberg, *Why the Security of USB Is Fundamentally Broken*, WIRED (July 31, 2014, 3:00 AM), http://www.wired.com/2014/07/usb-security/ (discussing a vulnerability in the firmware of USB drives); Moony Li, *Hacking Team Leak Uncovers Another Windows Zero-Day, Fixed in Out-of-Band Patch*, TREND MICRO: TRENDLABS SEC. INTELLIGENCE BLOG (July 20, 2015, 6:56 PM), http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-leak-uncovers-another-windows-zero-day-ms-releases-patch/; Richard Nieva, *Heartbleed Bug: What You Need to Know (FAQ)*, CNET (Apr. 11, 2014, 11:13 AM PST), http://www.cnet.com/news/heartbleed-bug-what-you-need-to-know-faq/ (discussing a vulnerability affecting OpenSSL encryption software).

15. Noah G. Susskind, Note, *Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know*, 11 N.Y.U. J.L. & BUS. 573, 575 (2015); *see also Cost of Data Breach Grows as Does Frequency of Attacks*, PONEMON INST. BLOG (May 27, 2015, 6:00 AM), http://www.ponemon.org/blog/cost-of-data-breach-grows-as-does-frequency-of-attacks (noting that in 2015, the average cost per record lost in the United States was $217).

credit card.[16] Such careless data practices magnify the potential financial harm from exploitation of technological security vulnerabilities.

By exploiting security vulnerabilities, attackers can wrest control away from the rightful owners and operators of machines. One goal of exploitation may be the theft of confidential information. When individual computers are compromised, cyber criminals can also make those computers part of a botnet.[17] Access to these botnets can then be sold on black markets so that buyers can use them for purposes that include spam dissemination, brute force attacks, and distributed denial of service ("DDoS") attacks.[18] Attackers may also use ransomware that encrypts the victim's hard drive and demands payment to restore the owner's access.[19]

Security vulnerabilities are also exploited by governments. Indeed, many countries have entire units of their militaries dedicated to cyber operations.[20] The most infamous cyber incident to date is the harm caused by Stuxnet, which purportedly destroyed approximately 1,000 nuclear centrifuges in two of Iran's nuclear facilities.[21] Stuxnet exploited four zero-day vulnerabilities in the Windows operating system,[22] and the sophistication of its code makes it extremely likely that the culprit was a national government.[23] No one has come forward to take responsibility for Stuxnet, but some theorize that Stuxnet was produced through

---

16. *2014 Infographic – 63% of Businesses Don't Encrypt Credit Cards*, SECURITYMETRICS: BLOG (July 18, 2014), http://blog.securitymetrics.com/2014/07/businesses-dont-encrypt-credit-cards.html; Susskind, *supra* note 15, at 585.

17. Susskind, *supra* note 15, at 598. A "botnet" is a network of malware-compromised computers. *Bots and Botnets—A Growing Threat*, NORTON BY SYMANTEC, http://us.norton.com/botnet/ (last visited Aug. 2, 2016).

18. Susskind, *supra* note 15 at 598–99; *see generally* Jaziar Radianti, *A Study of a Social Behavior Inside the Online Black Markets*, 2010 FOURTH INT'L CONF. ON EMERGING SEC. INFO., SYS., & TECHS., (Juan E. Guerrero ed., IEEE) (discussing online black markets).

19. Adam Chandler, *How Ransomware Became a Billion-Dollar Nightmare for Businesses*, THE ATLANTIC (Sep. 3, 2016), http://www.theatlantic.com/business/archive/2016/09/ransomware-us/498602/.

20. Matthew Rinear, *Armed with a Keyboard: Presidential Directive 20, Cyber-Warfare, and the International Laws of War*, 43 CAP. U. L. REV. 679, 711–14 (2015).

21. Susanna Bagdasarova, *Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance*, 119 PENN. ST. L. REV. 1005, 1007–08 (2015).

22. Jarred Shearer, *W32.Stuxnet*, SYMANTEC (Feb. 26, 2013, 7:15 PM), http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99. A "zero-day vulnerability" is a security bug that is unknown to the software developer and the general public prior to being exploited for destructive purposes. Roger Park, *Guide to Zero-Day Exploits*, SYMANTEC CONNECT: BLOG (Nov. 9, 2015), http://www.symantec.com/connect/blogs/guide-zero-day-exploits. For a discussion of zero-day vulnerabilities, see *infra* Section II.B.1.

23. David Kushner, *The Real Story of Stuxnet*, IEEE SPECTRUM (Feb. 26, 2013, 2:00 PM), http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

joint efforts of Israel and the United States.[24] Stuxnet illustrates that cybersecurity is national security.

In addition to possible offensive uses, governments utilize cyber intrusion tools for defense and intelligence purposes.[25] Security vulnerabilities can even be exploited by national governments to violate their own citizens' rights.[26] The Syrian government allegedly exploited an Adobe Flash vulnerability to target its citizens who visited a government website that was set up to receive their complaints.[27] There is also evidence that the regime of former Egyptian President Hosni Mubarak at least considered purchasing commercial spyware to monitor activists and opponents.[28]

This Article is not about attacks, but rather what enables them to occur—bugs![29] Many bugs are technological security flaws that could be fixed, but fixing them becomes much harder when criminals and governments are fighting to see who can use these bugs the longest and still keep them secret. Our ambitious proposal to create and operationalize a legitimate and transparent market for software vulnerabilities is aimed at making it more attractive and more profitable to fix bugs instead of hoarding them.

In some ways, computer security is like medical vaccination. Seventy years ago, approximately 35,000 people contracted polio each year in the United States.[30] Less than 1% of those infected with polio, or approximately 300 people per year, suffered paralysis.[31] After the vaccine was introduced in 1955, infections dropped dramatically—to fewer than 2,500 cases in 1957.[32] Sixty years later, people are still receiving polio vaccinations, and as of 2015, the number of new

---

24. *Id.*

25. *Cf.* White House, The Comprehensive National Cybersecurity Initiative, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (last visited Aug. 19, 2016) (referring to CNCI's goals as including improvements to defense and intelligence).

26. Mailyn Fidler, Anarchy or Regulation: Controlling the Global Trade of Zero-Day Vulnerabilities 8 (May 2014) (B.A.H. thesis, Stanford University Center for International Security and Cooperation), http://purl.stanford.edu/zs241cm7504.

27. *Id.* at 20.

28. Karen McVeigh, *British Firm Offered Spying Software to Egyptian Regime – Documents*, THE GUARDIAN, (Apr. 28, 2011), http://www.theguardian.com/technology/2011/apr/28/egypt-spying-software-gamma-finfisher.

29. For a discussion of the popular myth that the use of the word "bug" to refer to software errors arose because Admiral Grace Hopper found a moth in a computer, see *Moth in the Machine: Debugging the Origins of 'Bug'*, COMPUTER WORLD (Sep. 3, 2011, 7:00 AM), http://www.computerworld.com/article/2515435/app-development/moth-in-the-machine--debugging-the-origins-of--bug-.html.

30. *Polio Disease – Questions and Answers*, CTR. DISEASE CONTROL & PREVENTION (AUG. 11, 2014), http://www.cdc.gov/vaccines/vpd-vac/polio/dis-faqs.htm.

31. *Id.*

32. *Id.*

infections has dropped to just a few dozen worldwide.[33] Part of the success of vaccination programs is due to so-called "herd immunity," which protects those with weaker immune systems who cannot be vaccinated.[34] Likewise, computer communities benefit from pervasive and effective computer security practices.[35] But when even a small percentage of the community avoids preventative measures, the effectiveness of herd immunity plummets.[36] This reality emphasizes the need for consistent use of security technology.

In security, as with vaccinations, the controlled application of potentially harmful elements can create a stronger and more resilient environment.[37] Vaccines are often manufactured by using a weakened form of the virus.[38] This way, the immune system can steel itself against stronger versions of the virus and immunity is achieved.[39] Security researchers and even some mischievous hackers can provide a similar benefit for computer security.[40] Our proposal is fundamentally about helping these parties transfer their information to vendors who can fix security holes.

In the pursuit of inoculation, this Article focuses on the discovery, exploitation, and repair of technological security vulnerabilities, and proposes a market-based solution that improves upon existing vulnerability markets. This Article examines the policy implications of today's vulnerability markets, in which computer security may be sold to the highest bidder. We primarily use the term "vulnerability market," but we also distinguish between vulnerabilities and exploits. Vulnerabilities are security flaws, and exploits are weaponized vulnerabilities. In vulnerability markets, the vulnerability information or exploit is transferred to someone else to use as he or she wishes.

Most people likely think of antivirus companies and firewalls when they think of markets for information security products. Part of the information security market emphasizes defense, but there is a parallel market for offensive use of

---

33. *Polio Cases Worldwide*, POLIO GLOB. ERAD. INIT. http://www.polioeradication.org/Dataandmonitoring/Poliothisweek/Poliocasesworldwide.aspx (last visited Aug. 2, 2016).

34. *Community Immunity ("Herd Immunity")*, VACCINES.GOV, http://www.vaccines.gov/basics/protection/ (last visited Aug. 19, 2016) [hereinafter *Community Immunity*].

35. *Herd Immunity and Security in a Networked World*, MCAFEE: BUSINESS BLOG (Aug. 1, 2015), https://blogs.mcafee.com/business/herd-immunity-security-networked-world/.

36. *Community Immunity*, *supra* note 34.

37. For a discussion of how this theory applies to information security, see Note, *Immunizing the Internet, Or: How I Learned to Stop Worrying and Love the Worm*, 119 HARV. L. REV. 2442 (2006) [hereinafter *Immunizing the Internet*].

38. CTR. DISEASE CONTROL & PREVENTION, UNDERSTANDING HOW VACCINES WORK 1 (2013), http://www.cdc.gov/vaccines/hcp/patient-ed/conversations/downloads/vacsafe-understand-color-office.pdf.

39. *Id.*

40. *See Immunizing the Internet*, *supra* note 37 ("In essence, certain cybercrime can create more benefits than costs, and cybercrime policy should take this into account.").

information security knowledge.[41] For example, profit-minded security researchers can sell discoveries to brokers who deal in vulnerabilities and exploits.[42] These brokers may then sell exploits to governments or research firms, either individually or through subscription services.[43] There are also secretive black markets where terrorists or other criminals can purchase security exploits.[44] Offense-focused markets are plagued by questions of legitimacy and a lack of transparency.[45]

Commentators sometimes characterize vulnerability markets as being black, grey, or white.[46] This Article uses the term "black market" to refer to markets where there is malicious intent and, as is often the case, an emphasis on the targeting of individuals or private companies. A "white market," in contrast, is one where the vulnerability sales are almost exclusively made to the distributor of the vulnerable product. For example, the bug-bounty programs that many software companies operate are considered white markets.[47]

Somewhere in between dark-alley criminal enterprises and bug-bounty programs there is a very substantial "grey market."[48] In grey markets, buyers may be security research firms that will use the information for penetration testing.[49] National governments are also active in grey markets, where they might purchase vulnerability information and exploits for defensive, offensive, or intelligence purposes.[50] The grey market also includes vulnerability brokers like Zerodium that publicly advertise their desire to purchase vulnerabilities and exploits with an apparent intent to resell that information to other grey market actors.[51]

Black and grey markets are both problematic, even when putting aside concerns about the buyers' intentions. Because of the nonexclusive nature of

---

41. *E.g.*, Jose Pagliery, *Meet Zerodium, the Company that Pays $1 Million for Apple Hacks*, CNN: MONEY (Apr. 7, 2016, 4:55 PM), http://money.cnn.com/2016/04/07/technology/zerodium-apple-hacks/.

42. *Id.*

43. *Id.* ("In a sense, Zerodium is a cyber arms dealer. It pays hackers to learn about their tactics, then packages that and sells it to elite subscribers.")

44. Thomas Lee, *Dark Net Reveals How Hackers Exploit Vulnerabilities*, SFGATE (Jun. 28, 2014, 8:38 AM), http://www.sfgate.com/technology/article/Dark-Net-reveals-how-hackers-exploit-5585720.php.

45. *See* Marc Blackmer, *The Good, Bad, and Ugly of Vulnerability Markets*, SEC. LEDGER (July 27, 2016, 9:42 AM), https://securityledger.com/2016/07/the-good-bad-and-ugly-of-vulnerability-markets/.

46. *Id.*

47. *See generally* Andreas Kuehn & Milton Mueller, *Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities*, Presentation at the 42nd Telecomms. Policy Research Conf. (Sep. 13, 2014).

48. Blackmer, *supra* note 45.

49. Fidler, *supra* note 26, at 27.

50. *See* Andy Greenberg, *Inside Endgame: A Second Act for the Blackwater of Hacking*, FORBES: SEC. (Feb. 12, 2014, 9:00 AM), http://www.forbes.com/sites/andygreenberg/2014/02/12/inside-endgame-a-new-direction-for-the-blackwater-of-hacking/ (discussing a company that formerly sold exploits to governments).

51. *Our Exploit Acquisition Program*, ZERODIUM, https://www.zerodium.com/program.html (last visited Aug. 2, 2016).

information, neither sellers nor buyers can ensure that the vulnerability will not be found and exploited or fixed by someone else. This makes participation in these markets difficult and precarious. Moreover, an entity that purchases the vulnerability with the intent to use it is unlikely to disclose the vulnerability to the vendor to allow the vendor to fix it. The white market becomes more visible as more software firms offer bug bounties. Unfortunately, bug bounties are often just a fraction of what the researcher could earn if he or she sold the information to someone else.[52]

This Article recognizes and responds to the urgent need for legitimate and transparent vulnerability markets. The long-term goal for addressing vulnerability markets should emphasize incentives to sell on white markets instead of black or grey markets. Creating an incentive for freelance researchers to sell to those vendors who are able to fix these vulnerabilities will reduce the number of suppliers in socially harmful markets. With a lower number of suppliers, criminal organizations and governments will have to move their vulnerability discovery operations in-house. This could reduce the number of malicious actors who exploit the systems that many people rely on in every aspect of their lives.

Our proposal increases transparency through the use of a more formal market structure. We propose a multi-faceted market for vulnerabilities that will legitimize this often hidden market. In today's economy, information is a commodity. Vulnerabilities are also commodities and can be traded as such. Our solution to the problem of a hidden market for vulnerabilities is to create an Information Security Exchange ("Exchange") to allow participants to invest based on the direction they think the market will go. The Exchange would serve many purposes, including price discovery, threat classification, risk shifting, and mediation. At the center of this Exchange would be the Information Security Clearinghouse ("Clearinghouse") that would handle market transactions and mediate negotiations between buyers and sellers. There are already some vulnerability brokers, such as TippingPoint's Zero Day Initiative ("ZDI"), that act as intermediaries between researchers and the white market.[53] Together, the Exchange and the attached Clearinghouse go much further, opening the market up to speculation and hedging. The use of financial market models like commodity futures markets creates a forum for transparent market operation. These additional features provide the funding necessary to facilitate fair market transactions for an information product that has thus far been characterized by volatility. By providing a transparent marketplace, we hope that our proposed system will incentivize market transactions between vendors and researchers that will adequately reward security researchers without excessively burdening vendors.

In Part I, we explore and analyze cybersecurity issues using practical and policy-based perspectives. A thorough understanding of cybersecurity policy should be grounded in an appreciation of the technology, the relevant actors, and the existing legal and technological means of addressing these problems. In Part II,

---

52. *See Zerodium's Million Dollar iOS 9 Bug Bounty (Expired)*, ZERODIUM, https://www.zerodium.com/ios9.html (last visited Aug. 2, 2016).

53. *Zero Day Initiative Program Benefits*, TIPPINGPOINT, http://www.zerodayinitiative.com/about/benefits/ (last visited Aug. 2, 2016).

we narrow our focus to vulnerabilities and the emerging markets. Cybersecurity threats have both technological and economic aspects, both of which our proposal addresses. An understanding of the conditions that enable cyberattacks is necessary to identify a remedy. In Part III, we discuss a variety of noncybersecurity markets, including commodity futures markets for legitimate investors and international black markets for those who deal in looted antiquities. These markets provide insights that can be used to shape legitimate and transparent vendor-focused vulnerability markets. In Part IV, we propose a transparent, market-based, and vendor-focused solution for the trade of vulnerabilities. We also present an economic model to outline the most important factors to consider for improving the white market for vulnerabilities. The inoculation of the Internet requires incentives for socially beneficial security research and behavior. Information security risks are not going away, but they can be lessened through the creation of a transparent, self-sustaining marketplace for vendor-focused vulnerability exchanges.

I. CYBER THREATS AND DEFENSES

Hacking has grown in visibility over the last decade. In 2007, unidentified attackers hit Estonian government systems with politically motivated cyberattacks.[54] In 2008, cyberattacks against Georgia coincided with the beginning of its war with Russia.[55] In 2010, discussions of cyberwar exploded when researchers discovered Stuxnet, a pernicious and resilient worm that exploited four zero-day vulnerabilities in order to sabotage nuclear centrifuges in Iran.[56] Some scholars consider Stuxnet to be an anomaly because the Stuxnet attacks actually had physical effects, while most cyberattacks do not.[57] We disagree. Stuxnet was not an anomaly—it was a harbinger that exposed the increasingly ambiguous divide between the digital and physical realms. As evidence, consider the December 2015 cyberattack that reportedly caused a massive power outage in Ukraine lasting for several hours.[58]

---

54. *See* Brian Fung, *How Russia Could Easily Hack Its Neighbors' Elections*, WASH. POST: THE SWITCH (May 13, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/05/13/how-russia-could-easily-hack-its-neighbors-elections/ (addressing the vulnerability of Estonia's election system).

55. Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 447 (2012) [hereinafter Kesan & Hayes, *Counterstriking*]; *Russian Cyber Attacks on Ukraine: The Georgia Template*, CHANNEL 4 NEWS (May 3, 2014), http://www.channel4.com/news/ukraine-cyber-warfare-russia-attacks-georgia.

56. *See* Roland L. Trope & Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks That Target and Degrade the Grid*, 40 WM. MITCHELL L. REV. 674, 675 (2014).

57. Gary D. Brown & Andrew O. Metcalf, *Easier Said Than Done: Legal Reviews of Cyber Weapons*, 7 J. NAT'L SEC. L. & POL'Y 115, 115 (2014).

58. James Titcomb, *Ukrainian Blackout Blamed on Cyber-Attack*, THE TELEGRAPH (Jan. 5, 2016), http://www.telegraph.co.uk/technology/news/12082758/Ukrainian-blackout-blamed-on-cyber-attack-in-world-first.html.

After the discovery of Stuxnet in 2010, cyberattacks continued to proliferate, and 2011 soon earned the title of "the Year of the Hack."[59] Prominent targets included government contractors,[60] security technology firms,[61] and entertainment companies like Sony Computer Entertainment.[62] Hacktivism also gained global attention with events like Operation Arab Spring, where political activists were supported by the loose-knit hacker collective Anonymous.[63] One of 2011's high-profile targets was federal cybersecurity contractor HBGary Federal. When company leaders announced that they were preparing to unmask Anonymous, the hacker collective responded by breaking into HBGary Federal's systems and downloading sensitive information from company email accounts.[64]

The 2011 attacks called attention to cybersecurity matters, but this was far from the end of the struggle against cybercrime. In 2013, Target suffered a major security breach during the holiday shopping season when hackers stole millions of payment records.[65] The Target breach may have affected as much as one-third of the U.S. population.[66] In November 2014, hackers released mountains of sensitive information from servers at Sony Pictures Entertainment[67] and threatened further harm if Sony Pictures went forward with its planned release of *The Interview*, a

---

59. Kirsch, *supra* note 5, at 383.

60. *See* Peter Bright, *With Arrests, HBGary Hack Saga Finally Ends*, ARS TECHNICA (Mar. 10, 2012, 1:15 PM), http://arstechnica.com/tech-policy/2012/03/the-hbgary-saga-nears-its-end/ (discussing the hack of a security firm); Robert Johnson, *The Biggest Hacking Attacks of 2011*, BUSINESS INSIDER (June 13, 2011, 4:05 PM), http://www.businessinsider.com/imf-cyber-attacked-hackers-sony-rsa-lockheed-martin-epsilon-michaels-2011-6?op=1 (discussing how hackers infiltrated Lockheed Martin using stolen SecurID codes); Gerry Smith, *Jeremy Hammond, Anonymous Hacker, Pleads Guilty to Stratfor Attack*, HUFFINGTON POST (May 28, 2013. 3:22 PM), http://www.huffingtonpost.com/2013/05/28/jeremy-hammond-anonymous-hacker-guilty-stratfor_n_3347215.html (discussing the aftermath of an attack on Stratfor, a "company that provides geopolitical analysis for clients" including government agencies).

61. John Markoff, *SecurID Company Suffers a Breach of Data Security*, N.Y. TIMES, Mar. 18, 2011, at B7. RSA Security offers multifactor authentication through the use of tokens. David Strom, *EMC RSA Authentication Manager and SecurID Multifactor Authentication Product Overview*, TECHTARGET: BUYER'S GUIDE (Jan. 2015), http://searchsecurity.techtarget.com/feature/Multifactor-authentication-products-EMC-RSA-Authentication-Manager-and-SecurID.

62. John Gaudiosi, *Why Sony Didn't Learn From Its 2011 Hack*, FORTUNE (Dec. 24, 2014), http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/.

63. Yasmine Ryan, *Anonymous and the Arab Uprisings*, AL JAZEERA: POLITICS (May 19, 2011), http://www.aljazeera.com/news/middleeast/2011/05/201151917634659824.html.

64. *See* Brown & Metcalf, *supra* note 57, at 126 ("Unfortunately, [the CEO] failed to follow a basic rule—before taking on a hacker group, ensure your computer systems are secure.").

65. Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG (Mar. 13, 2014), http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

66. Kirsch, *supra* note 5, at 384.

67. Ryan, *supra* note 63.

comedy about journalists traveling to North Korea.[68] In March 2015, Premera Blue Cross announced that it had been hacked, resulting in the leak of the health records of eleven million people.[69] Later in 2015, the federal Office of Personnel Management ("OPM") announced its discovery of a massive theft of the personal information of government employees and applicants for security clearances.[70] While only a few million people were initially thought to be affected by the OPM hack, that number soon leapt to 21.5 million.[71]

Sometimes, cybercrime victims are noteworthy because of who they are. Hacking Team, for instance, is an Italian company that sells spyware tools to national governments.[72] In a fit of cosmic irony, Hacking Team was hacked in July 2015, and the culprit published the company's internal documents for all to see.[73] The leak included invoices, emails, and some of the company's tools.[74] Another striking example is the Equation Group, a group of hackers identified by security researchers who say that the group's skill and resources make it likely that they have ties to the NSA.[75] In August 2016, a hacker group named ShadowBrokers released hacking tools and promised the auction of more tools that were stolen during a hack of Equation Group's servers.[76]

Over the last several years, many of the publicized attacks on private companies have involved "SQL injections," a very popular and effective method of hacking.[77] SQL stands for "Structured Query Language," which is a coding language that is commonly used for managing large databases.[78] In some instances, website code is written in a way that permits the user to use the input field to give the system more commands.[79] An SQL injection essentially interrupts

---

68. Julia Boorstin, *The Sony Hack: One Year Later*, CNBC (Nov. 24, 2015, 4:42 PM), http://www.cnbc.com/2015/11/24/the-sony-hack-one-year-later.html.

69. Jim Finkle, *Premera Blue Cross Hacked, Medical Information of 11 Million Customers Exposed*, HUFFINGTON POST (Mar. 17, 2015), http://www.huffingtonpost.com/2015/03/17/premera-blue-cross-cybera_n_6890194.html.

70. *See* Jonathan Chew, *China Says It Wasn't Behind the Massive U.S. Government Hack*, FORTUNE (Dec. 2, 2015, 8:52 AM), http://fortune.com/2015/12/02/china-opm-hack/.

71. *Id.*

72. Joseph Cox, *The FBI Spent $775K on Hacking Team's Spy Tools Since 2011*, WIRED (Jul. 6, 2015), https://www.wired.com/2015/07/fbi-spent-775k-hacking-teams-spy-tools-since-2011/.

73. *Id.*

74. *Id.*

75. Dan Goodin, *Confirmed: Hacking Tool Leak Came from "Omnipotent" NSA-Tied Group*, ARS TECHNICA (Aug. 6, 2016, 2:09 PM), http://arstechnica.com/security/2016/08/code-dumped-online-came-from-omnipotent-nsa-tied-hacking-group/ [hereinafter Goodin, *Confirmed*].

76. *Id.*

77. Kirsch, *supra* note 5, at 395; *see also* Joseph Cox, *The History of SQL Injection, The Hack That Will Never Go Away*, VICE: MOTHERBOARD (Nov. 20, 2015, 8:00 AM), http://motherboard.vice.com/read/the-history-of-sql-injection-the-hack-that-will-never-go-away.

78. *Cox*, *supra* note 72.

79. *Id.*

the existing commands and inserts new commands by using similar syntax.[80] For example, the input may include a semicolon to indicate the end of the line within the input, followed by more text.[81] The computer then interprets the text after the semicolon as being a new command, instead of just being part of the contents of the input field.[82] This idea is demonstrated in a popular xkcd comic,[83] presented in Figure 1 below.

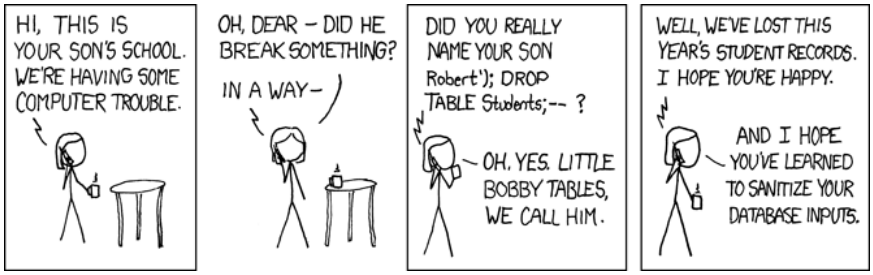

Figure 1: "Exploits of a Mom"

In the comic, the input "Robert');" tells the school's computer that the input ends with "Robert." The injected command is "DROP TABLE," a command that will delete a database.[84] The student records were lost because the injected code instructed the computer to delete the database named "Students." The hacker here relied on the semicolon being interpreted as the end of the input, and that the student records database would actually be named "Students." SQL injections are just one possible type of exploit.

Software products inherently have bugs, and some of these bugs are security flaws that allow outsiders to exercise some control over the system.[85] Vulnerabilities in SQL code are just one example. After identifying a place for an SQL injection, the hacker might then write a tool to take advantage of this vulnerability, perhaps as a "Trojan horse" attached to something the user wants to install.[86] Once this tool has been written, the aim is to infiltrate a system that the

---

80. *See id.* (discussing mitigation methods to avoid SQL injections that use syntax to change the system's operations).

81. Andy Lester, *Bobby Tables: A Guide to Preventing SQL Injection*, http://bobby-tables.com/ (last visited Aug. 22, 2016).

82. *Id*.

83. Randall Munroe, *Exploits of a Mom*, XKCD, http://xkcd.com/327/ (last visited Aug. 2, 2016).

84. *14.1.29 DROP TABLE Syntax*, MYSQL: 5.7 REFERENCE MANUAL, http://dev.mysql.com/doc/refman/5.7/en/drop-table.html (last visited Aug. 28, 2016).

85. Paco Hope, *Bugs Versus Flaws: Know What You're Up Against, Business Computing World*, BCW (May 29, 2013), http://www.businesscomputingworld.co.uk/bugs-versus-flaws-know-what-youre-up-against/.

86. Hahn & Layne-Farrar, *supra* note 10, at 290. Trojan horses are also known as "Trojans." *See Trojan Horse*, SYMANTEC, https://www.symantec.com/security_response/writeup.jsp?docid=2004-021914-2822-99 (last visited Sept. 12, 2016).

hacker wants to compromise.[87] Traditionally, this required the target to actually open an executable file, but hackers have also successfully embedded malware in word processing and PDF files.[88] Additionally, a malicious hacker can infect website visitors with a Trojan by using an iframe tag to create an invisible frame where the malicious code rests, or through the use of malicious script language.[89]

A hacker targeting an institution will often need credentials to gain access. There are many possible ways of obtaining these, but arguably one of the most effective methods is phishing, which exploits a different type of vulnerability—the human operator. Phishing scams have long been an effective way to obtain access, and the fallout from these scams can be very expensive.[90] When one company employee falls victim to a phishing attack that also involves malware, this puts other company computers at risk.[91] Even if a hacker obtained only one employee's credentials, this may still be enough to facilitate a large-scale theft of customer information or intellectual property.[92]

Security breaches like these are a major area of concern. Susskind notes that in 2014, reported cybersecurity incidents rose 48%.[93] But detection of these breaches is not always easy. Citing a study by Verizon, Deborah Norris Rodin makes the alarming observation that 70% of the time a company does not know that it has experienced a security breach until informed by a third party.[94]

Security breaches are costly to companies: they harm systems, degrade business operations, and damage consumer confidence.[95] A 2015 study estimated that when confidential information is stolen in the United States, the cost of addressing the breach averages $217 for each breached record.[96] Sony Computer Entertainment is said to face $170 million in costs as a result of the 2011 attacks—

---

87. *Id.*

88. Leyla Bilge & Tudor Dumitras, *Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World*, 19 ACM CONF. ON COMPUTER & COMMS. SEC. 833, 837 (2012).

89. Jianwei Zhuge et al., *Studying Malicious Websites and the Underground Economy on the Chinese Web*, *in* MANAGING INFORMATION RISK AND THE ECONOMICS OF SECURITY 236–37 (M.E. Johnson ed., 2009).

90. *See* Hahn & Layne-Farrar, *supra* note 10, at 290 ("According to one research firm, phishing scams cost banks and credit-card issuers more than $1.2 billion in 2004.").

91. Michelle Starr, *Oh-oh, This Computer Virus Can Spread Via Wi-Fi*, CNET: TECH CULTURE (Feb. 27, 2014, 12:54 PM), http://www.cnet.com/news/uh-oh-this-computer-virus-can-spread-via-wi-fi/.

92. Doug Olenick, *Phishing, POS and Stolen Credentials Top Data Breach Methods: Verizon*, SC MAGAZINE (Apr. 27, 2016) http://www.scmagazine.com/phishing-pos-and-stolen-credentials-top-data-breach-methods-verizon/article/492641/.

93. Susskind, *supra* note 15, at 574–75.

94. Deborah Norris Rodin, Note, *The Cybersecurity Partnership: A Proposal for Cyberthreat Information Sharing Between Contractors and the Federal Government*, 44 PUB. CONT. L.J. 505, 520–21 (2015).

95. Hahn & Layne-Farrar, *supra* note 10, at 303.

96. PONEMON INST., 2015 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 2 (2015), http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03053wwen/SEW03053WWEN.PDF; *see also* Zureich & Graebe, *supra* note 7, at 195 (discussing earlier Ponemon Institute studies).

not including class action settlements.[97] Regulators may impose additional costs on companies that fail to take basic precautions, like maintaining firewalls, updating antivirus software, and encrypting sensitive information like passwords and credit card numbers.[98]

The Federal Trade Commission has some authority in this arena. In *FTC v. Wyndham Worldwide Corp.*, the Third Circuit Court of Appeals held that the FTC can sue companies with inadequate security practices under Section 5 of the FTC Act in order to prevent unfair or deceptive acts or practices.[99] However, the FTC tends to rely on ad hoc adjudication, and the penalties authorized under Section 5 may be inadequate to deter bad security behavior.[100] The Third Circuit's *Wyndham* decision concerned the FTC's litigation against the Wyndham hotel group, which was first brought in 2012 after the discovery of multiple data breaches.[101] This litigation went on for several years before the parties settled.[102] Wyndham stored customer credit cards in an unencrypted format and did not use firewalls.[103] Further, individual hotels were often connected to Wyndham's central network with easily discoverable default usernames and passwords.[104] In spite of these shortcomings, the final settlement with the FTC only addressed future monitoring and did not include any financial penalties.[105]

The *Wyndham* litigation concerned the theft of a large amount of customer credit card information.[106] The danger that a thief could make purchases with a stolen credit card is very real, but the threat goes beyond dollars and cents. Every industry that uses computers and the Internet needs effective cybersecurity. In the legal field, safeguarding client information has become an ethical matter, not just a technological or financial matter.[107]

Critical infrastructure systems are especially at risk.[108] Most critical infrastructure is owned and operated by the private sector, so security practices can vary significantly.[109] Rodin notes that in 2012, attackers compromised Telvent, a company that provides information technology services to operators of oil and gas

---

97. Roberta D. Anderson, *Viruses, Trojans, and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz*, 49 TORT TRIAL & INS. PRAC. L.J. 529, 541 (2014).

98. *See* Susskind, *supra* note 15, at 584 (addressing CorporateCarOnline's failure to use encryption or update their firewalls prior to that company's data breach).

99. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 236 (3d Cir. 2015).

100. *See* 15 U.S.C. § 45(b) (2012) (setting forth procedures for actions brought under this section).

101. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014).

102. Peterson, *supra* note 13.

103. *Wyndham Worldwide*, 10 F. Supp. 3d at 626.

104. *Id.*

105. Peterson, *supra* note 13.

106. *Wyndham Worldwide*, 10 F. Supp. 3d at 609.

107. Zureich & Graebe, *supra* note 7, at 193–94 (noting amendments that the American Bar Association has made to rules concerning ethics and cybersecurity practices).

108. "Critical infrastructure" refers to services relied upon throughout society, like transportation and electricity. *What Is Critical Infrastructure?*, DEP'T HOMELAND SEC., https://www.dhs.gov/what-critical-infrastructure (last visited Aug. 28, 2016).

109. *See* Trope & Humes, *supra* note 56, at 663; Susskind, *supra* note 15, at 577.

pipelines.[110] The Telvent intruders may have stolen sensitive information like blueprints and remote access codes for oil and gas pipelines across North and South America.[111] Cyber threats also endanger economic infrastructure. Financial actors on Wall Street are frequently targeted with DDoS attacks,[112] and hackers have compromised brokerage accounts to execute "hack, pump, and dump" schemes to manipulate the prices of penny stocks.[113] In 2013, hackers compromised the Twitter account of the Associated Press and sent out a false tweet about an explosion at the White House, causing the S&P 500 index to drop almost a full percentage point in just seconds.[114]

The critical information infrastructure underlying the Internet is another attractive target for attackers.[115] A survey by Symantec revealed that politically motivated cyberattacks affected approximately half of the providers of critical information infrastructure in 2010.[116] In December 2015, members of the media reported that unknown hackers were attempting to shut down the entire Internet by targeting vital servers with DDoS attacks.[117] Some threats to information infrastructure are physical, such as the repeated incidents of vandals cutting fiber-optic cables in California.[118] Whether physical or digital, vulnerabilities in critical information infrastructure can have national security implications due to the overlap between civilian and military networks.[119]

Even the most intelligent policymakers often do not understand the full ramifications of technological issues.[120] Bruce Schneier coined the term "security theater" to describe security proposals that provide the appearance of security, but

---

110. Rodin, *supra* note 94, at 506.

111. *Id*.

112. *Id.* at 511.

113. Jose Pagliery, *JPMorgan's Accused Hackers Had Vast $100 Million Operation*, CNN MONEY (Nov. 10, 2015, 5:27 PM), http://money.cnn.com/2015/11/10/technology/jpmorgan-hack-charges/.

114. Christopher Matthews, *How Does One Fake Tweet Cause a Stock Market Crash?*, TIME (Apr. 24, 2013), http://business.time.com/2013/04/24/how-does-one-fake-tweet-cause-a-stock-market-crash/.

115. *See generally* David Satola & W.J. Luddy, Jr., *The Potential for an International Legal Approach to Critical Information Infrastructure Protection*, 47 JURIMETRICS J. 315, 316 (2007) (discussing a variety of elements relating to critical information infrastructure).

116. Oriola, *supra* note 8, at 454.

117. Mary-Ann Russon, *Mysterious Hackers Attempting to Bring Down Entire Internet by DDoS-ing Critical Servers*, INT'L BUS. TIMES (Dec. 10, 2015, 15:08), http://www.ibtimes.co.uk/mysterious-hackers-are-trying-bring-down-entire-internet-by-ddos-ing-critical-servers-1532762.

118. Trevor Hughes, *Attackers Sever Fiber-Optic Cables in San Francisco Area, Latest in a String*, USA TODAY (Sep. 16, 2015, 10:51 AM), http://www.usatoday.com/story/tech/2015/09/15/att-fiber-optic/72340020/.

119. Tene, *supra* note 3, at 398.

120. Lorenzo Franceschi-Bicchierai, *Congress Talks About 'Cybersecurity' More Than Ever, But Still Doesn't Get It*, VICE: MOTHERBOARD, (Nov. 9, 2015, 12:50 PM), http://motherboard.vice.com/read/congress-talks-about-cybersecurity-more-than-ever-but-still-doesnt-get-it.

might not actually improve it.[121] In this Part, we explore some of the nuances and possible responses to the threat. Having a more thorough understanding of the security environment will likely be helpful in avoiding meaningless security theater.

A. Characterizing Hackers

Attacks vary significantly in complexity and impact,[122] as do the abilities and intentions of the attackers. One study estimates that highly skilled hackers with malicious intent make up only 1% of the total hacker population.[123] This 1% may be responsible for many of the high complexity and high impact cyber incidents. The remaining hackers either have a low skill level or are not malicious.[124]

Hackers are often described as wearing white, grey, or black hats.[125] We view these three hat colors as representing a morality scale based on the hacker's intentions—good, neutral, or evil. Hackers are often considered to be black hats when they violate the law,[126] but law and morality are not the same. A more detailed categorization of hackers would be possible if we introduced an ethics scale that examines how much a hacker prioritizes the rule of law. In the terminology of the popular role-playing game *Dungeons and Dragons*,[127] the points on the ethics scale would be lawful, neutral, and chaotic.[128] Lawful actors prioritize following the law, neutral actors do not view it as an ultimate authority, and chaotic actors may actively work to subvert it.[129] The chart below suggests what types of activity might fall within each alignment, where the moral good-to-evil scale is based on the intentions of the actor.

---

121. Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951, 968 (2006); *See* Bruce Schneier, *Beyond Security Theater*, SCHNEIER ON SECURITY (Nov. 13, 2009, 6:52 AM), https://www.schneier.com/blog/archives/2009/11/beyond_security.html.

122. *See The Two Faces of Hacking*, IEEE SPECTRUM (July 2, 2011, 1:19 AM), http://spectrum.ieee.org/static/hacker-matrix.

123. Hahn & Layne-Farrar, *supra* note 10, at 296.

124. *Id.*

125. Kirsch, *supra* note 5, at 386.

126. *See* Nadia Kovacs, *What Is the Difference Between Black, White, and Grey Hat Hackers?*, NORTON: PROTECTION BLOG (Apr. 17, 2015, 8:50 AM), https://community.norton.com/en/blogs/norton-protection-blog/what-difference-between-black-white-and-grey-hat-hackers (listing two factors to determine what color of hat a hacker is wearing: his or her motivations, and whether he or she is breaking the law).

127. In Dungeons and Dragons, players create characters from a range of possible races (including humans and elves) and classes (including barbarians and wizards) and craft the characters' internal motivations. *See* DUNGEONS AND DRAGONS PLAYER'S HANDBOOK 4 (Kim Mohan et al. eds., 2003). Players often meet for a few hours at a time and play the game through multiple sessions, using dice and their imaginations to propel their characters through elaborate fantasy-based storylines.

128. *Id.* at 103–04.

129. *Id.* at 104.

The Morality Axis	The Ethics Axis: Lawful	The Ethics Axis: Neutral	The Ethics Axis: Chaotic
Good	Hacker hired by vendor to look for vulnerabilities in vendor's product	Unauthorized testing to find vulnerabilities that should be fixed for the public good	Hacktivism
Neutral	Governments using vulnerability knowledge to improve defense	Curiosity-motivated hacking	Hacking for amusement ("for the lulz")
Evil	Governments using court-approved spyware to suppress dissent	Digital fraud or theft	Hacking to harm—e.g., DDoS, data theft, and ransomware

Table 1: Hacker Alignment

The problem with current laws governing cybercrime is that they reject the utility of anything in the neutral and chaotic columns.[130] Further, actions that violate the law often get characterized as black hat actions regardless of intent. Cassandra Kirsch suggests that grey hat hackers should be viewed as potential allies.[131] Expounding on this idea, categorizing hackers based on intent (The Morality Axis) and lawfulness (The Ethics Axis) reveals different types of hackers, many of whom could be helpful, and the various motivations that drive them. These are the potential market actors whose participation in a vendor-focused vulnerability market will be the most valuable. By considering their different motivations, we can better design the right incentives for each hacker alignment.

B. Cybersecurity Regulation

Over the last thirty years, policymakers around the world have become more aware of the threats facing an increasingly connected and digitized world. In the United States, legislators became concerned about the scenarios depicted in the 1983 film *WarGames*,[132] which contributed to the enactment of the Computer Fraud and Abuse Act ("CFAA") in 1986.[133]

International regulatory solutions have evolved with the introduction of new threats. In 2007, Germany criminalized the distribution of hacking tools with

130. The Computer Fraud and Abuse Act, for instance, criminalizes unauthorized access to and actions that damage protected computers, in many cases without concern for the offender's motivations. *E.g.*, 18 U.S.C. § 1030(a)(2) (2012) (obtaining information through intentional unauthorized access).

131. Kirsch, *supra* note 5, at 385–86.

132. WARGAMES (United Artists 1983).

133. H.R. Rep. No. 98-894, at 10–11 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3689; Kirsch, *supra* note 5, at 392.

a law that might be broad enough to encompass the market for vulnerabilities.[134] China has a high imprisonment rate for crime that occurs online, especially compared to other countries.[135] The European Convention on Cybercrime attempts to harmonize national laws and encourage cross-border cooperation in investigations.[136] Marietje Schaake, a member of European Parliament, has expressed interest in a law that would restrict the distribution of hacking tools to oppressive governments.[137] In 2015, the Wassenaar Arrangement, an export control agreement for dual-use goods, was amended to include "intrusion software" and products that are used in or interact with intrusion software.[138]

In the United States, the CFAA remains the primary federal cybercrime statute, though some question the government's enforcement patterns. A majority of referred CFAA cases are left unprosecuted due to lack of evidence,[139] while CFAA prosecutions that do go forward sometimes play fast and loose with what it means to access a computer without authorization.[140] Criminal laws like the CFAA are often viewed as an important tool against hackers. However, inconsistent applications of cybercrime laws threaten to discourage benevolent security research while encouraging the actions of malicious hackers who know that their odds of being caught and prosecuted are slim.[141] Some commentary even suggests that cybercrime that is more mischievous than malicious should be tolerated to some extent because of its possible benefits for the immune system of the Internet.[142] Ultimately, when the CFAA's effect is too coercive, more beneficial hacking activity is deterred, making it more difficult to improve security.[143] Instead, not only do security researchers worry about criminal prosecutions following unauthorized security tests, but they also worry about injunctions and

---

134. Fidler, *supra* note 26, at 57, 60.

135. Zhuge et al., *supra* note 89, at 232.

136. Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185, http://www.state.gov/documents/organization/131807.pdf; *see also* Fidler, *supra* note 26, at 123–24.

137. Fidler, *supra* note 26, at 66.

138. THE WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES: LIST OF DUAL-USE GOODS AND TECHNOLOGIES 210 (2015), http://www.wassenaar.org/wp-content/uploads/2015/08/WA-LIST-15-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf.

139. Hahn & Layne-Farrar, *supra* note 10, at 333.

140. *See* United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2014) (appending numbers to the end of a publicly accessible URL in order to view user email addresses); United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (violating a website's terms of service); Brian Fung, *The Justice Department Used This Law to Pursue Aaron Swartz. Now It's Open to Reforming It*, WASH. POST: THE SWITCH (Feb. 7, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/02/07/the-justice-department-used-this-law-to-pursue-aaron-swartz-now-its-open-to-reforming-it/ (automated downloading of academic articles using an authorized account).

141. *See Immunizing the Internet*, *supra* note 37, at 2455 (noting that penalties could be enormous for cybercrime that has beneficial effects).

142. *Id.* at 2442.

143. *Id.* at 2463.

civil liability when companies do not want their security flaws to be disclosed to the public.[144]

Administrative agencies in the United States wrestle with how to regulate when their areas of specialization intersect with cybersecurity. In 2015, the Bureau of Industry and Security at the U.S. Department of Commerce issued a proposed rule and request for comments concerning the implementation of the Wassenaar Arrangement.[145] The Securities and Exchange Commission has weighed in on cybersecurity as well, due to the effects that cybersecurity breaches could have on a company's stock valuation.[146] The FTC has investigated and subjected multiple companies to consent orders because of the companies' inadequate security practices.[147] Additionally, as noted previously, the Third Circuit recently upheld the FTC's authority to bring suit against a company for unfair business practices based on egregious security failures.[148]

The effectiveness of the available legal approaches is unclear. For example, in the United States, a common regulatory response to data breaches is to require disclosure after a data breach.[149] Companies also typically insert information about security practices and expectations in end user license agreements ("EULAs") or privacy policies.[150] Some scholars are skeptical of these approaches, however, in part because such practices do not provide effective feedback loops to improve self-correction.[151]

This Article asserts that other dominant approaches to regulation are also questionable. If the Wassenaar Arrangement restricts the legitimate market for vulnerabilities, this could drive market participants to the black market. Strengthening criminal laws and enforcement may primarily serve to deter more benevolent market actors while rewarding those who are better at evading detection. Regulatory agencies like the FTC are increasingly involved in these

---

144. *See infra* Section II.B.2.c.

145. Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. 28,853 (May 20, 2015).

146. *See* Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 NW. U.L. REV. 795, 823–24 (2013) [hereinafter Matwyshyn, *Speech*] (noting the issuance of guidance on the topic in 2011); Hahn & Layne-Farrar, *supra* note 10, at 306 (acknowledging the effect that security breaches can have on a company's stock price); Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCIENCE 610, 612 (2006) (same). *See generally* SEC: Division of Inv. Mgmt., No. 2015-02, IM GUIDANCE UPDATE (2015), http://www.sec.gov/investment/im-guidance-2015-02.pdf (discussing the cybersecurity of online investment activities).

147. Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L.J. 267, 283–84 (2016).

148. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 243 (3d Cir. 2015).

149. Most states have data breach laws, of which requiring notice after a breach is a common feature. *E.g.*, ARIZ. REV. STAT. ANN. §44-7501 (2015).

150. *E.g.*, *Your Security*, GOOGLE: PRIVACY, https://privacy.google.com/your-security.html (last visited Aug. 28, 2016).

151. Andrea M. Matwyshyn, *Hidden Engines of Destruction: The Reasonable Expectation of Code Safety and the Duty to Warn in Digital Products*, 62 FLA. L. REV. 109, 121–22 (2010) [hereinafter Matwyshyn, *Hidden Engines*].

issues, but their options for enforcement may not sufficiently deter harmful or negligent behavior.[152]

Punishment and export restrictions are only part of the equation. Ultimately, cybercrime will need to be addressed with a comprehensive approach that preserves incentives for benevolent or curiosity-based security research. This need is the foundation of our market-based proposal.

1. Cybersecurity Information Sharing

Recently, policymakers have considered an alternative model that emphasizes cybersecurity information sharing, especially between the government and the private sector.[153] Streamlining processes for security clearances could, for example, facilitate efforts by the government to pass along sensitive security information to private companies.[154] Ronald Trope and Stephen Humes, however, have argued that such information sharing might not be appealing to companies because of the burdens it imposes and its questionable benefits.[155]

Congressional interest in cybersecurity information sharing was piqued in 2015, perhaps as a result of the OPM hack, which brought the danger of security breaches very close to home for government employees.[156] In the OPM hack, over 20 million personal records were stolen, and these personal records covered all applicants who had previously been investigated for the purpose of receiving a security clearance—and often their families as well.[157] This may have contributed to a legislative environment more amenable to proposals for sharing information about cyber threats.

In October 2015, the Senate approved the Cybersecurity Information Sharing Act ("CISA").[158] CISA permits the voluntary sharing of cyber threat indicators and defensive measures.[159] At that time, CISA was just the latest bill to

---

152. *See* Andrea Peterson, *Wyndham Agrees to Settle with FTC in Case That Challenged Agency's Data Security Enforcement Powers*, WASH. POST: THE SWITCH (Dec. 9, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/12/09/wyndham-agrees-to-settle-with-ftc-in-case-that-challenged-agencys-data-security-enforcement-powers/ (discussing the settlement following *FTC v. Wyndham* in the Third Circuit, under which Wyndham is not obligated to pay any financial penalties).

153. *See* Exec. Order No. 13,691, 80 Fed. Reg. 9,349 (2015); *see also* Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015). In December 2015, CISA was largely incorporated into the Consolidated Appropriations Act of 2016. 114 H.R. 2029 (2015).

154. Rodin, *supra* note 94, at 520.

155. Trope & Humes, *supra* note 56, at 708.

156. *See* Chew, *supra* note 70 (addressing China's response to allegations that it was responsible for the OPM hack).

157. Lisa Rein, *The Chinese Didn't Just Hack Federal Employees. Journalists Were Swept Up in the Massive Breach, Too.*, WASH. POST: FEDERAL INSIDER (Dec. 14, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/12/14/the-chinese-didnt-just-hack-federal-employees-journalists-were-swept-up-in-the-massive-breach-too/.

158. S. 754, 114th Cong. (2015).

159. *Id.*

cause public outcry over threats to internet privacy.[160] But in a surprising move, House Speaker Paul Ryan inserted almost all of the language of the Senate-approved version of CISA into the Consolidated Appropriations Act of 2016,[161] an omnibus budget bill enacted in December of 2015 to prevent another government shutdown.[162] CISA permits private companies to share information with the government and provides a broad liability exemption protecting private entities from liability for action or inaction relating to this information.[163]

Cybersecurity information sharing raises substantial privacy concerns. Earlier legislative proposals that emphasized information sharing often used broad wording that threatened to encompass the communications and information of law-abiding citizens.[164] CISA requires irrelevant personal information to be redacted from disclosures, but does little to address how any wrongfully disclosed information should be treated. Instead, the statute gives that responsibility to the Attorney General and the Secretary of Homeland Security to address in the privacy and civil liberties guidelines. In June 2016, the Department of Homeland Security and the Department of Justice published the final guidelines for privacy and civil liberties concerns related to the implementation of CISA.[165] The guidelines require notifications to be sent when information is improperly disclosed and also address retention procedures for such information.[166]

Government agencies also sometimes request the voluntary participation of service providers to monitor information transiting their systems.[167] Online monitoring may include the content of transmissions, or it may be limited to metadata.[168] In the context of communications, metadata is the noncontent information of the transmission, including where the parties were located at the time of the communication, who the target was communicating with, and how long

---

160. Jay P. Kesan & Carol M. Hayes, *Creating a "Circle of Trust" to Further Digital Privacy and Cybersecurity Goals*, 2014 MICH. ST. L. REV. 1475, 1490–92 [hereinafter Kesan & Hayes, *Trust*] (discussing cybersecurity legislation in previous sessions of Congress).

161. Dominic Rushe, *Librarians and Privacy Advocates Ally to Condemn Cybersecurity Bill*, THE GUARDIAN (Dec. 9, 2015, 11:00 EST), http://www.theguardian.com/world/2015/dec/09/cisa-cybersecurity-bill-congress-american-library-association-letter.

162. Kyle J. Gilster, *Congress Passes Omnibus Spending and Tax Bill for 2016*, LEXOLOGY (Dec. 22, 2015), http://www.lexology.com/library/detail.aspx?g=5da04187-4a58-4ac2-a591-e68a16860120.

163. Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015).

164. *See* Kesan & Hayes, *Trust*, *supra* note 160, at 1500 (discussing the Cyber Intelligence Sharing and Protection Act).

165. DEP'T HOMELAND SEC., PRIVACY AND CIVIL LIBERTIES FINAL GUIDELINES: CYBERSECURITY INFORMATION SHARING ACT OF 2015 3 (2016), https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_(Sec%20105(b)).pdf.

166. *Id.*

167. *See NSA Spying on Americans*, ELEC. FRONTIER FOUND., https://www.eff.org/nsa-spying (last visited Aug. 28, 2016) (documenting evidence that AT&T cooperated with the NSA in surveillance of its customers).

168. *Id.*

the communication lasted.[169] Revelations by Edward Snowden in 2013 revealed that the NSA sought and received cooperation from telecommunications companies to collect metadata transiting through their systems.[170] A recent survey found that participants were often more concerned about the warrantless disclosure of content information than about the warrantless disclosure of metadata.[171] Indeed, courts have been uncertain about the extent to which noncontent information, such as geolocation data and call durations, requires a warrant.[172] However, the privacy concerns for both types of information are fundamentally the same. At the heart of surveillance is the desire to find out where someone went, with whom, and for how long; what he or she actually said is often secondary to these considerations.[173]

Suspicionless and warrantless information collection threatens the principles underlying the Fourth Amendment, even if it might not violate the Fourth Amendment itself.[174] Peter Swire cites the findings of the 1976 Church Committee in Congress, noting that, historically, intelligence activities have tended to expand further than intended.[175] The controversy is not limited to the United States. As Omer Tene observes, other governments looking to improve cyber defense have also considered monitoring transmissions online.[176]

Encouraging more information sharing between government agencies is less controversial and an area that could be improved.[177] The Federal Information Security Management Act imposes requirements on agencies and contractors, though practices vary based on the agency.[178] Standardizing information security practices across different agencies could improve overall security by avoiding the sort of variance that might make a particular agency an attractive target. Agency

---

169. *Id.*

170. Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on a Vast Scale*, N.Y. TIMES, Aug. 16, 2015, at A1.

171. Kesan, Hayes & Bashir, *supra* note 147, at 345.

172. *Compare* ACLU v. Clapper, 785 F.3d 787, 818 (2d Cir. 2015) (holding that the bulk collection of cell phone metadata was not authorized by Section 215 of the Patriot Act), *with* United States v. Davis, 785 F.3d 498, 498 (11th Cir. 2015) (holding that historical cell site location data are business records that could be collected from the service provider without a warrant), *and In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 600 (5th Cir. 2013) (same).

173. Tene, *supra* note 3, at 411.

174. Swire, *supra* note 121, at 968; *see also* Tene, *supra* note 3, at 398 ("In particular, emerging cybersecurity threats may require increasingly comprehensive programs for scanning mass quantities of information; yet such programs strain existing constitutional and legal frameworks.").

175. Swire, *supra* note 121, at 969.

176. Tene, *supra* note 3, at 392.

177. *See* Swire, *supra* note 121, at 951 (citing the 9/11 Report as criticizing "the lack of information sharing between law enforcement and intelligence agencies"); Hahn & Layne-Farrar, *supra* note 10, at 347 ("Most government agencies, however, pay little or no attention to security issues.").

178. Rodin, *supra* note 94, at 514.

standardization is part of the goal of President Obama's Cybersecurity National Action Plan, which was announced in February 2016.[179]

Another variety of information sharing concerns the security technology being used. In Executive Order 13,636, the Obama Administration focused on improving cybersecurity in the government and the private sector.[180] Executive Order 13,636 directed the National Institute of Standards and Technology ("NIST") to draft a set of voluntary standards, the Cybersecurity Framework, which could be adopted by operators of critical infrastructure.[181] Some critics question the wisdom of even voluntary cybersecurity standards, due to the risk that companies will adopt the bare minimum required to comply.[182] Providing a higher baseline than what might have existed before is valuable,[183] but the danger comes when agencies mistake practices that are *necessary* to improve security, and practices that are *sufficient* to improve security. On the other hand, mandatory regulations that apply to security features would be very difficult to implement and enforce.[184]

2. Cybersecurity and International Law

A major spot of contention concerns how laws governing relations between countries apply to international conflicts that are based on cyber operations. Russia reportedly utilized cyber operations during a recent conflict in Ukraine,[185] and experts allege that Stuxnet is the result of government research, perhaps through the coordinated efforts of the United States and Israel.[186]

The standards for cyberwar are still unclear under international law.[187] Concepts found in the Charter of the United Nations ("UN Charter"), like "use of force" and "armed attack," are fairly clear in conventional warfare,[188] but the UN Charter was written decades before cyber warfare was a threat. In addition to the

---

179. Press Release, White House, Office of the Press Sec'y, FACT SHEET: Cybersecurity National Action Plan (Feb. 9, 2016), https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

180. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (2013).

181. *Cybersecurity Framework*, NIST, http://www.nist.gov/cyberframework/ (last updated July 29, 2016).

182. Trope & Humes, *supra* note 56, at 734.

183. *Id.* at 707.

184. Hahn & Layne-Farrar, *supra* note 10, at 343.

185. Fidler, *supra* note 26, at 160.

186. Ellen Nakashima & Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, WASH. POST, June 3, 2012, at A1.

187. *See* Kesan & Hayes, *Counterstriking*, *supra* note 55, at 511 ("It is not completely clear what international framework should apply to cyberwarfare . . . ."). *See generally* NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael Schmitt ed., 2013) [hereinafter TALLINN MANUAL] (providing recommendations for applying international law to cyber conflicts).

188. U.N. Charter art. 2, para. 4 (prohibiting the use of force or threat of force); U.N. Charter art. 51 (permitting self-defense in response to an armed attack).

problem of determining when cyber operations become "uses of force," it is not even clear which (if any) tools of cyber operations are "weapons."[189]

A committee of experts put together by the UN concluded that international law does apply in cyberspace, but failed to clarify definitional issues.[190] Another collection of experts supported by NATO worked on a similar project, eventually publishing the Tallinn Manual in 2013.[191] The Tallinn Manual is a nonbinding document about how existing laws of war can be applied to cyber conflict, and includes a number of definitional recommendations.[192]

Cybersecurity tools are an example of dual-use goods under international law.[193] Dual-use goods are those that can be used either peacefully or offensively.[194] Established international law already includes treaties concerning dual-use goods, such as the Biological Weapons Convention. The Convention represents an attempt to find a workable compromise between the need for peaceful research into biological weapons, like developing a new anthrax vaccine, and the need to prohibit large scale research with ultimately destructive goals.[195] Recent changes to the Wassenaar Arrangement were likely made to address security software's dual-use nature in a similar way;[196] although, as a voluntary export control regime, restrictions on intrusion software distribution lack the force of law of a treaty.

The changes to the Wassenaar Arrangement do not represent the first time that governments attempted to address computer security concerns with export controls.[197] Encryption technology has long been considered a dual-use technology, and regulation of the export of encryption technology has waxed and waned since cryptography controls were first introduced by Congress in 1979.[198] Export restrictions on cryptography led to several incidents where researchers

---

189. Brown & Metcalf, *supra* note 57, at 115–16.

190. Fidler, *supra* note 26, at 118–19.

191. *Tallinn Manual Process*, NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, https://ccdcoe.org/tallinn-manual.html (last visited Aug. 2, 2016).

192. TALLINN MANUAL, *supra* note 187, at 1.

193. Sean Gallagher, *US to Renegotiate Rules on Exporting "Intrusion Software"*, ARS TECHNICA (Mar. 2, 2016, 4:00 AM), http://arstechnica.com/tech-policy/2016/03/us-to-renegotiate-rules-on-exporting-intrusion-software-under-wassenaar-arrangement/; Trey Herr & Paul Rosenzweig, *Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model*, 8 J. NAT'L SEC. L. & POL'Y 301, 302–03 (2015) (arguing that only the payload part of a cyberweapon is strictly military in nature, and that the propagation and exploit aspects of the product are dual-use).

194. *Controls on Dual-Use Goods*, GOV.UK: GUIDANCE (Sep. 12, 2012), https://www.gov.uk/guidance/controls-on-dual-use-goods (describing dual-use goods as goods that have both civil and military applications).

195. Fidler, *supra* note 26, at 126–27.

196. *Id.* at 20–21 (noting the influence that Marietje Schaake's push for laws addressing cybersecurity and human rights in the EU may have had on the changes to the Wassenaar Arrangement).

197. *Id.* at 82.

198. *Id.* at 84.

faced restrictions when attempting to present cryptography research at international conferences.[199]

The mass market for encryption became more liberalized about 15 years ago and, in an apparent victory for the industry, the barrier for encryption exports was very low by 2002.[200] Twenty years of uncertainty, however, is a long time; if the Wassenaar Arrangement's inclusion of intrusion software follows a similar trajectory as encryption export controls, it may be 2035 or later before national governments are prepared to address vulnerability markets. Our proposal seeks to avoid such a prolonged period of controversy. Cyber threats are real and immediate, and research should be encouraged and not derailed.

C. Technological Defensive Measures

Potential victims have many options for defense. Passive defense options include firewalls, antivirus software, encryption, and access controls.[201] The goal of passive defense is typically to prevent intrusions.[202] If these safeguards fail, active defense measures allow network owners to respond to events as they happen.[203]

Viewing active defense as a series of actions, we have argued that the first element of active defense is the use of intrusion detection systems.[204] Some recent research has examined ways to detect possible zero-day attacks by focusing on anomalous network activity.[205] Collaborative intrusion detection systems are another tool that can improve capabilities for detecting an attack.[206]

Once an intrusion has been detected, an active defense system operator might attempt a "traceback" to identify the origin of the attack.[207] Attribution of cyberattacks to individuals is notoriously difficult,[208] but technologies have improved to at least provide a better opportunity for identifying the attacking

---

199. Matwyshyn, *Speech*, *supra* note 146, at 809–10.

200. Fidler, *supra* note 26, at 90.

201. Kesan & Hayes, *Counterstriking*, *supra* note 55, at 457.

202. *See* ROBERT M. LEE, THE SLIDING SCALE OF CYBER SECURITY 2 (2015), https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240 (distinguishing passive defense from other approaches).

203. Kesan & Hayes, *Counterstriking*, *supra* note 55, at 460.

204. *Id*. at 475.

205. Ratinder Kaur & Maninder Singh, *A Survey on Zero-Day Polymorphic Worm Detection Techniques*, 16 IEEE COMMS. SURVS. & TUTS. 1520, 1533 (2014).

206. Kesan & Hayes, *Counterstriking*, *supra* note 55, at 475, 481–82.

207. *Id.* at 481–83.

208. *See* COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 139 (William A. Owens et al. eds., 2009).

machine.[209] Another option is to use "honeypots" to attract attackers and gather their information.[210]

The highest level of active defense is an actual counterstrike.[211] Some counterstrikes may be aimed at neutralizing an active threat, but others may have retribution as their goal.[212] Presently, there is no exception in the CFAA for cyber self-defense,[213] so any counterstrike is likely to violate the CFAA to the same degree as the initial attack.

The legality of active defense is a topic of considerable debate.[214] Even the identification stages of active defense may be legally ambiguous. Depending on how they are implemented, for example, proactive countermeasures like honeypots might violate the CFAA and wiretap laws.[215] Methods that provide unauthorized access to any system without consent are excluded from the definition of "defensive measure" in the recently enacted CISA.[216]

D. Other Defensive Measures

If the government fails to regulate vulnerability markets or adopt meaningful exceptions for cyber self-defense, the market will have to self-regulate to adapt to cybersecurity threats. If it remains difficult to identify attackers, one possibility would be to hold third parties liable for harm caused by hackers.[217] This is the current approach at the FTC.[218] Another promising approach is the use of insurance as a risk-shifting mechanism, though coverage of cyber incidents under traditional policies is often unclear.[219] For this reason, the introduction of specialized cyber insurance is growing in popularity.[220]

The costs of insurance and adopting new practices could potentially be overwhelming for small companies. To address this type of problem, Susskind proposes a tiered approach to improving security, where the steps to be taken are determined by a company's current security practices.[221]

---

209. *See* Hayley Tsukayama, *This Program Lets You Snap a Photo of Whoever's Trying to Hack You*, WASH. POST: THE SWITCH (Sep. 8, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/09/08/this-program-lets-you-snap-a-photo-of-whoevers-trying-to-hack-you/.

210. Kesan & Hayes, *Counterstriking*, *supra* note 55, at 471–72.

211. *Id.* at 475.

212. *Id.* at 475–76.

213. 18 U.S.C. § 1030 (2012) (providing exceptions for law enforcement but not other actors).

214. Kesan & Hayes, *Counterstriking*, *supra* note 55, at 475.

215. Oriola, *supra* note 8, at 505–06.

216. Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. § 102(7) (2015).

217. *Immunizing the Internet*, *supra* note 37, at 2462.

218. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 236 (3d Cir. 2015) (evaluating the FTC's authority to charge companies with unfair or deceptive business practices after a security breach).

219. Anderson, *supra* note 97, at 543.

220. *See generally id.* (discussing the growth of the cyber insurance market).

221. Susskind, *supra* note 15, at 580–81.

Ultimately, however, security is a moving target, and threats can emerge from anywhere. The most disturbing development over the last decade has arguably been the development of viable markets for zero-day exploits.[222] This is the arms trading of the twenty-first century, where battles often take place through the Internet. Some have asserted that government purchases of zero days should be considered legitimate,[223] but the idea of any government using this knowledge for cyberwar is not very comforting. The risk of collateral damage is high; with the current overlap between civilian and military networks, civilians can become digital refugees in a war that they cannot see and therefore cannot avoid.[224]

II. SOFTWARE VULNERABILITIES AND THE MARKET

In Part I, we examined a number of problems and attempted solutions associated with our increasingly networked world. In Part II, we drill down into the origin of information insecurity: the inherent vulnerabilities within systems designed and operated by humans.[225] One estimate is that 75% of information security breaches are due to flaws in software.[226] Many, if not most, of these breaches are probably a combination of software flaws and human error.[227]

Not all software packages are targeted equally. Harry Sverdlove reports that in 2012, Java was the most exploited endpoint software.[228] In 2015, that honor went to Adobe Flash Player, which remains a very popular target for hackers even as the market attempts to shift away from using the Flash Player plug-in on websites.[229]

The battles against security flaws are plagued by externality problems. As Ross Anderson and Tyler Moore keenly observe, "systems are particularly prone to failure when the person guarding them is not the person who suffers when they fail."[230] A single infected computer might inconvenience its user, but the aggregate

---

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

223. *See* LILLIAN ABLON ET AL., RAND CORP., MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA: HACKERS' BAZAAR 25, (2014) (stating that some "advocate for governments and security vendors to buy zero-day actively to keep them off the black market").

224. *See* Tene, *supra* note 3, at 400.

225. ABLON ET AL., *supra* note 223, at 34.

226. Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1060 (2011).

227. Kirsch, *supra* note 5, at 396.

228. Harry Sverdlove, *The Java Vulnerability Landscape*, NETWORK SEC., April 2014, at 9, 9.

229. Jeremy Kirk, *No Surprise Here: Adobe's Flash Is a Hacker's Favorite Target*, COMPUTER WORLD (Nov. 9, 2015, 4:33 AM PST), http://www.computerworld.com/article/3003062/security/no-surprise-here-adobes-flash-is-a-hackers-favorite-target.html.

230. Anderson & Moore, *supra* note 146, at 610; *see also* Jason Franklin et al., *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants*, 2007 ASSOC. COMPUTING MACH'Y CONF. ON COMPUTER & COMMS. SEC. 387, (discussing research about incentives to maintain security).

harm that it could do as part of a botnet is not a cost that the user has to bear.[231] Incentivizing security investment can be even more difficult if the costs that the user would bear to prevent the problems are greater than the user's expected loss from an attack.[232]

In part because of potential costs, inaction in the face of security threats does not always indicate ignorance. In 2007, researchers found that the general public is aware of security threats and what to do about them, but often still do not use freely available countermeasures.[233] They may instead choose to rely on investments made by others.[234] Risks and benefits associated with cybersecurity are both shared, which may limit users' incentives for unilateral investment.[235]

The harm as experienced by the individual user is, in turn, an externality not borne by the vendor.[236] In product development, some argue that vendors are likely to focus on functionality more than security,[237] perhaps because consumers tend to be more knowledgeable about functionality than security. A lemons market[238] may form when informational asymmetry leads to a reduction in the quality of the goods being sold. If consumers are not demanding and are not informed about software security, developers have fewer incentives to invest in security features, potentially leading to a lemons market for security.[239]

Some scholars, including Robert Hahn and Anne Layne-Farrar, argue that there is not currently a lemons market for security, because consumers do demand secure software.[240] However, security is an invisible aspect of software, and the software market is highly competitive. It is unclear the extent to which consumers would be willing to submit to higher prices to shoulder the costs of extra security

---

231. Bambauer & Day, *supra* note 226, at 1058–59; Hahn & Layne-Farrar, *supra* note 10, at 318.

232. JENS GROSSKLAGS ET AL., THE PRICE OF UNCERTAINTY IN SECURITY GAMES 7 (2009), http://people.ischool.berkeley.edu/~johnsonb/Welcome_files/Price_of_Uncertainty_10.pdf.

233. Michael Workman, William H. Bommer & Detmar Straub, *Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test*, 24 COMPUTERS HUM. BEHAV. 2799, 2800 (2008).

234. Rainer Böhme, *Vulnerability Markets: What is the Economic Value of a Zero-Day Exploit?* 1, in PROCEEDINGS OF 22C3, (Berlin, Germany, Dec. 27–30, 2005), http://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf

235. *Id*.

236. Bambauer & Day, *supra* note 226, at 1059; *see also* Oriola, *supra* note 8, at 456–57 (discussing scholarship exploring the economics of software security).

237. Oriola, *supra* note 8, at 481.

238. Economists often refer to lemons markets, which are based on the work of George Akerlof, who argued that the market for used cars is a lemons market because of the informational asymmetry between dealer and buyer. *Id.* at 469–70. Because buyers typically cannot discern between good and bad used cars, dealers cannot charge more for the good cars, so dealers do not have an incentive to sell high quality cars. *Id.*

239. Anderson & Moore, *supra* note 146, at 612; Böhme, *supra* note 234, at 1; Hahn & Layne-Farrar, *supra* note 10, at 310.

240. Hahn & Layne-Farrar, *supra* note 10, at 312; *see also* Oriola, *supra* note 8, at 472.

testing. If there is eventually market failure that cannot be solved by private parties, government intervention in the software security market may be appropriate.[241]

Software vulnerabilities become dangerous when someone invests the time and energy to weaponize that vulnerability, thereby creating an exploit.[242] Exploits can then be used maliciously, or they can be used in peaceful research.[243] Furthermore, exploits may simply be nuisances to the computer owner because they cause infected machines to run slower, or they might be destructive and cause the corruption or deletion of important files.[244] Security consumers may respond more ambivalently to nuisance exploits compared to destructive exploits, even though the social cost of nuisance exploits may be the same if the computer's impaired operation is because the computer is now part of a botnet.

In Part I, this Article discussed SQL injections, a type of attack that exploits a known type of vulnerability that affects SQL code.[245] Other possible vulnerabilities include bugs in permission settings, buffer overflow bugs, and kernel flaws.[246] Buffer overflow bugs are a very common target of malware, in part because of their familiarity and predictability.[247] Functionally, buffer overflow bugs have some similarities to SQL injections.[248] Software often allocates a set amount of space, the buffer, for operations.[249] If the input provided does not fit into the assigned buffer, the buffer could overflow.[250] A hacker might include new commands in the overflow portion that cause something else to happen.[251] The Heartbleed bug affecting OpenSSL encryption software is a variation on this type of bug, as it allowed attackers to exploit buffer-limit issues to view protected data.[252]

As discussed above, the morality and ethics of hacker behavior can vary.[253] Regardless, the best hackers are often driven to innovate by money or prestige;[254] the same motivations that drive people in any other profession. The annual Pwn2Own hacking competition attracts talent from all over the world,

---

241. Hahn & Layne-Farrar, *supra* note 10, at 299.

242. Paul N. Stockton & Michele Golabek-Goldman, *Curbing the Market for Cyber Weapons*, 32 YALE L. & POL'Y REV. 239, 245 (2013).

243. *Id.*

244. Hahn & Layne-Farrar, *supra* note 10, at 308.

245. *See supra* note 77 and accompanying text.

246. Oriola, *supra* note 8, at 463–6.

247. *Id.* at 464.

248. *Id.*

249. *Id.*

250. *Id.*

251. Fidler, *supra* note 26, at 15.

252. *Id.* at 1.

253. *See supra* Section I.A.

254. Marcia Clemmitt, *Once Shunned, Hackers Are Embraced by Industry*, 21 CQ RESEARCHER 757, 762–63 (2011) (quoting a professor who observed: "But you can't eat prestige").

promising financial incentives and lots of bragging rights.[255] Competitions are found outside of the private sector as well. To identify top talent, the Chinese government holds regional hacking competitions.[256] Furthermore, hacking is an industry with its own economy, and hackers are often rational actors in the free market. This is explored further in Part IV.

"Hacker" is not an inherently negative term but, going forward, we will primarily refer to nonmalicious hackers as "security researchers." This is a less controversial term and is more descriptive of the typical motivations that drive people to look for holes in software. This Part examines the roles of security researchers and provides foundational information about software and vulnerabilities before introducing the issues surrounding vulnerability markets.

A. Computers and Software

Engineers and mathematicians laid the foundation for the Information Age in the middle of the twentieth century. Several elements relating to computers and security were developed during World War II.[257] Afterwards, computer technology innovations focused on private-sector uses in addition to military uses.[258] Early computers could take up entire rooms.[259] Intel made the first microprocessor commercially available in 1971 and, as computers started to shrink, the personal computing market grew.[260]

Computers accomplish tasks based on input from the operator. The instructions ultimately must be in machine language, which consists entirely of numbers and would be unreadable for most humans.[261] High-level programming languages, like C#,[262] allow programmers to write the instructions in something that resembles human language. The instructions are then compiled into machine

---

255. Dan Goodin, *All Four Major Browsers Take a Stomping at Pwn2Own Hacking Competition*, ARS TECHNICA (Mar. 20, 2015 1:15), http://arstechnica.com/security/2015/03/all-four-major-browsers-take-a-stomping-at-pwn2own-hacking-competition/ [hereinafter Goodin, *Stomping*].

256. Susskind, *supra* note 15, at 633.

257. *See, e.g.*, R.K. Shyamasundar, *The Computing Legacy of Alan M. Turing (1912-1954)*, 106 CURRENT SCI. 1669, 1677 (2014).

258. *See generally* Bernadette Longo, *Mathematics, Computer Development, and Science Policy Debates After World War II*, IEEE Anns. Hist. Computing, at 64 Jul.–Sep. 2008.

259. *Retro delight: Gallery of early computers (1940s – 1960s)*, PING: BLOG (Dec. 11, 2009), http://royal.pingdom.com/2009/12/11/retro-delight-gallery-of-early-computers-1940s-1960s/.

260. *See Timeline of Computer History*, COMPUTER HIST. MUSEUM, http://www.computerhistory.org/timeline/computers/ (last visited Aug. 2, 2016).

261. *See* David Hemmendinger, *Computer Programming Language*, ENCYCLOPEDIA BRITTANICA, http://www.britannica.com/technology/computer-programming-language (last visited Aug. 2, 2016).

262. Many different programming languages exist, and C# is just one of them. Matt Sherman, *"Why Are There So Many Programming Languages?"*, STACK OVERFLOW (July 29, 2015), https://blog.stackoverflow.com/2015/07/why-are-there-so-many-programming-languages/.

language and executed by the computer.[263] This package of instructions is commonly called software.[264]

As modern life places more demands on software functionality, software becomes more complicated. Some commentators suggest that addressing information security by giving programmers incentives to release more-secure code.[265] However, complex software packages contain a lot of instructions for computers. A relatively simple mobile app may contain 10 thousand lines of code,[266] while the 2011 version of the Android operating system had over 1 million lines of code.[267] It takes 50 million lines of code to run the Large Hadron Collider, and Facebook relies on over 60 million lines of code.[268]

But Facebook seems almost minimalist when you consider that modern high-end cars may rely on software that contains 100 million lines of code.[269] This volume of code can make it possible to hide functionalities that flout regulations. Volkswagen skidded into a scandal in September 2015, when it was revealed that millions of their diesel vehicles contained software designed to produce false emission test results.[270]

1. Evolving Malware Threats

Malicious software, or malware, follows the same rules as other software.[271] Malware is a series of instructions designed to take advantage of security flaws.[272] While the vendor's programmers are trying to innovate to make code more secure, malware authors are trying to innovate to make exploits harder to detect.[273] Racing against malicious hackers will only become more challenging

---

263. *Id.* ("Underlying this fact is that all of these languages serve the same purpose: to turn human thoughts into the 1's and 0's that the computer understands.").

264. *Software*, COMPUTER HOPE, http://www.computerhope.com/jargon/s/software.htm (last visited Aug. 28, 2016).

265. Stockton & Golabek-Goldman, *supra* note 242, at 242; *see also* Oriola, *supra* note 8, at 469 (citing economic literature to support an incentivized approach to information security).

266. *Codebases*, INFO. IS BEAUTIFUL (Sep. 24, 2015) http://www.informationisbeautiful.net/visualizations/million-lines-of-code/.

267. Matt Brian, *Google's Andy Rubin: There Are Over 1 Million Lines of Code in Android*, THE NEXT WEB (Oct. 9, 2011), http://thenextweb.com/google/2011/10/19/googles-andy-rubin-there-are-over-1-million-lines-of-code-in-android/.

268. *Codebases*, *supra* note 266.

269. *Id.*; David Gelles, Hiroko Tabuchi & Matthew Dolan, *The Weak Spot Under the Hood*, N.Y. TIMES, Sep. 27, 2015, at BU1.

270. Jack Ewing, *Diesel Scandal at VW Spreads to Core Market*, N.Y. TIMES, Sep. 23, 2015, at A1.

271. Bijay Swain, *What Are Malware, Viruses, Spyware, and Cookies, and What Differentiates Them?*, SYMANTEC: CONNECT (Jul. 2, 2009), http://www.symantec.com/connect/articles/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them.

272. *Id.*

273. In hacking terminology, one of the goals is to make an exploit "FUD"—fully undetectable. For an example of hacking terminology, see Vineet Bharadwaj, *How to FUD*

as these hackers become more sophisticated.[274] Even if a company could make itself invulnerable to cyber threats, that invulnerability would only last until cyber threats evolve.[275]

Two recent malware innovations are polymorphic and metamorphic worms.[276] When a vulnerability and the manner of its exploit are known, antivirus software vendors update their databases with the new virus signatures.[277] Polymorphic and metamorphic worms can evade these protections.[278] Polymorphic worms have encrypted payloads and an encryption key that changes every time it is transmitted.[279] Metamorphic worms alter the code slightly at each infection so that the code is still semantically equivalent but may be missed by automated antivirus screening.[280]

Another alarming development is the possibility of sonic malware.[281] Historically, the best security measure that could be taken was to "air gap" a system by not connecting it directly to the Internet.[282] In 2013, scientists announced a prototype of malware that jumps between machines using sound waves, though the jumps were limited to about 65 feet.[283] Leap forward to 2015, and marketing companies have started using ultrasonic, inaudible sound beacons to link consumer devices through a process called "cross-device tracking."[284] This

---

a RAT Stub with Backtrack/Kali, THE HACKING GUIDE (June 8, 2014, 9:36 AM), http://www.thehackingguide.com/2014/06/how-to-fud-rat-stub-with-backtrackkali.html. RAT stands for "remote access Trojan," and Backtrack and Kali are Linux builds popular with those working in computer security or digital forensics – and also with malicious hackers. *Webcam Hacking*, BOS. COMMONS (Oct. 8, 2015), http://www.bostoncommons.net/webcam-hacking/. Stubs are programs that decrypt malicious code that had been encrypted to evade detection. Brent Graveland, *Fully Undetectable Cryptors and the Antivirus Detection Arms Race*, SYMANTEC: SEC. RESPONSE (Jan. 20, 2011), http://www.symantec.com/connect/blogs/fully-undetectable-cryptors-and-antivirus-detection-arms-race.

274. Anderson, *supra* note 97, at 532.

275. Trope & Humes, *supra* note 56, at 763.

276. Kaur & Singh, *supra* note 205, at 1521.

277. *U.S. Cert, Security Tip (ST04-005): Understanding Anti-Virus Software*, US–CERT (June 5, 2015), https://www.us-cert.gov/ncas/tips/ST04-005.

278. Kaur & Singh, *supra* note 205, at 1520.

279. *Id.*

280. ABLON ET AL., *supra* note 225, at 34; Kaur & Singh, *supra* note 205, at 1521.

281. Susskind, *supra* note 15, at 634.

282. Air gapping is second only to not turning the computer on at all. *See* Bruce Schneier, *Want to Evade NSA Spying? Don't Connect to the Internet*, WIRED (Oct. 7, 2013, 6:29 AM), http://www.wired.com/2013/10/149481/ (recommending using an air gap as a method of keeping communications secure).

283. Dan Goodin, *Scientist-Developed Malware Prototype Covertly Jumps Air Gaps Using Inaudible Sound*, ARS TECHNICA (Dec. 2, 2013, 11:29 AM PST), http://arstechnica.com/security/2013/12/scientist-developed-malware-covertly-jumps-air-gaps-using-inaudible-sound/ [hereinafter Goodin, *Malware*].

284. Dan Goodin, *Beware of Ads That Use Inaudible Sound to Link Your Phone, TV, Tablet, and PC*, ARS TECHNICA (Nov. 13, 2015, 10:00 AM), http://arstechnica.com/tech-policy/2015/11/beware-of-ads-that-use-inaudible-sound-to-link-your-phone-tv-tablet-and-pc/.

tracking method enables marketers to identify when a viewer watches a television commercial that has been embedded with these ultrasonic pitches by linking that viewing information to nearby devices.[285] Though transmissions are likely still limited based on proximity and require a microphone that is constantly listening,[286] the possibility of transmitting computer instructions via sound waves instead of network cables undermines air gapping as a security measure.

The ability to attack will likely continue to outpace the ability to defend.[287] Lilian Ablon's research team notes that defenders must be able to defend against everything, while a single attacker can focus on just one attack method and do it well.[288] In the long run, shoring up cyber defenses will rely on encouraging a plethora of cybersecurity research.

2. Software and Law

Some have floated the possibility of holding software vendors liable for inadequate security.[289] This is unlikely, in part because of the way modern law often favors software vendors. For example, courts have enforced contracts that limit what users can do with a software package after purchase.[290] If a person walks into a store and buys a box that holds a disk that contains software, it seems logical to conclude that the person owns what they are purchasing. However, commercial software is almost universally distributed with detailed EULAs attached, which often: (1) specify that the producer is granting the customer a license to the software; and (2) place limits on what the purchaser can do with the software.[291] Such clickwrap agreements typically apply the moment the purchaser opens the product.[292] Thus, restrictive contract terms may limit what researchers can do with purchased software packages.

If a consumer purchases defective software, products liability or negligence litigation may be possible.[293] However, EULAs often limit civil liability options for software consumers by restricting venue or including mandatory arbitration clauses.[294] Early attempts to enforce the CFAA explored the

---

285. *Id.*

286. Goodin, *Malware*, *supra* note 283.

287. ABLON ET AL., *supra* note 223, at 31.

288. *Id.*

289. *See* Katherine Booth Wellington, *Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions*, 30 SANTA CLARA HIGH TECH. L.J. 139, 175 (2014) (proposing that patients injured by cyberattacks against medical devices or hospital networks could potentially sue the manufacturer or the hospital).

290. *See* MDY Industries, LLC v. Blizzard Entertainment, Inc., 629 F.3d 928 (9th Cir. 2010) (concerning the use of bots in World of Warcraft).

291. *Id.*; *see also* Corynne McSherry, *You Bought It, But You Don't Own It,* ELEC. FRONTIER FOUND. (Jul. 15, 2008), https://www.eff.org/deeplinks/2008/07/you-bought-it-you-dont-own-it.

292. Juliet M. Moringiello & William L. Reynolds, *From Lord Coke to Internet Privacy: The Past, Present, and Future of the Law of Electronic Contracting*, 72 MD. L. REV. 452, 466 (2013).

293. Hahn & Layne-Farrar, *supra* note 10, at 329.

294. Moringiello & Reynolds, *supra* note 292, at 455.

possibility of using the CFAA to hold software producers liable for bugs,[295] but Congress promptly jettisoned this approach by amending the CFAA to clarify that civil liability for transmission of harmful code did not attach to the manufacturers.[296] In short, imposing legal liability on software vendors for vulnerabilities would likely be an uphill battle. Moreover, as discussed in the following section, software vendors have occasionally used their positions to limit discussion of security flaws.

B. Vulnerabilities

The more lines of code there are in software, the more opportunities there are for bugs. Jay Choi, Chaim Fershtman, and Neil Gandal argue that it would be "virtually impossible" to design vulnerability-free software.[297] They further assert that a firm that develops software has two main approaches to combating vulnerabilities: reduce the number of vulnerabilities, or increase the firm's likelihood of identifying vulnerabilities before the hackers.[298]

One study estimates that there are between five and fifteen bugs for every thousand lines of code.[299] Not every bug is a security vulnerability, but if even 10% of software bugs are security flaws, and 1% of those have critical security implications, a software package like Microsoft's Windows 7, with 40 million lines of code, could still have dozens of critical security holes.[300]

Many vulnerabilities are repaired without incident. A report from Secunia indicates that in 2014, 83% of software vulnerabilities had patches available the same day the vulnerability was disclosed.[301] This is a substantial increase from previous years when similar studies found that 70% or fewer of the disclosed vulnerabilities had a patch[302] available the same day.[303] Vulnerabilities that vendors do not patch are left open to exploitation. Even after a vendor patches a vulnerability, users who do not install the patch remain unprotected. Additionally, patches are not perfect: one study indicates that there are bugs in over 10% of security patches.[304]

---

295. *E.g.*, Shaw v. Toshiba Am. Info. Sys., Inc., 91 F. Supp. 2d 926, 934 (E.D. Tex. 1999).

296. Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (USA PATRIOT Act) Act Of 2001, Pub. L. No. 107-56, § 814(e), 115 Stat. 272, 382–83.

297. Jay Pil Choi et al., *Network Security: Vulnerabilities and Disclosure Policy*, 58 J. INDUS. ECON. 868, 869 (2010).

298. *Id.* at 882.

299. Oriola, *supra* note 8, at 466.

300. *Codebases*, *supra* note 266.

301. *Vulnerability Review 2014: Time to Patch*, FLEXERA SOFTWARE, https://secunia.com/resources/vulnerability-review/time-to-patch/ (last visited Aug. 2, 2016).

302. Ross Gardler, *What Is a Software Patch?*, OSS WATCH (Feb. 8, 2013), http://oss-watch.ac.uk/resources/softwarepatch.

303. Bambauer & Day, *supra* note 226, at 1061–62; Bilge & Dumitras, *supra* note 88, at 836.

304. Bilge & Dumitras, *supra* note 88, at 836.

Jaziar Radianti, Eliot Rich, and Jose Gonzalez enumerate three stages in the lifecycle of a vulnerability: (1) unknown; (2) manifest; and (3) patched.[305] Leyla Bilge and Tudor Dumitras propose a more detailed timeline for the vulnerability lifecycle.[306] Their findings indicate that the full vulnerability lifecycle, based on the time that it takes for a vulnerability to arrive at the point where it is almost universally patched, may be longer than four years.[307]

A zero-day vulnerability is a vulnerability used before the vendor learns about it.[308] The phrase "zero-day" is often attached to every point in the process. For example, zero-day vulnerabilities are turned into zero-day exploits that are used in zero-day attacks.[309] Depending on the writer, any of these phrases may be shortened to simply "zero days."[310]

When it comes to modern vehicles, having 100 million lines of code introduces inestimable opportunities for critical security flaws.[311] In 2015, noted technology journalist Andy Greenberg voluntarily submitted himself to a demonstration of the security vulnerabilities in a late model Jeep Cherokee.[312] The demonstration started when he was on the highway ten miles away from the researchers, and quickly escalated out of his comfort zone when the researchers turned off the Jeep's transmission at seventy miles per hour.[313] After that close call, Greenberg continued with the experiment in a safer environment and received more information about the vulnerabilities.[314] The security researchers, Charlie Miller and Chris Valasek, showed Greenberg how the hack worked.[315] The researchers used a device that was connected to the Sprint network, the same network that Chrysler uses for its UConnect service in Chrysler-made cars, to hack into the Jeep's UConnect feature and move from there into other parts of the car's controls.[316]

In our revised approach to describing hacker alignment discussed in Section I.A, Miller and Valasek would probably be considered "neutral good."[317] It took Miller and Valasek three years to figure out how to remotely hack a car from

---

305. Jaziar Radianti et al., *Vulnerability Black Markets: Empirical Evidence and Scenario Simulation*, 2009 PROC. 42ND HAW. INT'L CONF. SYS. SCIS. 8, 8.

306. Bilge & Dumitras, *supra* note 88, at 835.

307. *Id*.

308. Oriola, *supra* note 8, at 462 (referring to the Stuxnet virus as exploiting "four previously unknown or 'zero-day' vulnerabilities in Microsoft's Windows.").

309. *But see What Is a Zero-Day Vulnerability?*, SYMANTEC: PC TOOLS, http://www.pctools.com/security-news/zero-day-vulnerability/ (last visited Aug. 23, 2016) (conflating zero-day exploits and zero-day attacks.

310. Mailyn Fidler, *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis*, 11 I/S: J. L. & POL'Y FOR INFO. SOC'Y 405, 406 (2015).

311. Gelles, *supra* note 269.

312. Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, WIRED (July 21, 2015, 6:00 AM), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [hereinafter Greenberg, *Jeep*].

313. *Id.*

314. *Id.*

315. *Id.*

316. *Id.*

317. *See Supra* Section I.A.

across the country.[318] They undertook the research of the Jeep Cherokee partially because representatives of the automobile industry did not seem to be taking the threat of car hacks seriously.[319]

Security researchers like Miller and Valasek provide a valuable service and deserve to be compensated for their time and skill. This is part of the reason why many large software companies now offer bug-bounty programs.[320] Unfortunately, many other companies do not offer such programs, and some companies are more likely to sue a researcher who discovers a flaw than pay them.[321] Meanwhile, governments, criminals, and other researchers are looking to buy information that they can use to exploit these types of vulnerabilities. The Internet has enabled the rise of a global market to provide compensation to security researchers when vendors attempt to threaten them into silence. Vendor hostility is not the only motivation for a security researcher to turn to the grey or black markets, but it is the most clearly correctable motivation.

1. Zero-Day Vulnerabilities and Research

So far, the process we have examined proceeds as follows: (1) software has bugs; (2) some bugs are security flaws; and (3) researchers find security flaws. What happens next could follow many paths.

If the researchers are searching on behalf of the vendor, they will notify the vendor, who will decide whether to patch the security flaw. If the vendor patches the flaw, there will typically be an announcement that encourages users to apply updates. Because not all users will update immediately, there is likely to be a surge of exploitations of that vulnerability after an announcement. One study indicates that the attacks using a particular vulnerability may increase by five orders of magnitude after an announcement.[322]

Freelance researchers might offer the bug to the vendor, either for free or for a price.[323] Alternatively, they might choose to sell the information to a vulnerability broker or other market actor, or to use the knowledge towards other security research.[324] The researchers may also opt to demonstrate the vulnerability

318. Greenberg, *Jeep*, *supra* note 312.

319. *Id.*

320. Fidler, *supra* note 310, at 414.

321. *See, e.g.*, Robert Lemos, *Settlement Reached in Cisco Flaw Dispute*, SECURITYFOCUS (Jul. 29, 2005), http://www.securityfocus.com/news/11260; Joseph Menn, *Legal Fears Muffle Warnings on Cybersecurity Threats*, REUTERS (Oct. 29, 2012, 10:10 PM), http://uk.reuters.com/article/uk-cyberwar-infrastructure-idUKBRE89S1AF20121029. For a (slightly biased) list of documented incidents of more legal threats, see *Legal Threats Against Security Researchers*, ATTRITION.ORG, http://attrition.org/errata/legal_threats/ (last visited Aug. 2, 2016).

322. Bilge & Dumitras, *supra* note 88.

323. CHARLIE MILLER, INDEPENDENT SECURITY EVALUATORS THE LEGITIMATE VULNERABILITY MARKET: INSIDE THE SECRETIVE WORLD OF 0-DAY EXPLOIT SALES 2 (2007), http://weis2007.econinfosec.org/papers/29.pdf.

324. *Id.*

at a conference or during a competition, exploit the vulnerability,[325] or simply do nothing.[326]

Because zero days are unknown by definition, detecting and preventing damage is very difficult. Above, we mentioned polymorphic worms as an example of malware innovation that makes it harder for anti-malware measures to detect malicious code. The problem is compounded when the malware is a zero-day polymorphic worm, making it even more difficult to detect and identify.[327]

Researchers are working on ways to defend against zero-day attacks. As noted above, antivirus software works by looking for signatures associated with known exploits. Because zero-day exploits have unknown signatures, defenders cannot use traditional signature-based detection methods.[328] Instead, defenders might utilize monitoring techniques that are host-based or network-based.[329] Network-based methods may look for the type of behavior that is associated with worms.[330] Ratinder Kaur and Maninder Singh have reviewed several network-based approaches and note that all of them have significant weaknesses.[331]

Zero-day events are difficult to observe in the wild. Because of their high value, zero days are often saved for use against a specific target, so they are not often intercepted by honeypots.[332] It is thus difficult to estimate how common they really are. Using historical data, Bilge and Dumitras identified 18 zero days by looking for executable files with known signatures over a four-year period.[333] These were considered zero days because they were announced and patched after the date when they were first detected. In some cases, years elapsed between the zero day appearing on the Internet and the zero day being patched.[334] Of those 18 zero days, 11 were not previously known to have been used prior to the patch being released.[335] Based on their findings, the authors noted that zero days are more common than previously believed.[336] They also acknowledge that their methods failed to identify some known zero days, especially when the known zero

---

325. Stockton & Golabek-Goldman, *supra* note 242, at 244.

326. The security firm Medsec tried a new approach in August2016, when, before making a public announcement, it disclosed security flaws in St. Jude pacemakers to an investment firm, which then "shorted" St. Jude stock. Jordan Robertson & Michael Riley, *Carson Block's Attack on St. Judge Reveals a New Front in Hacking for Profit*, BLOOMBERG MARKETS (Aug. 25, 2016, 10:59 AM PDT), http://www.bloomberg.com/news/articles/2016-08-25/in-an-unorthodox-move-hacking-firm-teams-up-with-short-sellers. For an explanation of short-selling, see *infra* note 613.

327. Kaur & Singh, *supra* note 205, at 1520.

328. *Id.* at 1522.

329. *Id.* at 1522–23.

330. *Id.* at 1524, 1529.

331. *Id.* at 1543.

332. *See* Bilge & Dumitras, *supra* note 88, at 833.

333. *Id.* at 833–44.

334. *Id.*

335. *Id.* at 834.

336. *Id.*

days were exploited with polymorphic malware or when the exploit was not an executable file.[337]

2. Finding and Disclosing Zero Days

Many security researchers are driven by curiosity and the motivation to improve technology.[338] Taiwo Oriola argues that "legitimate vulnerability research" is ethical and moral, but that malicious research and disclosure are unethical.[339] Unfortunately, the distinction between legitimate and malicious is often blurry, and researcher intentions might not be considered by vendors or courts. In this subsection, we explore a wide range of issues relating to the discovery and disclosure of zero days.

a. Legal issues in vulnerability research

Vulnerability hunters must generally be skilled coders to identify hidden security flaws.[340] Being able to identify vulnerabilities is a morally neutral skill on paper, and discoveries can be used for good or evil. However, even well-intentioned researchers must contend with the implications of violating policies or the law.

Unauthorized security research can run afoul of a variety of laws that protect software. Computer programs are protected by copyright law, and the processes that a program carries out can be protected by patent law.[341] Vendors may try to protect their intellectual property from even benevolent security researchers by threatening lawsuits.

Because of the nature of searching for vulnerabilities, these activities might violate reverse engineering provisions of license agreements and are often illegal if the researcher did not have permission to test for security flaws.[342] Tools like static code analysis enable security consultants to quickly identify possible

337. *Id.* at 841–42.

338. Bambauer & Day, *supra* note 226, at 1054; Kirsch, *supra* note 5, at 388; *see also* Matwyshyn, *Speech*, *supra* note 146, at 829.

339. Oriola, *supra* note 8, at 522.

340. Fidler, *supra* note 26, at 24.

341. *See* Matwyshyn, *Speech*, *supra* note 146, at 807 (observing that computer programs can be treated as text or machine).

342. Mary Ann Davidson, Chief Technology Officer of Oracle, caught a lot of criticism from the security community when she made a blog post telling people to stop looking for vulnerabilities in Oracle's products. *See* Sean Gallagher, *Oracle Security Chief to Customers: Stop Checking Our Code for Vulnerabilities*, ARS TECHNICA (Aug. 11, 2015, 7:35 AM), http://arstechnica.com/information-technology/2015/08/oracle-security-chief-to-customers-stop-checking-our-code-for-vulnerabilities/. Although her post was removed within two days of being posted, archived versions are available online—because the Internet *never* forgets. *E.g.*, Matt Blaze (@mattblaze), TWITTER (Aug. 11, 2015, 5:21 AM), https://twitter.com/mattblaze/status/631077946338476032 ("Looks like Oracle took down that 'vulnerabilities: don't ask, don't tell' blog post. But I printed a pdf of the page. [http://www.crypto.com/papers/oracle-blog.pdf].").

vulnerabilities but may be considered reverse engineering in violation of EULAs.[343]

In the United States, one available cause of action against security researchers is trespass to chattels, which has been applied in cases of computer trespass.[344] Through its prohibition on unauthorized access, the CFAA offers a second avenue for suing or prosecuting security researchers.[345] Vendors can also sue researchers using the Digital Millennium Copyright Act ("DMCA"), which makes it illegal to circumvent access control technology, though there are limited exceptions for encryption research and security testing.[346] The DMCA also prohibits reverse engineering, except when undertaken to achieve interoperability.[347] Derek Bambauer and Oliver Day criticize the deleterious effects that such intellectual property laws have on security research and note that such laws can also be wielded to restrict disclosure.[348]

b. Zero days and the government

The U.S. government has demonstrated significant interest in software security vulnerabilities for a variety of purposes. The Department of Justice, for instance, proposed using zero-day vulnerabilities to enable a search of a suspect's computer when the location of the computer is unknown.[349] In 2015, the U.S. government was revealed to be a customer of The Hacking Team, an Italian company that sells sophisticated spyware to national governments.[350] Rumors also abound that the NSA has ties to a highly sophisticated hacking organization that security experts have nicknamed the Equation Group.[351]

Information about the use of zero-day vulnerabilities at the NSA came to light when Edward Snowden leaked classified documents in 2013. Some reports indicate that the NSA runs a program called FoxAcid where they store vulnerability and exploit information for use against future targets.[352] According to leaked documents, the NSA budgeted $25.1 million for the purchase of software vulnerabilities for the 2013 fiscal year.[353] After the Snowden leak, the Obama

343. Kaur & Singh, *supra* note 205, at 1521.
344. Oriola, *supra* note 8, at 487.
345. *Id.* at 498-99.
346. 17 U.S.C. § 1201(g), (j) (2012); Oriola, *supra* note 8, at 508–09.
347. 17 U.S.C. § 1201(f) (2012).
348. Bambauer & Day, *supra* note 226, at 1054.
349. Fidler, *supra* note 26, at 2, 168.
350. Cora Currier & Morgan Marquis-Boire, *Leaked Documents Show FBI, DEA, and U.S. Army Buying Italian Spyware*, THE INTERCEPT (July 6, 2015, 10:00 AM), https://theintercept.com/2015/07/06/hacking-team-spyware-fbi/.
351. Goodin, *Confirmed*, *supra* note 75.
352. Fidler, *supra* note 26, at 27; Sam Biddle, *The NSA Leak Is Real, Snowden Documents Confirm*, THE INTERCEPT (Aug. 19, 2016), https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/.
353. 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.

administration issued a report recommending increased oversight of government use of zero-day vulnerabilities.[354] The future of this recommendation is uncertain, especially after the leak by ShadowBrokers of data allegedly stolen from the Equation Group in 2013.[355]

Many have criticized the NSA's purchases of zero days as prioritizing intelligence objectives over user and internet security.[356] The use of spyware in law enforcement is another controversial area.[357] Others, however, would likely argue in favor of the covert use of zero days for intelligence or law enforcement purposes because it helps the good guys catch the bad guys. This latter category of arguments is unpersuasive for one fundamental reason: every zero day that is secretly used by a government is one more zero day that can be used against that government's law-abiding citizens, either by that government or by someone else. The recent large-scale theft of malware tools from an alleged affiliate of the NSA reinforces this conclusion.[358] When ShadowBrokers publicly posted part of the stolen data, affected companies scrambled to fix the newly disclosed zero days that the NSA had allegedly known about for at least three years.[359] The ShadowBrokers dump strengthens our conviction that the hoarding of zero days by any government runs counter to the public interest.

c. Public disclosure

Zero-day discovery and disclosure are clearly volatile in terms of moral and ethical implications, and they also have significant financial ramifications. Zero days are valuable on the open market and are in high demand by both governments and criminal organizations—as long as they remain unknown to others.[360] But zero days are discovered, not created, so there is nothing preventing others from discovering the same information.[361] This aspect of zero days may be one reason why many security researchers prefer to publicly disclose vulnerabilities. By shedding light on the vulnerability, the value of the vulnerability to malicious actors plummets.

One popular method of public disclosure is to announce and demonstrate vulnerabilities at industry conferences.[362] Information security researchers often

354. Fidler, *supra* note 26, at 101.

355. Goodin, *Confirmed*, *supra* note 75.

356. *E.g.*, *id.* at 3.

357. *Grassley Wants Details on FBI Spyware Programs*, THE IOWA STATESMAN, (June 13, 2015, 7:30 AM), http://www.theiowastatesman.com/3576/grassley-wants-details-on-fbi-spyware-programs.

358. Russell Brandon, *After ShadowBrokers, Should the NSA Still Be Hoarding Vulnerabilities?*, THE VERGE (Aug. 19, 2016, 9:53 AM), http://www.theverge.com/2016/8/19/12548462/shadow-brokers-nsa-vulnerability-disclosure-zero-day.

359. *Id.*

360. *See* ABLON ET AL., *supra* note 225, at 25.

361. Fidler, *supra* note 26, at 10.

362. Amanda Schupak, *A Look Inside the Hostile, Helpful World of Hacking Conventions*, CBS NEWS (Aug. 8, 2015, 7:00 AM), http://www.cbsnews.com/news/black-hat-def-con-look-inside-the-hostile-helpful-world-of-hacking-conventions/.

have differences of opinion about zero days, especially the ethics of announcing zero days without giving the vendor a chance to fix it, and of selling zero days to parties other than the vendor.[363] The current prevailing norm is to work with the vendor ahead of time to ensure that the vulnerability is patched before the presentation.

Researchers might use conference demonstrations as a means to prompt remedial action by a vendor who is slow to patch vulnerabilities.[364] Trope and Humes recount a recent incident involving a vulnerability that could affect critical infrastructure systems, where the discovery was promptly disclosed to the Industrial Control Systems Computer Emergency Response Team ("ICS-CERT"), which is a trusted intermediary. However, the vulnerability information was not acted upon for approximately four months.[365] A notification of a planned presentation might have incentivized quicker action.

Another reason why researchers may prefer public disclosure at conferences is the reputation gain from a successful demonstration. Presenting a discovery at a high profile industry conference is an excellent vehicle for researchers looking to rise in their careers. Reputation is practically a currency in the information security field. Being known as the person who discovered a major security flaw might prove as valuable as being paid in legal currency.[366]

As a practical matter, some have argued that any public disclosure of vulnerabilities may be harmful because of the possibility that malicious hackers will use the information, but others argue that disclosure improves security in the long run and that it provides vendors with incentives to fix bugs promptly.[367] Disclosure is thus a double-edged sword, increasing the likelihood of attacks while simultaneously supporting improvements in security.[368] Overall, Bilge and Dumitras find that disclosure to the public is likely more beneficial than private disclosure to vendors.[369] Vendors who discover vulnerabilities in their own products must also weigh the pros and cons of public disclosure. Choi, Fershtman, and Gandal assert that vendors currently disclose vulnerabilities primarily when it would be more efficient to do so.[370]

There is a troubling possibility that public disclosure can lead to more attacks. Researchers have empirically demonstrated that the use of particular exploits rises significantly when vulnerabilities are announced, indicating that

---

363. Matwyshyn, *Speech*, *supra* note 146, at 826–27.

364. Trope & Humes, *supra* note 56, at 681.

365. *Id.*

366. See Bambauer & Day, *supra* note 226, at 1066.

367. For a discussion of these arguments, see Anderson & Moore, *supra* note 146, at 611; Choi et al., *supra* note 297, at 879-80; Oriola, *supra* note 8, at 482.

368. Matwyshyn, *Speech*, *supra* note 146, at 821; *see also* Choi et al., *supra* note 297, at 870 (citing observations by renowned technologist and security professional Bruce Schneier).

369. Bilge & Dumitras, *supra* note 88, at 842.

370. Choi et al., *supra* note 297, at 871; *see also* Karthik Kannan & Rahul Telang, *Market for Software Vulnerabilities? Think Again*, 51 MGMT. SCI. 726, 728 (2005) (discussing previous research about software vendors and vulnerability disclosure).

hackers stay highly informed about current vulnerabilities.[371] However, the rise in use may also be for economic reasons. In the black markets that facilitate the exchange of contraband like drugs, weapons, and hacking tools, the price for tools exploiting a particular vulnerability plummet when the vulnerability becomes publicly known.[372] If a vendor was previously one of the few people either using or selling a particular toolkit as a zero-day exploit, dropping the price when the exploit is discovered is an economically rational thing to do.

Uncoordinated and decentralized public disclosures may put researchers at odds with vendors, who may seek injunctions to prevent researchers from presenting vulnerabilities at conferences.[373] Planned presentations may also be delayed to allow the vendor more time to fix the problem. In 2009, Juniper Networks barred one of its own researchers from presenting information about a vulnerability that affected ATMs.[374] Exploitation of the vulnerability would allow an attacker to eject money from an ATM.[375] Information about the security flaw was eventually presented in 2010 at the DEFCON information security conference.[376]

Some vendors have attempted to argue that the act of publicly disclosing a vulnerability or exploit is a violation of computer crime law, but no court has officially ruled on this question. In 2008, the Massachusetts Bay Transit Authority ("MBTA") sued three MIT students to prevent them from giving a presentation at a conference that included information about a vulnerability in MBTA's ticketing system.[377] The court denied MBTA's request for a preliminary injunction and remarked that it was unlikely that MBTA's claim would succeed on the merits, in part because a PowerPoint presentation is not a transmission under the CFAA.[378]

d. Different types of disclosure

Generally speaking, sharing vulnerability information with the affected vendor or a trusted intermediary is almost never controversial. CERT has often acted as a trusted intermediary between vulnerability researchers and vendors.[379] However, such disclosures are not always effective at protecting the public

371. Zhuge et al., *supra* note 89, at 235.

372. Oriola, *supra* note 8, at 513.

373. *See, e.g.*, Fidler, *supra* note 26, at 167 (noting the tensions that uncoordinated disclosures can cause); Matwyshyn, *Speech*, *supra* note 146, at 825 ("In other words, complications and legal wrangling frequently arise when software vulnerabilities are first discovered."); Oriola, *supra* note 8, at 483 (discussing disclosures made by competitors or through public listing services like BUGtrack).

374. Bambauer & Day, *supra* note 226, at 1063.

375. Matwyshyn, *Speech*, *supra* note 146, at 796–97.

376. *Id.*

377. Michael McGraw-Herdeg & Marissa Vogt, *MBTA Sues Three Students to Stop Speech on Subway Vulnerabilities*, THE TECH (Aug. 25, 2008), http://tech.mit.edu/V128/N31/subway.html.

378. Mass. Bay Transp. Auth. v. Anderson, No. 1:08-CV-11364(GAO), 2008 WL 6954925 (D. Mass. Jan. 26, 2009).

379. Oriola, *supra* note 8, at 483; Kannan & Telang, *supra* note 370, at 726.

interest. Many software vendors allow weeks or months to pass before issuing a patch.[380]

These delays may often be for business reasons, frustrating security specialists who believe that security should always be the top priority.[381] Those on the financial side of the business, on the other hand, may have different priorities based on consumers and the market.[382] By and large, what consumers want is new features and fast releases.[383]

As noted above, information security conferences often include demonstrations of vulnerabilities. A security researcher who does not disclose directly to the vendor and does not disclose at an industry conference might instead independently report the vulnerability to the general public via the Internet. This type of disclosure was at the heart of *United States v. Auernheimer*, where the defendant exploited a vulnerability in AT&T's system, thereby obtaining the email addresses of approximately 114,000 iPad owners.[384] The defendant's findings were published online. Ethically questionable disclosures might also take place in the marketplace for vulnerabilities that is the primary focus of this Article.

After a vulnerability is found, disclosed, and patched, there remains one significant problem: ensuring that a high enough percentage of users have installed the patch. The Conficker worm is a complex exploit that can disable security protections and other system services.[385] It first emerged in 2008, when it infected seven million computers.[386] About 30% of Windows users did not install the patch that would prevent a Conficker infection.[387] Fast-forward seven years, and there remain enough vulnerable machines to allow Conficker to reemerge as a significant threat. Conficker is associated with malware used in 20% of cyberattacks in October 2015.[388] These exploits may also be assisted by hacking techniques that make hacking tools fully undetectable ("FUD") or that encrypt the malicious code to prevent detection by antimalware tools.

e. Disclosure and the First Amendment

As noted above, some vendors seek injunctions against researchers who intend to present their findings at hacking conferences.[389] Security researchers are

---

380. Kirsch, *supra* note 5, at 389; Bambauer & Day, *supra* note 226, at 1063.

381. Matwyshyn, *Speech*, *supra* note 146, at 825.

382. Bambauer & Day, *supra* note 226, at 1063.

383. *Id.*

384. United States v. Auernheimer, 748 F.3d 525, 531 (3d Cir. 2014).

385. *Worm:Win32/Conficker.B*, MICROSOFT: MALWARE PROT. CTR., http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Worm%3aWin32%2fConficker.B (last visited Aug. 2, 2016).

386. Susskind, *supra* note 15, at 586.

387. *Id.*

388. John Leyden, *Conficker, Back From the Undead, Dominates Malware Threat Landscape*, THE REGISTER (Dec. 1, 2015, 11:29 AM), http://www.theregister.co.uk/2015/12/01/conficker_dominates_threat_landscape_malware/.

389. Bambauer & Day, *supra* note 226, at 1053; *see also* Menn, *supra* note 321 (discussing last minute changes to a security conference's agenda when two talks were canceled over threats to file suit).

keenly aware of the possibility that a vendor might seek criminal prosecution for the researcher's activities[390] or assert intellectual property rights to enforce silence.[391] In discussing this quickness to sue security researchers, Bambauer and Day argue that for some vendors, "the perception of security is often more important than security itself."[392]

Using the law to silence security researchers may violate the First Amendment. A presentation of exploit information is clearly speech, and courts acknowledge that constitutionally protected speech includes computer code.[393] However, the First Amendment is not without limitations, so the scope of the researcher's right to present findings is unclear. When a vendor attempts to use a court to prevent exploit demonstrations, this raises two significant First Amendment issues relating to how the information was obtained and what the information enables.[394] If the information about the vulnerability was obtained through unlawful means, how strong is the discoverer's First Amendment right to present that information? Another tricky First Amendment area with vulnerability disclosure concerns the line between unlawful advocacy and information speech.

The right to communicate unlawfully obtained information was addressed by the Supreme Court in 2001 in *Bartnicki v. Vopper*, which concerned the dissemination of information by a journalist whose source obtained the information unlawfully.[395] Specifically, a radio talk show host played a recording obtained in violation of federal wiretapping law.[396] In *Bartnicki*, six justices held that even if information was obtained illegally by a third party, the First Amendment protects journalists who disseminate this information when it is a matter of public concern.[397] The Supreme Court has not yet addressed what the outcome would be if the journalist is the party who violated the law to obtain the information. In *Dahlstrom v. Sun-Times Media*, the Seventh Circuit held that the First Amendment did not shield journalists who violated the federal Driver's Privacy Protection Act by publishing personal information that the journalists obtained from the Department of Motor Vehicles.[398] The defendant in *Dahlstrom* petitioned the Supreme Court for certiorari, but this motion was denied.[399]

If the Supreme Court had decided to hear arguments in *Dahlstrom*, the subsequent decision could have sent shockwaves through the hacker community

---

390. Matwyshyn, *Speech*, *supra* note 146, at 825–26.

391. Bambauer and Day, *supra* note 226, at 1067.

392. *Id.* at 1069.

393. *E.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 445 (2d Cir. 2001). The Supreme Court has not weighed in on this definitively, but has ruled that video games are a form of protected speech. Brown v. Entm't Merchs. Ass'n, 564 U.S. 786, 790 (2011).

394. Similar First Amendment issues have previously been raised concerning export restrictions that prevented the export of materials about encryption. Fidler, *supra* note 26, at 86–87.

395. 532 U.S. 514, 517–18 (2001).

396. *Id.*

397. *Id.* at 534.

398. 777 F.3d 937 (7th Cir. 2015).

399. 136 S. Ct. 689 (2015).

and the *new* media, in addition to the *news* media. If the Supreme Court ruled that the First Amendment protects information that the journalist obtained illegally, this would be good for security researchers because it could limit the ability of courts to grant injunctions against conference presentations when the vulnerability is a matter of public concern.

A second First Amendment issue concerns unlawful advocacy and informational speech. Informational speech cases are tricky in part because some types of information may have beneficial uses as well as harmful uses.[400] Information security conferences attract thousands of security professionals, and most of the people at exploit demonstrations are likely more interested in learning about possible threats than about actually exploiting vulnerabilities for personal gain.

Informational speech issues were especially common in the middle of the twentieth century. During the McCarthy era, the Communist Party of the USA ("CPUSA") was viewed with hostility, and individuals were famously persecuted for their affiliations with the CPUSA. The Cold War was a period of high paranoia and tense relations with the Soviet Union, and the United States government feared that the CPUSA was working with the Soviet Union. Informational speech was implicated because of the Communist and Socialist writings often kept by party members, some of which advocated overthrowing the government. Documents which were revealed in the 1990s proved that the CPUSA in fact had been aiding the Soviet Union in espionage activities against the United States.[401] Martin Redish argues, however, that even if the threat of espionage was real, prosecutions based on association rather than actual espionage-related activities violated the First Amendment.[402] The prohibition of all hacking activity and hacking speech because some hacking activity is dangerous toes this same line.

A related concern involves unlawful advocacy. Presentations at hacking conferences are typically demonstrations of an exploit, accompanied by explanations. Presenters often omit key information to prevent listeners from reproducing their findings. Even with such omissions, does this constitute unlawful advocacy and incitement of criminal activity? Case law is unclear. In *Rice v. Paladin*, the Fourth Circuit held that the First Amendment did not shield a publisher from civil liability when it published a graphic and extremely detailed how-to manual about becoming a contract killer.[403] Applying *Rice* to hacking speech, Matwyshyn suggests that information that is easily accessible and usable by members of the public should receive less protection than more scarce knowledge.[404] But because vulnerability discoveries *are* scarce knowledge, this supports an argument against a strict application of *Rice* to exploit speech.

One policy argument against viewing exploit demonstrations as unprotected speech is that exploit presenters discovered something that already

---

400. Matwyshyn, *Speech*, *supra* note 146, at 815–16.

401. Martin H. Redish, *Unlawful Advocacy and Free Speech Theory: Rethinking the Lessons of the McCarthy Era*, 73 U. CIN. L. REV. 9, 10–12 (2004).

402. *Id.* at 14–15.

403. Rice v. Paladin Enters., 128 F.3d 233, 267 (4th Cir. 1997).

404. Matwyshyn, *Speech*, *supra* note 146, at 836.

existed but was unknown. The author of the how-to manual for contract killing did not discover the practices described in the book, but merely consolidated them into a single text. There is a degree of intellectual innovation inherent in exploit presentations that is simply not present in a standard how-to manual, regardless of the subject matter. Because intellectual innovation should be encouraged, outlawing the fruits of the innovation may run counter to the public interest. Additionally, the common practice of omitting essential steps during presentations mitigates the risk of the demonstrated knowledge being used destructively.

3. Vulnerability Markets

As noted above, hacking is essentially an institution with a separate economy. Andreas Kuehn and Milton Mueller note that software vulnerability information has become a commodity.[405] Money often changes hands for this valuable information good.[406] The moral and ethical foundations of vulnerability markets vary significantly. One vulnerability seller, Netragard, confirms that some buyers purchase vulnerabilities for penetration testing to improve security practices.[407] Other intentions are not so harmless.

Paul Stockton and Michele Golabek-Goldman use the familiar black-grey-white color scheme of hacker hats to describe the different kinds of vulnerability markets.[408] In this usage, white markets would focus on selling to vendors, while black market trades include at least one party with malicious intent. The grey market falls somewhere in between, with many buyers being national governments.[409] Bug-bounty programs are a part of the white market. Hahn and Layne-Farrar evaluate several proposals for improving security and note that bug-bounty programs are "moderately successful and cost effective."[410]

Regardless of market shade, all of the market participants tend to be very secretive about what is being purchased and for how much. The secretive nature of the white and grey markets is often supported by nondisclosure agreements.[411] The black market for vulnerability information, especially zero-day exploits, is often buried in "darknet" forums, accessible only through highly secure web browsing methods, where vendors are paid in cryptocurrency.[412]

---

405. Kuehn & Mueller, *supra* note 47, at 1.
406. *Id.* at 2.
407. Fidler, *supra* note 26, at 27.
408. Stockton & Golabek-Goldman, *supra* note 242, at 247.
409. *Id.*
410. Hahn & Layne-Farrar, *supra* note 10, at 337.
411. Paul F. Roberts, *Glitches to Riches: The Hackers Who Make a Killing Off Software Flaws*, CHRISTIAN SCI. MONITOR: PASSCODE (Oct. 30, 2015), http://www.csmonitor.com/World/Passcode/2015/1030/Glitches-to-riches-The-hackers-who-make-a-killing-off-software-flaws.
412. Jake Swearingen, *A Year After the Death of Silk Road, Darknet Markets are Booming*, THE ATLANTIC, (Oct. 2, 2014), http://www.theatlantic.com/technology/archive/2014/10/a-year-after-death-of-silk-road-darknet-markets-are-booming/380996/.

Digital cryptocurrencies like Bitcoin are very popular on black market sites,[413] where encryption of private messages using personalized encryption keys is the norm. Encryption provides a layer of security for people whose activities are either illegal or likely to attract negative attention. Cryptocurrencies serve a similar purpose by improving security for exchanges of goods and services. Cryptocurrencies are exchanged using cryptographic credentials as validation.[414] Cryptocurrencies like Bitcoin are decentralized and not subject to regulation in many jurisdictions.[415]

Darknet markets include the now-defunct Silk Road, which was shut down and its founder arrested.[416] Law enforcement continually tries to shut down these markets, but darknet markets are part of a functioning economy.[417] Once shut down, more inevitably pop up in a vicious and never-ending game of Whack-a-Mole.[418] In the context of organized crime, Nora Demleitner notes that if members of an organized crime group are imprisoned, the organization keeps committing crimes.[419] Post-Silk Road darknet markets have a similar behavior, but there, the behavior is based on the decentralized nature of the market, rather than the organized nature of the market. In this way, today's darknet markets are an example of the success of *dis*-organized crime.

In the white and grey markets, there are many firms that operate as intermediaries between discoverers and those who would use the information. These vulnerability brokers often operate openly, though information about pricing and buyers is often closely held. Professor Rainer Böhme notes that many vulnerability brokers offer annual subscription fees that far exceed the amount paid for an individual vulnerability.[420] The white market includes vulnerability brokers like TippingPoint who focus on disseminating the information to software vendors so that the flaws can be fixed.

Other vulnerability brokers focus on selling exploits and refuse to share their knowledge with vendors.[421] This side of the business can be rough. The CEO of Endgame, a former seller of exploits, is quoted as saying, "The exploit business

---

413. ABLON ET AL., *supra* note 223, at 11–12.

414. Sarah Jane Hughes & Stephen T. Middlebrook, *Advancing the Framework for Regulating Cryptocurrency Payments Intermediaries*, 32 YALE J. REG. 495, 505 (2015).

415. *Id.* at 513. *See generally* Brad Plumer, *Here's a Simple, 60-Second Primer on Bitcoin*, WASH. POST (Apr. 3, 2013), https://www.washingtonpost.com/news/wonk/wp/2013/04/03/heres-a-simple-60-second-primer-on-bitcoin/ (providing facts about Bitcoin, how it's used, and how it works).

416. Swearingen, *supra* note 412.

417. *Id.*

418. *Id.*

419. Nora V. Demleitner, *Organized Crime and Prohibition: What Difference Does Legalization Make?*, 15 WHITTIER L. REV. 613, 617 (1994).

420. Böhme, *supra* note 234, at 3.

421. Andy Greenberg, *Meet the Hackers Who Sell Spies the Tools to Crack Your PC (And Get Paid Six-Figure Fees)*, FORBES: SECURITY (Mar. 21, 2012, 9:08 AM), http://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/.

is a crummy business to be in."[422] Some sellers, however, seem perfectly comfortable in the legally grey environment of exploit sales. Vupen is a French exploit firm that is widely disparaged in security communities, but this has not been a deterrent. Vupen's founder, Chaouki Bekrar, recently founded Zerodium, a new firm that focuses exclusively on high-end exploits.[423]

Grey market exploit vendors often sell to research firms,[424] governments, and defense contractors. For everyone else, including those engaged in organized crime, there is the black market. Black markets thrive when there is a demand for goods or services that cannot be sold in the open market.[425] Prices in the black market are also often higher because the seller is risking more by selling in that market than he or she would by selling in a legitimate market.[426]

Sellers of vulnerabilities on the black market typically either follow a purchase model or a hacker-for-hire model.[427] Black market forums on the darknet are governed by a variety of internal rules and norms, including harsh condemnation of sellers who scam buyers.[428] In lower level markets, buyers are often interested in spam, phishing tools, and credit card numbers.[429] Sales of zero-day exploits are mainly observed in more sophisticated markets.[430]

Currently, the market for software vulnerabilities is unregulated, unstructured, decentralized, and lacks transparency in almost every important area.[431] Bambauer and Day note that the software vulnerability market's flaws include high transaction costs and informational asymmetry.[432] The Arrow paradox also complicates matters: because vulnerabilities are an information good, it is impossible to ensure exclusivity of the knowledge being purchased.[433] This lack of exclusivity is a problem for both buyer and seller: sharing the information to establish its value also destroys its value.

---

422. Andy Greenberg, *Inside Endgame: A Second Act for the Blackwater of Hacking*, FORBES: SEC. (Feb. 12, 2014, 9:00 AM), http://www.forbes.com/sites/andygreenberg/2014/02/12/inside-endgame-a-new-direction-for-the-blackwater-of-hacking/ (internal quotation marks omitted).

423. Andy Greenberg, *Here's a Spy Firm's Price List for Secret Hacker Techniques*, WIRED: SEC. (Nov. 18, 2015, 7:26 AM), http://www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques/.

424. Fidler, *supra* note 26, at 27.

425. Demleitner, *supra* note 419, at 616.

426. Igor V. Dubinsky, *How Bad Boys Turn Good: The Role of Law in Transforming Criminal Organizations into Legitimate Entities by Making Rehabilitation an Economic Necessity*, 5 DEPAUL BUS. & COM. L.J. 379, 384 (2007); *see also* Demleitner, *supra* note 419, at 617.

427. Radianti et al., *supra* note 305, at 2.

428. *Id.* at 4.

429. *Id.* at 5.

430. *Id.* at 6.

431. Oriola, *supra* note 8, at 512–13.

432. Bambauer & Day, *supra* note 226, at 1100.

433. 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, 615 (1962).

Zero-day sales are especially tricky because of potential timing issues.[434] Charlie Miller recounts a personal experience where he had almost completed a sale when the vulnerability was patched.[435] With no more zero-day value, the sale fell through.

Vulnerability sales often require proof of concept, in which case the seller will have to build a working exploit.[436] At that time, the seller is faced with another choice because he or she now has the start of a product, the exploit, which could demand a high price on the black market.[437] Black markets for exploits emerged long before legitimate vulnerability markets, and early market participants often traded exploits among themselves for no payment other than prestige.[438]

Vulnerability markets have not been examined extensively in the current academic literature. Attempts to explore this topic have often focused on theoretical approaches for designing a legal market, economic modeling, or direct observation.[439] Some observational research into black markets and zero-day exploits has examined popular exploit archives, communications in IRC channels, and the appearance of virus signatures in executable files.[440]

4. Vulnerability Market Regulation

In the aftermath of cyber events like Stuxnet, the Target breach, and the OPM hack, Congress has taken steps towards regulating cybersecurity.[441] The U.S. government has benefited from the market for zero-day vulnerabilities, but policymakers cannot continue to ignore the market's harmful effects.[442] Currently, the discovery, development, and sale of vulnerabilities and exploits is morally and ethically grey at best. Future vulnerability market regulations should address a way to verify that market participants are behaving ethically.[443]

---

434. MILLER, *supra* note 323, at 8–9.

435. *Id.* at 9.

436. Kuehn & Mueller, *supra* note 47, at 3.

437. *Id.*

438. MILLER, *supra* note 323, at 2.

439. Radianti et al., *supra* note 305, at 1.

440. Bilge & Dumitras, *supra* note 62; Radianti, *supra* note 18. IRC stands for "Internet Relay Chat" and is an application protocol used for the transmission of text. *IRC FAQ*, MIRC, http://www.mirc.com/ircintro.html (last visited Aug. 29, 2016).

441. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014); National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066 (2014); Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014); Andy Greenberg, *Congress Slips CISA Into a Budget Bill That's Sure to Pass*, WIRED: SEC. (Dec. 16, 2015, 12:24 PM), http://www.wired.com/2015/12/congress-slips-cisa-into-omnibus-bill-thats-sure-to-pass/.

442. Stockton & Golabek-Goldman, *supra* note 242, at 243; *see also* Kannan & Telang, *supra* note 370, at 726 (noting the importance of social welfare concerns when deciding whether to regulate a market).

443. *See* Lisa J. Borodkin, Note, *The Economics of Antiquities Looting and a Proposed Legal Alternative*, 95 COLUM. L. REV. 377, 395 (1995) (noting the difficulty of establishing that antiquities were excavated illegally).

Matwyshyn notes that one possibility is that Congress will prohibit the sale of all exploits for national security reasons, which could have harmful effects for security vulnerability research.[444] Criminalizing the market would have the greatest effect on sellers, who might shift to a legitimate market if one is available,[445] or they might go deeper into the black market and raise their prices. Widespread adoption of export controls like the Wassenaar Arrangement could have similar effects. With their legal options limited, freelance security researchers might choose to end their research or enter the black market. Kirsch recommends that any potential regulations recognize and legitimize the beneficial effects of the activities of grey hat hackers.[446]

As noted above, the current legal market for vulnerabilities is decentralized and unregulated. Radianti, Rich, and Gonzalez designed a simulation model to explore how the legal–illicit market duality will develop in the long run.[447] Their findings underscore the need for some type of regulation, internal or external. Consistency in the market will be vital. According to their model, if vendors learn about vulnerabilities through the legal market, and do not consistently fix these flaws, software security and quality could be even worse than they would be in the absence of any legal vulnerability market.[448] Thus, any legitimate vulnerability market must receive the full cooperation of software vendors.

In their research, Choi, Fershtman and Gandal considered the possibility of mandatory disclosure requirements for vendors once they learn about vulnerabilities through bug-bounty programs.[449] This approach might increase the incentive to promptly fix vulnerabilities, but regulators would need to establish a disclosure level that is adequate for persuading users to install patches without providing so much information that malicious hackers can reverse engineer an exploit based on the disclosure.

To encourage responsible participation in vulnerability markets, some scholars have proposed some type of immunity. Bambauer and Day, for example, recommend granting researchers immunity from intellectual property litigation if they follow a responsible disclosure model.[450] One of the requirements their proposal would include is a prohibition on weaponizing the vulnerability,[451] but this may prove difficult because proof-of-concept demonstrations are important for buyers. If the concept of weaponization is defined as including something more than creating a basic exploit demonstration, it will be much easier to adhere to this requirement. The end goal of Bambauer and Day's recommendation is to make using the black market less appealing,[452] which is also a goal of this Article.

444. Matwyshyn, *Speech*, *supra* note 146, at 840.

445. *See* Radianti et al., *supra* note 305, at 8 (predicting that market participants would migrate to an attractive legal market for these products); Fidler, *supra* note 26, at 80.

446. Kirsch, *supra* note 5, at 387.

447. Radianti et al., *supra* note 305, at 1.

448. *Id.* at 10.

449. Choi et al., *supra* note 297, at 868.

450. Bambauer & Day, *supra* note 226, at 1086.

451. *Id.* at 1088.

452. *Id.* at 1090–91.

Bambauer and Day suggest employing a trusted third party to act as a coordinator for vulnerability deals,[453] a possibility that we examine in more detail in Part IV.

Other suggestions for regulating the vulnerability markets have included proposals for a "cap and trade" system for vulnerabilities[454] or imposing export restrictions.[455] Export restrictions are currently the most likely development in the present legal environment. The Wassenaar Arrangement, a voluntary international export control regime, was recently amended to include intrusion software.[456] Fidler notes that malware and zero days were not the original target of the changes to the Wassenaar Arrangement.[457] Instead, these changes were focused on products like the surveillance software that the firm Hacking Team sells to governments.[458]

However, the zero-day market might still be affected, depending on how adopters implement the new recommendations. In 2015, the Bureau of Industry and Security ("BIS") at the Department of Commerce issued a proposed rule for implementing the Wassenaar Arrangement.[459] The proposal by BIS would impose license requirements for the export of technology relating to intrusion software.[460] Because exploits are often integral in intrusion software, this could easily encompass the market for zero days.[461] Many members of Congress and the security industry have expressed opposition to the proposed rule, warning that it would hurt security research.[462] In response, BIS posted an open letter in which U.S. Secretary of Commerce Penny Pritzker states that the United States has proposed eliminating "the controls on the technology required for the development of intrusion software."[463] If such changes are implemented, the restrictions would still apply to intrusion software, but not to the dual-use upstream research that contributes to intrusion software.

The CFAA is a frequent guest in discussions of domestic vulnerability market concerns. Some scholars would narrow the CFAA by crafting a definition

---

453. *Id.* at 1101.

454. Fidler, *supra* note 26, at 30.

455. Stockton & Golabek-Goldman, *supra* note 242, at 243.

456. Fidler, *supra* note 26, at 146.

457. *Id.* at 147–48.

458. *Id.*

459. Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. 28,853 (Proposed May 20, 2015) (to be codified at 15 C.F.R. pts. 740, 742, 748, 772, 774).

460. *Id.*

461. *See* Kim Zetter, *Hacking Team Leak Shows How Secretive Zero-Day Exploit Sales Work*, WIRED: SEC. (Jul. 24, 2015, 7:00 AM), http://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/.

462. Nate Cardozo & Eva Galperin, *House Grills State Department Over Wassenaar Arrangement*, ELEC. FRONTIER FOUND. (Jan. 12, 2016), https://www.eff.org/deeplinks/2016/01/house-grills-state-department-over-wassenaar-arrangement.

463. Letter from Penny Pritzker, U.S. Sec'y Commerce, to Am. Petrol. Inst. et al. (Mar. 1, 2016), https://www.bis.doc.gov/index.php/forms-documents/doc_download/1434-letter-from-secretary-pritzker-to-several-associations-on-the-implementation-of-the-wassenaar-arrang.

of "authorization" to address current ambiguity and potentially allow more leeway for beneficial security research.[464] Others would instead add new provisions to the CFAA to broaden it. Because of the sensitivity of critical infrastructure, Stockton and Golabek-Goldman propose amending the CFAA to criminalize the sale of some types of zero-day exploits to terrorists, rogue governments, and other entities adversarial to the United States.[465] They also note that for the proposed changes to be effective, the United States should have the ability to prosecute foreign researchers who sell exploits to governments hostile to the United States.[466] Extra-territoriality issues must be considered carefully, however, and when neither buyer nor seller is located in the United States, it is unclear if a nexus to this country is present if there is merely a possibility that an exploit could be used against the United States.

Some scholars have proposed that regulations might focus on creating more-secure code. Stockton and Golabek-Goldman's proposal would emphasize software used by critical infrastructure.[467] Matwyshyn, drawing from the common law, proposes a reasonable expectation of code safety to address informational asymmetry.[468]

In this Article, we present a new model for regulating the vulnerability market. Our ambitious proposal would increase pricing transparency, facilitate exchanges between vendors and sellers at a fair market price, and provide an institution that promotes and contributes to innovative security research. In shaping this proposal, we drew from analogous market models, which is the subject to which we now turn.

III. CYBERSECURITY AND DIFFERENT MARKET APPROACHES

In the previous parts, we focused on the technology and policy issues relating to information security, software, and the vulnerability market. In this Part, we will examine other types of markets, both legal and illegal, that provide inspiration and support for our proposed vulnerability market model.

A. Regulated Financial Markets

The first type of market we explore is financial markets, where investors make or lose millions. Financial markets may be based on many different financial instruments.[469] The trade of financial instruments enables the creation of wealth or the shifting of risk, or both.[470] Securities are a category of financial instrument, which includes stocks. In the stock market, a company that needs to raise money can sell stock to investors. Selling stock provides the company with capital; the

---

464. Kirsch, *supra* note 5, at 399.
465. Stockton & Golabek-Goldman, *supra* note 242, at 264–65.
466. *Id.* at 263–64.
467. *Id.* at 242
468. Matwyshyn, *Hidden Engines*, *supra* note 151, at 139.
469. *See* 12 U.S.C. § 5341(8) (2012) (defining "financial instrument").
470. *See* Bernard J. Karol, *An Overview of Derivatives as Risk Management Tools*, 1 STAN. J.L. BUS. & FIN. 195, 196 (1995).

purchasers then bear part of the risk that the company could fail—but they also reap part of the reward if the company succeeds.

Another broad category of financial instrument is the derivative; so called because the contracts derive their value from some underlying asset.[471] Derivatives are primarily categorized as either options or forwards.[472]

Stock options are a common form of option that many employees encounter as part of their benefits. When a company issues stock options to an employee, he or she has the option, but not the obligation, to purchase company stock at an agreed upon price—the "strike price."[473] If the strike price is less than the market price, the employee has profited as soon as she exercises the option. If the strike price is higher than the market price, on the other hand, the stock option is worthless.

Forwards are sales contracts for future delivery.[474] These are unlike spot contracts, which are settled immediately.[475] Futures are forward contracts that are traded in exchanges instead of between private parties.[476] Futures contracts allow parties to mitigate price risks, and the trading of futures also serves a price-discovery function for the spot market.[477] Lots of information is contained in the price of futures contracts.

This characterization of prices as vehicles for information comes from the work of Nobel-Prize-winning economist Friedrich Hayek.[478] The price signals many things to purchasers and enables them to more efficiently allocate resources.[479] When a price increases, consumers do not know whether that increase is due to lower supply or higher demand. They just know that they have to economize their use of the resource, either by using less or by putting what they have to a more profitable use.[480] Hayek praises the price system because it leads to consumers making the more desirable decision without being told why the

---

471. Matthew R. Quetsch, Note, *Corporations and Hedging: Distinguishing Forwards from Swaps Under the Commodity Exchange Act Post-Dodd-Frank*, 39 J. CORP. L. 895, 896 (2014); Yesha Yadav, *The Problematic Case of Clearinghouses in Complex Markets*, 101 GEO. L.J. 387, 401 (2013).

472. Karol, *supra* note 470, at 195.

473. NerdWallet, *Understanding Employee Stock Options*, NASDAQ (Dec. 3, 2013, 3:12 PM EDT), http://www.nasdaq.com/article/understanding-employee-stock-options-cm308665.

474. Karol, *supra* note 470, at 196; Quetsch, *supra* note 471, at 904.

475. Quetsch, *supra* note 471, at 899.

476. Karol, *supra* note 470, at 196.

477. Michael Greenberger, *Closing Wall Street's Commodity and Swaps Betting Parlors: Legal Remedies to Combat Needlessly Gambling Up the Price of Crude Oil Beyond What Market Fundamentals Dictate*, 81 GEO. WASH. L. REV. 707, 711–12 (2013).

478. F.A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 525 (1945); *see also* Chao-Hung Christopher Chen, *Information Disclosure, Risk Trading and the Nature of Derivative Instruments: From Common Law Perspective*, 4 NAT'L TAIWAN U. L. REV. 1, 11 (2009) ("Presumably, in an efficient market, the current market price should reflect all the information available in the market.").

479. Hayek, *supra* note 478, at 525.

480. *Id.* at 526.

decision is desirable.[481] Hayek's theory of prices views the price system as facilitating "a coordinated utilization of resources based on an equally divided knowledge."[482]

Careful research goes into estimating which way a particular futures market is going to move, and this research adds new information that can contribute to price discovery.[483] This is a way that the futures market can influence the spot market.[484] Timothy Lynch refers to part of the informational benefit as "information arbitrage." If an investor has knowledge that the current price does not take into account, the terms of that investor's derivatives contract signal to the marketplace that there is additional information that other investors should consider.[485]

Investors often use futures contracts to trade commodities. Under U.S. law, a "commodity" is defined to include goods, services, and interests that may be subject to contracts for future delivery.[486] This legal definition also identifies over two-dozen specific agricultural products as being commodities. If a trade involves a commodity falling within this definition, the trade likely falls within the jurisdiction of the Commodity Futures Trading Commission ("CFTC").[487] However, some things that meet this definition of commodity, like economic indexes, may be exempt from CFTC jurisdiction.[488]

An investor in the futures market may be either hedging or speculating.[489] Hedging generally refers to the practice of balancing the party's own risk,[490] because the party is actually purchasing or selling the good subject to the futures contract. The commodity futures market originally developed to enable farmers to hedge against the possibility that a future harvest will be poor.[491] Speculating refers to the practice of investing without an intended connection to the underlying commodity.[492] Bernard Karol describes this dichotomy by explaining that the goal of a hedger is to reduce risk, while the goal of a speculator is to acquire risk.[493]

---

481. *Id.* at 527.

482. *Id.* at 528.

483. Yadav, *supra* note 471, at 403.

484. Greenberger, *supra* note 477, at 713; Timothy E. Lynch, *Gambling by Another Name: The Challenge of Purely Speculative Derivatives*, 17 STAN. J.L. BUS. & FIN. 67, 111–12 (2011).

485. Lynch, *supra* note 484, at 82.

486. 7 U.S.C. § 1a(9) (2012) (defining "commodity").

487. Matthew Beville, Dino Falaschetti, and Michael J. Orlando, *An Information Market Proposal for Regulating Systemic Risk*, 12 U. PA. J. BUS. L. 849, 895 (2010).

488. *Id.* at 896.

489. Karol, *supra* note 470, at 197.

490. Quetsch, *supra* note 471, at 896; *see* Arrow, *supra* note 433, at 611.

491. Karol, *supra* note 470, at 197–98; *see also* Chen, *supra* note 478, at 15 ("As a US judge has argued, the securities market was established for the formation of capital and the futures market for hedging.").

492. Quetsch, *supra* note 471, at 896.

493. Karol, *supra* note 470, at 197. Lynch points out that this characterization of the relationship between the speculator and hedger provides the basis for the insurance industry. Lynch, *supra* note 484, at 79.

Michael Greenberger notes that speculators play a vital role in futures markets because speculation ensures that the market has sufficient liquidity.[494]

A speculator might sometimes act as a middleman. Consider a corn farmer. Last year, the price of corn dropped to $3 a bushel. This year, the corn farmer knows that she needs at least $4 a bushel to make a profit. A speculator who believes that the price of corn will be $5 a bushel might agree to buy the farmer's corn for $4 a bushel. The speculator then enters into another contract to sell the corn at $5 a bushel to a cereal maker. At harvest time, the market price is $5 a bushel. The speculator has a profit, the ultimate buyer acquired the corn at market rate, and while the farmer does not get the extra $1 per bushel from that contract, she was nonetheless protected against the risk that the price would be too low to make a profit.

The trade of financial instruments can be facilitated by exchanges and clearinghouses.[495] An exchange is the marketplace where financial instruments are traded.[496] Clearinghouses are the intermediaries that ensure the trades are settled.[497] Yesha Yadav notes that clearinghouses also support the stability of the exchanges and improve market efficiency.[498]

Derivatives can lead to profits for investors, and as noted above, may also facilitate price discovery. Third parties like brokers, researchers, and exchanges also benefit from trades.[499] However, there are many negative sides to derivative markets. Derivatives are sometimes characterized as a zero-sum game, because one person's successful deal relies on another person's deal failing.[500] Derivatives can also increase systemic economic risk. Before 2008, the average person likely had never heard of a credit default swap or a credit derivative. When the housing market collapsed, the risks of overusing derivatives became very clear.[501]

Purely speculative derivatives are often looked at with a skeptical eye.[502] Lynch argues that such contracts reduce social wealth, increase moral hazard, and are economically irrational.[503] In Lynch's view, purely speculative derivative contracts are not about risk shifting, but in fact "create risk where no risk existed before."[504]

---

494. Greenberger, *supra* note 477, at 714.
495. Yadav, *supra* note 471, at 408.
496. *Id.*
497. *Id.* at 409.
498. *Id.* at 409–11.
499. Lynch, *supra* note 484, at 121.
500. Karol, *supra* note 470, at 196; *see also* Lynch, *supra* note 484, at 69–70 (discussing the opposite outcomes for two investors where one invested in derivatives that would pay out if the housing market crashed, and the other invested in derivatives that would pay out if the housing market did not crash).
501. Yadav, *supra* note 471, at 390–91.
502. Lynch, *supra* note 484, at 121; Yadav, *supra* note 471, at 440 (noting the risks that speculative swaps pose to clearinghouses).
503. Lynch, *supra* note 484, at 67.
504. *Id.* at 93.

It was in 1995 that a single rogue trader's bad choices and bad luck with speculative derivatives destroyed Barings Bank, the British merchant bank that financed the Louisiana Purchase.[505] Derivatives are also credited with the near-collapse of AIG in 2008. Further, Steven McNamara suggests that derivatives contributed significantly to the environment of uncertainty that ultimately drove the Wall Street powerhouse Lehman Brothers into bankruptcy.[506] Speculative derivative trading is also the downfall of the antagonists in the 1983 film *Trading Places*.[507]

The Commodity Exchange Act ("CEA") imposes limits on excessive speculation in commodity markets, though a loophole concerning swaps markets has enabled traders to avoid these limits.[508] Under the CEA, excessive speculation occurs when commodity contracts cause "sudden or unreasonable fluctuations or unwarranted changes in the price of such commodity."[509] Scholars have criticized excessive speculation in markets for derivatives.[510] Greenberger, former Director at the CFTC, identifies excessive speculation in oil futures as the cause of record high oil prices in 2008.[511] He warns of the unsupported price changes that may occur if too many people are betting on the direction that the market will move without possessing the commodity.[512] While the true cause of the volatility of oil prices is still debated,[513] in 2012 Greenberger testified before Congress that the amount of oil being traded in contracts was 33 times greater than the worldwide oil supply.[514]

Markets for some commodities operate relatively independently of other financial markets or exogenous factors.[515] With other commodities, future prices can be anticipated based on information about other aspects of the market or

---

505. James Titcomb, *Barings: The Collapse That Erased 232 Years of History*, TELEGRAPH: FIN. (Feb. 23, 2015, 6:00 AM), http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/11427501/Barings-the-collapse-that-erased-232-years-of-history.html. Barings was one of two banks that financed the Louisiana Purchase, with the other bank being the Dutch bank Hope & Co. *Id.*

506. Steven McNamara, *Financial Markets Uncertainty and the Rawlsian Argument for Central Counterparty Clearing of OTC Derivatives*, 28 NOTRE DAME J.L. ETHICS & PUB. POL'Y 209, 235–36 (2014).

507. TRADING PLACES (Paramount Pictures 1983).

508. Greenberger, *supra* note 477, at 715–16.

509. 7 U.S.C. § 6a (2012); Greenberger, *supra* note 477, at 738.

510. *E.g.*, Greenberger, *supra* note 477, at 716; Lynch, *supra* note 484, at 67.

511. Greenberger, *supra* note 477, at 735; *but see* James Smith, *The 2008 Oil Price Shock: Markets or Mayhem?*, RES. FOR THE FUTURE (Nov. 6, 2009), http://www.rff.org/blog/2009/2008-oil-price-shock-markets-or-mayhem (arguing that excessive speculation was not the cause of the fluctuation in oil prices); *accord* Michael D. Plante & Mine K. Yücel, *Did Speculation Drive Oil Prices? Market Fundamentals Suggest Otherwise*, ECON. LETTER, Oct. 2011, at 1, 1.

512. Greenberger, *supra* note 477, at 713.

513. *See* Smith, *supra* note 511.

514. *Gas Prices and Oil Speculation: Hearing Before the Dem. Steering & Policy Comm.*, 112th Cong. (2012) (statement of Michael Greenberger, Former Director, Div. Trading & Mkts., Commodity Futures Trading Comm'n).

515. Beville et al., *supra* note 487, at 879.

society.[516] The price of frozen concentrated orange juice on the futures market, for example, is strongly related to the weather in Florida.[517] Wars can affect availability and therefore the price of commodities as well.[518]

Having inside knowledge of the determining factors can enable insider trading in the futures market.[519] While insider trading is prohibited by the SEC, it is the CFTC that has regulatory authority over most futures contracts, and until recently the CFTC only prohibited insider trading by market professionals and CFTC employees.[520] A statutory ban on a specific type of insider trading was added by the Dodd-Frank Act in 2010. Called the "Eddie Murphy Rule," Section 746 of the Dodd-Frank Act bans traders from knowingly using insider information obtained from non-public government sources.[521] The CFTC urged the adoption of this rule based on concerns about the type of crop report leak that drove the subplot of *Trading Places*.[522]

B. Markets for Ideas

In Section III.A, we explained the Hayekian approach to prices that views prices as being generated through the consolidation of information. The concept of information markets builds on these principles.[523] Information markets deal in ideas, not goods. The theory is that consolidating large amounts of information from investors can provide accurate predictions for real world events.[524] These predictions are reflected in the market price for the contract as the relevant events unfold. Beville's research team focuses on the potential of information markets to track systemic economic risk and potentially mitigate future economic crises.[525]

Participants in information markets have fundamentally different motivations from people trying to reach a decision through deliberation. When a person is arguing a position, she wants to *convince others* that he or she is correct. When an investor is participating in a market, he or she wants to be *objectively*

---

516. *Id.* at 885.

517. Cass R. Sunstein, *Group Judgments: Statistical Means, Deliberation, and Information Markets*, 80 N.Y.U. L. REV. 962, 1032 (2005).

518. *See* Chen, *supra* note 478, at 4.

519. *See id.* at 41 (comparing the relative legitimacy of insider dealing in futures for hedgers and speculators).

520. Zachary T. Knepper, *Examining the Merits of Dual Regulation for Single-Stock Futures: How the Divergent Insider Trading Regimes for Federal Futures and Securities Markets Demonstrate the Necessity for (and Virtual Inevitability of) Dual CFTC-SEC Regulation for Single-Stock Futures*, 3 PIERCE L. REV. 33, 43–44 (2004).

521. 7 U.S.C. § 6c(a)(4) (2012); Tim Bakken, *Dodd-Frank's Caveat Emptor: New Criminal Liability for Individuals and Corporations*, 48 WAKE FOREST L. REV. 1173, 1193 (2013).

522. Bakken, *supra* note 521, at 1193. In reality, a similar abuse of non-public government information from crop reports occurred in 1905 for the cotton market. Donna M. Nagy & Richard W. Painter, *Selective Disclosure by Government Officials and the Case for an FGD (Fairer Government Disclosure) Regime*, 2012 WIS. L. REV. 1285, 1310–11.

523. *See* Sunstein, *supra* note 517, at 1023–24.

524. Cherry, *supra* note 2, at 427.

525. Beville et al., *supra* note 487, at 862.

correct.[526] This subtle distinction is the line between learning everything that supports her argument and studying all of the information available.[527] Information markets provide incentive for participants to share all information, instead of just the information that is relevant to their individual interests.[528]

Depending on implementation, a market for information security vulnerabilities could be an information market. Information markets have appeared in many forms, some more successful than others. Since 1988, participants have used the Iowa Electronic Markets ("IEM") to wager on the outcome of national elections.[529] The IEM has outperformed polls 76% of the time.[530]

In part because of IEM's success, some scholars have considered how information markets could benefit government agencies tasked with making policy decisions or preparing for natural disasters.[531] The Hollywood Stock Exchange was another successful and accurate information market that allowed investors to predict box office returns and Oscar nominations.[532] Internal information markets can also benefit businesses by encouraging uncensored and anonymous evaluation of the company's activities.[533]

Information markets might trade in play money or real money. The Hollywood Stock Exchange, for example, used play money. In 2011, an entrepreneur promoted BeeWise, a software vulnerability event futures market that also used play money.[534] The IEM uses real money, but participants can invest no more than $500.[535]

Information markets do not always work, however. Powerful speculators could potentially manipulate these markets.[536] Some topics are not appropriate for information markets because the market participants would not have enough knowledge.[537] An information market may also fail if there are not enough market participants.[538]

Sometimes, the failure is because of public interest concerns. The Defense Advanced Research Projects Agency ("DARPA") proposed the Policy

---

526. *Id.* at 866–67; Sunstein, *supra* note 517, at 970.

527. Sunstein, *supra* note 517, at 1048–49.

528. Cherry, *supra* note 2, at 427–28.

529. *Id.* at 428–29.

530. Beville et al., *supra* note 487, at 865; Cherry, *supra* note 2, at 429; Sunstein, *supra* note 517, at 1030.

531. Beville et al., *supra* note 487, at 873; Sunstein, *supra* note 517, at 1027.

532. Andrew S. Goldberg, Note, *Political Prediction Markets: A Better Way to Conduct Campaigns and Run Government*, 8 CARDOZO PUB. L. POL'Y & ETHICS J. 421, 430 (2010); Sunstein, *supra* note 517, at 1031–32.

533. Sunstein, *supra* note 517, at 1032–33.

534. *See* Eduardo Vela, *Creating a Decentralized Security Rewards Market*, SIRDARCKCAT BLOG (Mar. 28, 2016), http://sirdarckcat.blogspot.com/2016/03/creating-decentralized-security-rewards.html (identifying Beewise and Consensus Point as having "briefly experimented with" Böhme's exploit derivatives in 2011).

535. Cherry, *supra* note 2, at 428–29.

536. Sunstein, *supra* note 517, at 1037.

537. *Id.* at 1040.

538. *Id.* at 1041.

Analysis Market as an information market that would focus on national security matters.[539] The plan was to make the market only available within federal agencies like the FBI, but then the media got wind of DARPA's proposal. The Policy Analysis Market was painted as a futures market for terrorist attacks, causing its political feasibility to plummet.[540] Then-Senator Byron Dorgan called it "morally bankrupt" to turn international politics into something people could bet on.[541]

Regulatory concerns also limit the proliferation of information markets in the United States. Some of these concerns are related to the similarities between information markets and gambling, with some opining that the Unlawful Internet Gambling Enforcement Act of 2006 ("UIGEA") may apply to information markets.[542] If the UIGEA does not apply to information markets, the CFTC will likely have jurisdiction over event futures trading.[543] The CFTC prohibits the trade of contracts relating to terrorism, war, other unlawful acts, or matters contrary to the public interest.[544] The CFTC began exploring event contracts in more detail in 2008,[545] but to date there has been no proposed rule.

The development of a new information market could face significant regulatory costs. One option is for the new market to seek a no-action letter from the CFTC, or to fold itself into in an existing exchange.[546] Academic markets like the IEM continue to be well received by the CFTC. In October 2014, the CFTC granted "no-action relief" to permit a university in New Zealand to proceed with plans to make an academic, nonprofit event contract market open to participants from the United States without having to comply with the CEA.[547] On the other hand, when North American Derivatives Exchange ("NADEX") proposed adding for-profit political futures contracts to their services, the CFTC found that such contracts "involve gaming and are contrary to the public interest."[548] NADEX is, however, approved by the CFTC to trade economic event options.[549]

---

539. Alan Joch, *Is There a Future for Futures Trading?*, FED. COMPUTER WK. (Aug. 30, 2004), https://fcw.com/articles/2004/08/30/is-there-a-future-for-futures-trading.aspx.

540. Sunstein, *supra* note 517, at 1028.

541. *Id.* at 1028.

542. Cherry, *supra* note 2, at 429–30; Goldberg, *supra* note 532, at 431.

543. *But see* Beville et al., *supra* note 487, at 897 (suggesting that government sponsorship of information markets would preempt concerns about violations of gambling statutes).

544. 17 C.F.R. § 40.11(a) (2016).

545. Beville et al., *supra* note 487, at 897; Goldberg, *supra* note 532, at 435–36.

546. Beville et al., *supra* note 487, at 896–97.

547. Press Release, U.S. Commodity Futures Trading Comm'n, CFTC Staff Provides No-Action Relief for Victoria Univ. of Wellington, N.Z., to Operate a Not-For-Profit Market for Event Contracts and to Offer Event Contracts to U.S. Persons (Oct. 29, 2014), http://www.cftc.gov/PressRoom/PressReleases/pr7047-14.

548. Press Release, U.S. Commodity Futures Trading Comm'n, CFTC Issues Order Prohibiting North American Derivatives Exchange's Political Event Derivatives Contracts (Apr. 2, 2012), http://www.cftc.gov/PressRoom/PressReleases/pr6224-12.

549. *Trade Economic Events*, NADEX, http://www.nadex.com/trade-economic-events.html (last visited Dec. 8, 2015).

The CEA defines a commodity as "all services, rights and interests in which contracts for future delivery are presently or in the future dealt in."[550] Goldberg argues that this definition of a commodity is broad enough that it could cover contracts in a political prediction market.[551] The CFTC's recent actions concerning NADEX and the university in New Zealand support this.

Trade Exchange Network ("TEN") and Intrade,[552] two firms that trade in binary option event futures contracts, recently challenged the CFTC's jurisdiction.[553] The event futures traded through the services included predictions about climate change and the unemployment rate in the United States at a particular future date.[554] Options would be purchased as either put options, which would pay out if the event does not occur, or call options, which would pay out if the event does occur.[555] The binary nature of the options meant that if an investor bought a put option, and the event did occur, the investor would get nothing.[556] The court held that such options fell within the CFTC's jurisdiction.[557]

C. Risk Shifting

Risk shifting is very important to the economy. Kenneth Arrow notes that if individuals are unable to buy protection against uncertainty, this reduces social welfare.[558] Jens Grossklags, Benjamin Johnson, and Nicolas Christin focus on the price of uncertainty, which they define as the difference between the maximum payoff expected in two different environments: one with complete information, and one with incomplete information.[559] When a party wants to avoid a risk, there is a net benefit to societal welfare when the party can pay a premium to have someone else take on part of that risk.[560] As long as the premium paid is less than the expected loss if the risk occurs, the risk-shifting decision is economically rational.

Any insurance provider, regardless of what they insure, enables their clients to hedge against adverse occurrences by shifting part of the risk to the insurer. Life insurance plans are not issued because somebody *wants* to die. They are instead hedging against the possibility of death so that their family will not be left without any support if a tragic event occurs. Of course, insurance covers much

---

550. 7 U.S.C. § 1a(9) (2012).

551. Goldberg, *supra* note 532, at 436.

552. *See* Andrew Rice, *The Fall of Intrade and the Business of Betting on Real Life*, BUZZFEEDNEWS (Feb. 20, 2014, 8:25 PM), http://www.buzzfeed.com/andrewrice/the-fall-of-intrade-and-the-business-of-betting-on-real-life.

553. Commodity Futures Trading Comm'n v. Trade Exch. Network Ltd., 117 F. Supp. 3d 29, 35–36 (D.D.C. 2015).

554. *Id.* at 34.

555. *See* S. Wade Hansen, *Options Basics: Puts and Calls*, FORBES (Aug. 24, 2006, 10:00 AM), http://www.forbes.com/2006/08/23/investools-options-ge-in_wh_0823investools_inl.html (defining puts and calls in the context of options).

556. *Trade Exch. Network Ltd.*, 117 F. Supp. 3d at 35–35.

557. *Id.* at 37–38.

558. Arrow, *supra* note 433, at 612.

559. GROSSKLAGS ET AL., *supra* note 232, at 1.

560. Lynch, *supra* note 484, at 80.

more than life and death. Paying premiums for health insurance allows individuals to hedge against the risk of future catastrophic medical costs. Commercial General Liability policies allow business owners to hedge against the risk of future events that could harm their business. Drivers hedge against the risk of future accidents by paying for automobile insurance.

Financial markets for derivatives are similar to the insurance industry in that they both involve risk shifting.[561] Arrow characterizes insurance as a risk-shifting mechanism that effectively involves parties placing bets on the state of nature.[562] The premiums collected by insurance companies are designed to reflect the insurer's risk exposure.[563] Christopher Chen argues that the duties of good faith and disclosure found in insurance law could also be found in other areas driven by risk shifting, namely the market for derivative contracts.[564]

The market for computer security works in similar ways. Computer users install anti-malware tools to mitigate risk. If this is not enough, cyber insurance allows further risk shifting.[565] The problem of determining appropriate premiums is a very difficult one, however, because risk in the cybersecurity context is often very broad and unpredictable, making it difficult for insurers to maintain balanced portfolios.[566] Part of this may be due to the current market for cyber insurance. Recent data indicate that less than a third of companies carry cyber insurance policies.[567] As demand grows, the business model for cyber risk shifting will mature.[568]

When two parties exchange their respective risks, information is vital because each party wants to know how much risk he or she is accepting.[569] One of the dangers of risk shifting is that it can create a moral hazard for the party with more knowledge and more ability to avoid the risk.[570] A party with superior information about a transaction can often reap greater benefits by selectively withholding information.[571] Arrow cites this moral hazard problem as a reason for personal property insurance being limited to the value of insured goods—it would not be wise to create an incentive to destroy things for the insurance money.[572]

---

561. Thomas Lee Hazen, *Disparate Regulatory Schemes for Parallel Activities: Securities Regulation, Derivatives Regulation, Gambling, and Insurance*, 24 ANN. REV. BANKING & FIN. L. 375, 377 (2005); Lynch, *supra* note 484, at 79.

562. Arrow, *supra* note 433, at 612.

563. Chen, *supra* note 478, at 18.

564. *Id.* at 20.

565. Böhme, *supra* note 234, at 3; Anderson & Moore, *supra* note 146, at 610; Zureich and Graebe, *supra* note 7, at 195.

566. Böhme, *supra* note 234, at 1.

567. Anderson, *supra* note 97, at 533.

568. Zureich & Graebe, *supra* note 7, at 197 (suggesting that cyber insurance will evolve in a manner similar to employment practices liability insurance).

569. Chen, *supra* note 478, at 3.

570. Arrow, *supra* note 433, at 613 (noting that fire insurance policies may weaken the motivation for fire prevention).

571. *See id.* at 614.

572. Arrow, *supra* note 433, at 612.

Yadav notes that in financial markets, clearinghouses serve a risk-sharing purpose, which may inadvertently provide market participants with an incentive to make reckless trading decisions.[573] Similarly, Anderson and Moore note that when financial fraud laws in the United Kingdom favored banks and placed high burdens on customers to establish fraud, bank staff often behaved carelessly, leading to more fraud.[574] Informational asymmetry is therefore extremely important to consider when evaluating a potential risk-shifting regime.

D. Markets for Illicit Goods

In this Section, we consider other illegal or legally ambiguous markets and the elements of criminality that underlie them. At the time of this writing, trading in software vulnerabilities is still a legally grey area, with the trade being considered appropriate or illicit mostly based on the motivations of the buyer. We posit that there is inelastic demand for zero days and other vulnerabilities. As long as countries, competitors, and criminals want to use computing technology to have an advantage over someone else, there will be a market for vulnerabilities. Scholars have noted the possibility that some aspects of the vulnerability trade could be criminalized.[575] Unfortunately, history shows that criminalizing transactions for goods that have an inelastic demand often backfires.

Igor Dubinsky notes that when a good or service is prohibited, criminal organizations emerge to provide that good or service.[576] The value of the good or service is then tied to the organization's skills at secrecy, rather than the quality of the product.[577] As the cost of avoiding detection increases, the cost of the product increases, and the more dangerous the market can potentially become.[578] Nora Demleitner argues that as a result of this, the laws against these practices may actually make these problems worse.[579]

Organized crime thrives in an environment where there is inelastic demand for a product or service that is prohibited by law.[580] Herbert Packer refers to laws against goods or services with inelastic demand as imposing a "crime tariff" that benefits entrepreneurs who are willing to risk being caught.[581] Even when there are competitors in the same illegal market, criminal organizations are likely to cooperate with each other and divide up territory, rather than allow conflicts to escalate into violence and increase everyone's chances of being caught.[582]

---

573. Yadav, *supra* note 471, at 392.
574. Anderson & Moore, *supra* note 146, at 610.
575. Stockton and Golabek-Goldman, *supra* note 242, at 264–65.
576. Dubinsky, *supra* note 426, at 409.
577. *Id.* at 410.
578. Demleitner, *supra* note 419, at 614.
579. *Id.* at 614.
580. Herbert Packer, *The Crime Tariff*, 33 AMERICAN SCHOLAR 551, 552–53 (1964).
581. *Id.* at 553.
582. Dubinsky, *supra* note 426, at 385.

The Prohibition era is a classic example of organized crime thriving in the face of laws prohibiting goods for which there is inelastic demand. Prohibition of alcoholic beverages changed things in unexpected ways. During Prohibition, regard for organized crime was sometimes closer to respect than fear.[583] Speakeasies replaced saloons, other drugs became more popular, and the illicit market for alcohol emphasized more efficient sources of alcohol, like whiskey, instead of beer.[584] There were fewer deaths from cirrhosis during Prohibition, but more deaths caused by alcohol poisoning.[585] This shift from less-risky to more-risky behavior by users is also seen in other illegal markets. When marijuana laws started to be more strictly enforced, the drug market shifted to more potent and dangerous drugs like cocaine.[586]

There are also thriving markets for nonrenewable illicit goods other than zero days. The sale of conflict diamonds is an example of such a market that harms social welfare. During the civil war in Sierra Leone, the rebels of the infamously brutal Revolutionary United Front were largely funded by the diamond trade.[587] In the vulnerability market, the biggest concern is often the motivations of the buyer, not the seller. Both markets, however, could be improved by greater transparency and incentives that reward socially beneficial behavior when making market transactions.

Cybersecurity and archaeology seem to have little in common, but unearthing zero days and ancient artifacts both take special skills. There are also ill-intentioned market players in both fields who would take advantage of these discoveries to generate a profit. The sale of antiquities looted from archaeological sites is a well-organized business that has been examined by many scholars.[588] In the illicit market for antiquities, profits are higher and penalties are lighter compared to the narcotics trade.[589] Patty Gerstenblith notes that looters may be paid $4 for a cuneiform tablet that is thousands of years old, and the purchaser could then sell the tablet for hundreds or thousands of dollars.[590]

Past attempts to regulate the antiquities market have included export controls and laws that make an artifact the property of the country where it was discovered.[591] Lisa Borodkin argues that reducing the economic incentives that support the antiquities trade would be an effective regulatory approach, and suggests creating incentives for looters to record their findings with the

583. Demleitner, *supra* note 419, at 623–24.
584. *Id.* at 624.
585. *Id.*
586. *Id.* at 633.
587. Amanda Bryant Banat, Note, *Solving the Problem of Conflict Diamonds in Sierra Leone: Proposed Market Theories and International Legal Requirements for Certification of Origin*, 19 ARIZ. J. INT'L & COMP. L. 939, 939–40 (2002).
588. *E.g.*, Patty Gerstenblith, *Controlling the International market in Antiquities: Reducing the Harm, Preserving the Past*, 8 CHI. J. INT'L L. 169, 169 (2007); Borodkin, *supra* note 443.
589. Borodkin, *supra* note 443, at 378.
590. Gerstenblith, *supra* note 588, at 180–81.
591. Borodkin, *supra* note 443, at 391–92.

government rather than selling to smugglers.[592] An analogous approach in the vulnerability market would emphasize incentives for discoverers to disclose vulnerability information to the owner of the code.

With the right incentives, a criminal organization may mature into a legitimate organization,[593] like how organized crime families in the United States invested Prohibition profits into the development of Las Vegas.[594] Dubinsky notes that at some point, it becomes more profitable for criminal organizations to become legitimate, and argues for flexibility in the law to assist this transition.[595] This is especially likely to happen when the law does not punish the reallocation of illegally obtained funds towards legal ventures.[596] Providing smaller actors in the market with more legal opportunities for work can also weaken illicit markets. For example, Borodkin suggests that the subsistence looters who take artifacts from archaeological sites could be employed and retrained to help find and preserve artifacts instead of selling them to smugglers.[597] This is the same type of evolution that has taken thousands of mischievous teenaged hackers and turned them into successful information security professionals.

IV. BUILDING A THRIVING VULNERABILITY MARKET

Market participants must work together for there to be a chance of an effective vulnerability marketplace. In exploring the need for collaboration between market participants, Yadav draws a comparison to the game theory model of the stag hunt.[598] In the stag hunt game, catching the stag requires players to work together. A quicker outcome would be for the players to go their own ways and each hunt rabbits, leading to everyone having a small reward instead of sharing a huge reward. In our proposal, the "stag" is a transparent, vibrant marketplace for vulnerabilities that improves social welfare by increasing security. Individual vulnerability sellers who chase rabbits may have a few sales, but as Miller noted, individual attempts to sell vulnerabilities and exploits can dissolve quickly due to unpredictable factors.[599] Moreover, by not chasing the stag, sellers are reducing the chance of success for everyone else.

At the center of our proposal is the clearinghouse that serves as the intermediary between buyer and seller. Many scholars have addressed the need for a trusted third party in the vulnerability market.[600] One of the strongest arguments for having a trusted intermediary is the Arrow Paradox.[601] Arrow observed that

592. *Id.* at 412–13.
593. Dubinsky, *supra* note 426, at 379.
594. Demleitner, *supra* note 419, at 621; Dubinsky, *supra* note 426, at 411.
595. Dubinsky, *supra* note 426, at 379.
596. *Id.* at 420.
597. Borodkin, *supra* note 443, at 414–15.
598. Yadav, *supra* note 471, at 417–18.
599. MILLER, *supra* note 323, at 9.
600. *E.g.*, Bambauer & Day, *supra* note 226, at 1101; MILLER, *supra* note 323, at 7; *see also* Radianti, *supra* note 18, at 193 (noting the role of moderators for judging the credibility of buyers and sellers in the black market).
601. Arrow, *supra* note 433, at 615; *see also* Kuehn & Mueller, *supra* note 47, at 7–8 (discussing the paradox in the context of vulnerability markets).

when information is the source of value, disclosing the information essentially destroys the value.[602] In the context of vulnerability markets, this plays out in the negotiations between buyer and seller. The seller is faced with a dilemma—how to establish the value of the information during negotiations without inadvertently giving the information away. A trusted intermediary can provide the solution.

The goal of our proposal is to provide a foundation for a well-functioning, rational marketplace for vulnerabilities, especially zero days. First, we address the type of incentives that might persuade sellers to participate in a vendor-focused marketplace instead of chasing rabbits. We then explain our proposed vulnerability market.

A. Crowding Out the Harmful Markets—An Economic Proposal

Ultimately, a legitimate vulnerability market's success depends on its ability to displace enough black and grey market transactions. Traditional wisdom tells us that if the chance of getting caught is small but the possible penalty is severe, actors may be deterred from committing a crime. On the other hand, even if the chance of getting caught is high, a sufficiently high reward could tempt a rational actor into illegal activity. As noted by Dubinsky, organized crime syndicates are likely to consider bribery costs and other factors when deciding whether to expand their operations.[603] The likelihood of committing a given crime is therefore directly related to the expected reward, and inversely related to the chance of getting caught times the possible penalty. The variables used in our analysis are provided in the table below.

Variable	Meaning
S_B	Likelihood of Sale (S) on the black market
S_G	Likelihood of Sale (S) on the grey market
S_W	Likelihood of Sale (S) on the white market
R_B	Reward (R) on the black market
R_G	Reward (R) on the grey market
R_W	Reward (R) on the white market
J	Likelihood of being caught (black market)
P	Penalty if caught (black market)
V	Visible recognition

Table 2: Variables.

602. Arrow, *supra* note 433, at 615.
603. Dubinsky, *supra* note 426, at 387.

Our first concern is the black market for vulnerabilities. The likelihood of sale on the black market (S_B) would be influenced by the likelihood of being caught (J), the penalty if caught (P) and the reward if the sale is completed (R_B). The function can be visualized as follows:

$$S_B = f(R_B - JP)$$

If the crime is to sell vulnerabilities and exploits on the black market, then the likelihood of engaging in that activity will go up as the possible reward goes up, and down as either the chance of getting caught goes up or the possible penalty goes up.

Proposals to regulate and deter harmful vulnerability markets are likely to focus on increasing either the likelihood of getting caught or the possible penalties. However, as the history of illicit economic industries shows, actors in an illegal business often simply increase prices when their risks increase, especially if there is inelastic demand. Accordingly, if regulators only focus on punishment for selling vulnerability information on the black market, the suppliers can simply raise their prices as a "crime tariff."[604] In this way, participation in the black market remains at an equilibrium, and those who are successful actually see their profits increase as a result of government intervention. This is an especially significant risk with vulnerability markets. In these markets, there is a total lack of transparency in terms of pricing, so suppliers can afford to make their prices entirely dependent upon their levels of risk, such that the prices go up when their risks go up:

$$R_B = f(JP)$$

By considering this likely effect of more regulation, we see that the variable that we should try to influence is the reward—the market price of the vulnerabilities and exploits being sold on the black market. This can be accomplished indirectly by establishing fair market prices in legitimate markets.

Focusing on the reward is even more important in the case of sales to grey markets. Because governments are often buyers on the grey market, enforcement in these markets is likely to be less strict, creating a more direct relationship between the likelihood of selling in the grey markets (S_G) and the possible reward (R_G).

$$S_G = f(R_G)$$

Due to the reduction in risk, the likelihood of selling in grey markets is already higher than the likelihood of selling in black markets. Meanwhile, the higher reward in grey markets compared to white markets makes grey markets more attractive to all but the most altruistic security researchers. It thus is advisable to increase the reward available in the white market (R_W).

Even if the reward in the white market is increased, the white market is currently inconsistent and unstructured. For example, many vendors do not offer bug bounties. Because of the inconsistency of vendor-focused markets, black and

604. Packer, *supra* note 580, at 553.

grey markets are often more accessible than white markets. Accordingly, a market should be designed with consistency concerns in mind in addition to rewards.

Another factor that might make white markets more appealing to security researchers is prestige. The lack of transparency in the current vulnerability market system makes it difficult for security researchers to be adequately recognized. Adding some type of recognition or prestige element (V) to the transparent white market could increase the likelihood that researchers will choose to sell in the white market. Thus:

$$S_W = f(R_W) + V$$

When organizations obtain vulnerability information and exploits with the intention of using them and not disclosing them to be fixed, every average computer network and user is left at risk. This is partially due to the nonexclusive nature of vulnerabilities. Purchasing the vulnerability does not prevent the seller from disclosing it, nor does it prevent others from discovering it. If a government purchases a vulnerability to use, one has to wonder whether someone else might have also discovered that vulnerability. And if they have discovered the vulnerability, what if they want to use it against that government's citizens? Under these facts, it would seem that disclosing and patching are more socially desirable than saving vulnerabilities for later use.

The end goal of our proposal is to make the white market more attractive to security researchers who might otherwise sell their findings on the black or grey markets. The likelihood of selling on white markets (S_W) should therefore be increased so that:

$$S_W > S_G > S_B$$

This will require several elements. The white market must be consistent between vendors, the barriers to entry for the market must not be too high, and the rewards should be high enough to sufficiently compensate security researchers for their expertise, with these prices being determined in a fair and transparent manner.

This reasoning is the foundation for our vulnerability market proposal. A uniform market to facilitate transactions with vendors would address the current inconsistencies found with bug-bounty programs. To optimize consistency, vulnerabilities should be priced based on severity tiers. The severity tiers, in turn, would be determined based on elements including: (1) the number of users affected by the security flaw; (2) the type of users affected by the security flaw—e.g., businesses, critical infrastructure, and individuals; and (3) the severity of the security flaw. The tier price would provide a starting point for negotiations between the buyer and the seller. The Common Vulnerability Scoring System

("CVSS") could be applied towards tier determinations.[605] CVSS is also currently used in the National Vulnerability Database ("NVD") maintained by the NIST.[606]

Demleitner observed that following Prohibition, many members of the American mafia invested in developing Las Vegas, using profits from illegal activity to support their entry into the legitimate marketplace.[607] Kirsch suggests providing grey hat hackers with a safe harbor under the CFAA,[608] and we echo this recommendation. If a security researcher were risking federal prosecution by introducing vulnerabilities into our proposed white market system, this would create a substantial barrier to entry. Instead, security researchers could be assured qualified immunity for transactions within the transparent marketplace. The development of this market would thus require the participation of regulators in addition to the private sector.

Criminal laws and export restrictions increase costs for buyers and sellers, but they do not affect the available rewards. Our proposal targets the reward element of vulnerability market decisions, with the ultimate goal being to improve the competitiveness of all types of rewards for vendor-oriented vulnerability transactions.

B. Vulnerability Derivatives

The exchange of vulnerabilities and exploits is at the core of our proposal. To support this exchange, we envision a financial market that exclusively focuses on computer security. At the center of this market is a clearinghouse to manage trades. The exchange and clearinghouse would operate as nonprofits dedicated to the improvement of computer security. Fees would support the operation of the market, and excess revenue would be invested into research. Our theoretical market builds on Professor Böhme's 2006 proposal for exploit derivatives.[609] Unlike Böhme's exploit derivatives market, which would focus on security events, our market would focus on tiers of security risks.

Our tiers would be based on the CVSS factors currently used in the NVD.[610] Vulnerabilities in the NVD are labeled according to whether they are low, medium, or high severity.[611] The market structure that we propose would be modeled on derivative markets, and market participants would enter into contracts based on whether they think the value of a particular vulnerability tier will go up or down. Our proposal uses the price discovery benefit of derivative markets to produce a fair market price based on the collective knowledge of all investors.

---

605. *See generally* PETER MELL ET AL., A COMPLETE GUIDE TO THE COMMON VULNERABILITY SCORING SYSTEM VERSION 2.0 (2007), https://www.first.org/cvss/v2/guide (providing information about the CVSS).

606. *CVSS v3 Information*, NAT'L VULNERABILITY DATABASE, https://nvd.nist.gov/cvss.cfm (last visited Aug. 2, 2016).

607. Demleitner, *supra* note 419, at 621.

608. Kirsch, *supra* note 5, at 400.

609. Böhme, *supra* note 234, at 3.

610. *CVSS v3 Information*, NAT'L VULNERABILITY DATABASE, https://nvd.nist.gov/cvss.cfm (last visited Aug. 2, 2016).

611. *Id.*

The first problem that must be addressed is financial. Our model views vulnerabilities and exploits as commodities, analogous to any other commodity traded in exchanges. Many commodities are low cost, like corn being traded at $4 per bushel. A single high-risk vulnerability that has been turned into an exploit, on the other hand, could potentially sell for hundreds of thousands of dollars in the current market. This may be the fair market value for these commodities, or prices might be inflated by the lack of transparency within the market. A contract for one high-risk vulnerability could potentially be enormously expensive for an investor, never mind actually buying contracts in bulk. We envision two possible solutions. One solution would involve utilizing binary options that would simply pay out based on whether a particular market condition was satisfied. However, this model may not facilitate price discovery as effectively as other models.

The second possible solution, which is the one that we would recommend, would be to base the contracts on the value of the vulnerability tier. There are two potentially effective options for this, selling contracts on margins or permitting investors to purchase micro- or nano-lots.

The first option is selling contracts on margin, which is a common market model for high value commodities. Buying on margin is like making a down payment on a mortgage. The investor puts up a percentage of the price, and the clearinghouse provides the balance as a loan to the investor. The risk for the investor, however, is considerable. Consider the following example:

Example 1

The current price for high-risk vulnerabilities is $50,000. An investor enters into a contract to purchase 10 high-risk vulnerabilities on margin at $5,000 each. The clearinghouse provides the additional $450,000 as a loan. The price for the high-risk tier increases to $60,000.

The investor sells. $450,000 goes to the clearinghouse, and the investor has a profit of $100,000.

Alternatively, the investor does not sell. The price drops to $40,000. The clearinghouse issues a "margin call" that requires the investor to pay back the loan. The investor's $50,000 investment is now gone, and he might owe the clearinghouse an additional $50,000.

As this example shows, buying on margin can either be very good or very bad for the investor. When the price goes up to $60,000, an investor who bought ten contracts and had invested the full amount would have a profit of 20%. The investor who bought on margin, on the other hand, only invested $50,000 and has earned the same profit, making this a 200% return on investment.

The situation where the price drops, in contrast, puts investors who buy on margin in a worse financial position compared to investors who pay the full amount outright. If an investor had paid the full amount and then the value dropped, his or her investment is still worth $400,000 and he or she could hold onto it and wait for the price to go back up. Meanwhile, the investor who purchased on margin has lost all of his or her investment and cannot pay back the

loan. Instead of requiring the investor to pay back more than he or she invested, the clearinghouse might instead close out the investment when the price drops to $45,000. This way, the clearinghouse can reclaim the value of the loan and the investor is just left with an empty account. Buying on margin thus increases the risk for the investor.

Our second option focuses on avoiding the risk of trading on margin. A less-risky approach could reduce barriers to entry and make it more likely that security researchers would actively participate in the market. We thus propose a different kind of contract that would be based on a fraction of the vulnerability tier's value. Each contract would concern this fractional unit. The unit would be 1/1000 of the cost of the vulnerability, and we call these vulnerability fraction units ("VFUs"). This kind of contract already exists in foreign exchange ("Forex") markets, where the standard contract size is $100,000 of the base currency. Many Forex brokers offer micro-lots at 1/100th of the base lot size and nano-lots at 1/1000th of the base lot size.[612] Our VFU model applies this structure to vulnerability trading. Consider the following example:

Example 2

An investor enters into a contract to purchase 100 high risk VFUs at $80 each on or before May 1st, 2016. The investor then enters into a separate contract to sell 100 medium risk VFUs at $40 each on or before May 1st, 2016. At the 1/1000 VFU value, this means that the investor expects that on May 1, 2016, the price of a high-risk vulnerability will be above $80,000, and the price of a medium-risk vulnerability will be below $40,000.[613]

Like the margin example, a contract for 100 VFUs requires the investor to put up 10% of the tier price. However, as discrete units, this is the full value of the investment, and the investor is not in debt to the clearinghouse. The less-risky VFU model would encourage market participation by security professionals, software vendors, and other potential vulnerability purchasers who might not be able to participate in high-stakes markets. This would improve the amount of information reflected in the market price.

These VFU contracts would subsidize qualifying vulnerability purchases by vendors. When the contract matures, contract-holding speculators will receive their profits, but not the initial value of the contract, as explained in more detail in Section IV.C. The value of any VFU contracts which are not immediately applied to sales will be stored in an escrow account and reserved for future sales and research. Once the market is established, we anticipate that the maturity dates of

612. Nick Bencino, *Lots, Leverage, and Margin*, FOREX4NOOBS (May 1, 2016), https://www.forex4noobs.com/forex-education/lots-leverage-margin/.

613. In conventional markets, the practice of agreeing to sell a commodity that you do not yet own is known as short selling. *Short Selling: A Trader's Guide*, TRADEKING: EDUC. CTR., https://www.tradeking.com/education/stocks/short-selling-explained (last visited Aug. 29, 2016).

contracts will be issued on a rolling basis with approximately two weeks between each maturity date.

Vendors and other potential purchasers could also use the market to hedge against price increases. In this case, the contract would have an option provision that would permit the contract holder to exercise the option to purchase a vulnerability at the contract price. The negotiated price would still be paid to the seller, but the buyer's account balance would reflect the discount obtained by exercising the option. If the vendor declines to purchase a particular vulnerability, it would become available to the market of investors who had option contracts for a vulnerability of that severity. In the event that more than one option holder wishes to exercise the option, an auction will decide the party permitted to exercise the option. In such a situation, the final auction price would be the amount paid to the seller, and the option holder would exercise the option and receive the difference between the strike price (as specified in the contract) and the sale price.

C. Vulnerability Sales

We now turn to the heart of our proposal: facilitating sales at a fair market price between vendors and security researchers. The derivative market this Article proposes could function independently, but we propose that the market would be most valuable as an institution that supports the actual exchange of vulnerability information between researcher and vendor. By using the collective knowledge of investors, security researchers, and vendors to establish a fair market price based on severity tiers, the market for vulnerabilities will become much more transparent. This market proposal would be most appropriate for proprietary software. Opensource software like Linux distributions may require a market that is structured differently.

The following chart depicts the complicated relationships between investors, the third-party intermediary, and the buyers and sellers of vulnerability information. The exchange attracts speculators and hedgers, who invest in either futures or option contracts, and as the maturity date approaches, they decide whether to sell or hold their VFUs. Selling transfers the VFUs to a new speculator or hedger. A hedger who holds an option contract would likely not be interested in their account being adjusted to reflect profits, because the option contract enables them to purchase at a discount. They can, however, convert the option contract to a futures contract before the maturity date if they do want to claim the profit. On the other side, a seller contacts the clearinghouse, who connects the seller with the buyer to facilitate a negotiation. A successful negotiation results in a sale, while a failed negotiation results in the vulnerability becoming available for option holders. If the vulnerability is sought by more than one option holder, an auction takes place.

Vulnerability Market Proposal

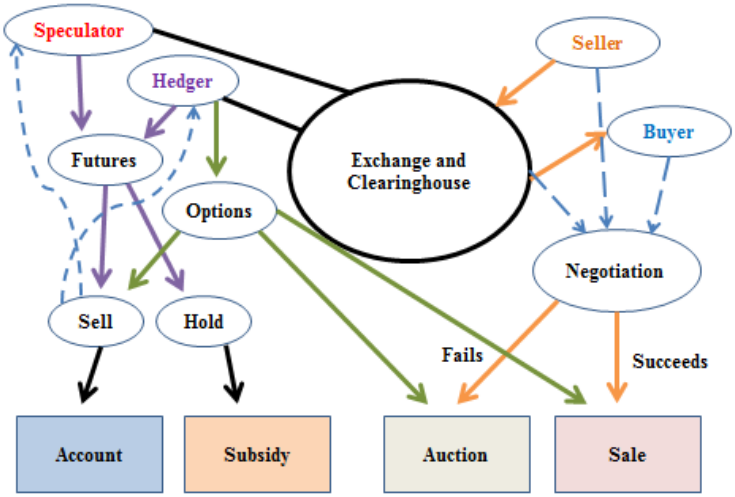

Figure 2

The clearinghouse that facilitates the trading of contracts will be instrumental for the actual purchasing activity as well. The idea of using an intermediary to facilitate vulnerability transactions is not new. US-CERT has served this role,[614] and scholars including Bambauer and Day have recommended the use of an intermediary for vulnerability transactions.[615] Our proposal builds on these precedents and ideas. The following figure provides a more detailed overview of the sale procedures.

---

614. *About Us*, U.S. COMPUTER EMERGENCY READINESS TEAM, https://www.us-cert.gov/ (last visited Aug. 2, 2016).

615. *E.g.*, Bambauer & Day, *supra* note 226, at 1056; Böhme, *supra* note 234, at 2.

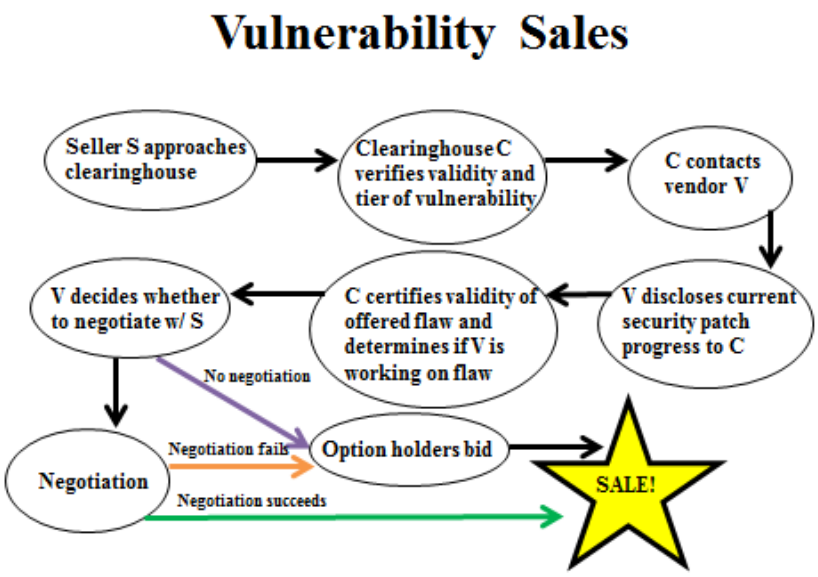

Figure 3

A number of organizational elements will improve the effectiveness of our proposal. First, the clearinghouse will employ highly skilled cybersecurity experts who can mitigate the effects of the Arrow paradox that arises when parties are transacting in information goods.[618] These intermediary experts will certify the validity and tier of an offered vulnerability, and the appropriate tier price will serve as the anchor price for the negotiations. Ideally, vendors would also provide clearinghouse experts with access to information about patches currently being developed so that the clearinghouse can certify that the offered security flaw is both valid and something that the vendor is not currently working on fixing. Second, the clearinghouse will mediate during the negotiations as necessary. Third, the vendor must have a right of first refusal. If the negotiations fail or if the vendor declines to purchase the vulnerability, the negotiation will be opened up to the larger market. Overall, the use of a trusted third party and the price discovery benefits of a derivatives market should significantly simplify the processes involved in the vulnerability trade. The right of first refusal is vital to ensure that the market caters to the public interest as much as possible by emphasizing a paradigm where vendors are the buyers, instead of encouraging vulnerabilities to simply be sold to the highest bidder.

Currently, the open market typically pays more for vulnerabilities and exploits than vendors offer through bug bounties. Many vendors may not have the resources necessary to offer market price for bugs. Futures contracts for VFUs will offset the difference between these two markets by subsidizing purchases by

618. *See* Arrow, *supra* note 433, at 615.

qualifying vendors. A qualifying vendor is the vendor responsible for the flawed code and who has committed to expedite the patching of purchased flaws.

A vendor who will not commit to expedited patching will not receive a subsidy, but they can still obtain a discount by participating in the derivatives market as a hedger. At the time of purchase, if the market price is higher than the price at which the vendor purchased an option contract, the vendor can exercise the option, paying the full price to the seller and having their account increased by the difference between the market price and the contract price. The options would still be calculated in terms of VFUs, so a vendor that wishes to use an option for the full price of a vulnerability may want to have contracts for 1,000 VFUs of that particular vulnerability tier. Because contracts can be converted between futures and options before the maturity date, this creates an incentive for vendors and other purchasers to be the final holders of contracts.

The following scenario describes how we envision the functioning of these markets:

> A few months ago, Sam the speculator held a contract for 100 high-severity VFUs at $65 each on or before May 1, 2016. He sold his contract for 100 VFUs to fellow speculator Susan at a price of $70 each, with the same maturity date. Since he bought the contract for $6,500 and sold the contract for $7,000, Sam's profit for this contract is $500. Susan retains the contract until the maturity date. On May 1st, the market price for the high risk tier is $85,000. The contract is now worth $1,500 more than what Susan paid, and $2,000 more than what Sam paid.
>
> The original value of Susan's contract, $7,000, can now be applied as a subsidy towards a qualifying vendor purchase. The clearinghouse deposits the extra $1,500 in Susan's account and issues Susan a receipt for a tax-deductible gift of $5,500—the value of her original contract minus her profit. The subsidy amount is based on the amount paid by the last purchaser. Here, the original contract is worth $7,000 instead of $6,500, because the $500 difference has already been claimed by Sam when he sold to Susan. Susan can continue to reinvest the remaining $1,500, but the exchange will not issue donation receipts for values higher than the capital actually invested.
>
> Rosa is a researcher who discovers a security flaw in an operating system distributed by the company Virtual, Inc. Rosa approaches the clearinghouse about a potential sale on April 20, 2016, and the security experts at the clearinghouse verify the validity of the vulnerability and assign a severity of High. The clearinghouse contacts Virtual about a potential sale and certifies the severity. Virtual agrees to negotiate with Rosa.
>
> Information about the subsidy is retained by the clearinghouse until the negotiations are concluded. On May 2, 2016, Virtual and Rosa agree on a sale price of $80,000. If Susan's contract is the only eligible contract for a high severity vulnerability that has matured on or before May 1st, the $7,000 will be applied towards Virtual's

purchase price, and the final cost to Virtual for this information is $73,000.

D. Implementation and Possible Counter Arguments

In this Part, we have sketched out a revolutionary proposal that has the potential to improve cybersecurity for everyone. While this proposal is fundamentally driven by the private sector, regulatory intervention will be necessary in some areas. The portion of the market dedicated to the trade of VFUs would almost certainly need to comply with CFTC regulations at a minimum. If the options element of the proposal is adopted, the SEC will likely need to be involved as well.

Another area where government intervention will be necessary concerns the current barriers to entry for this type of market. Because unauthorized security research is likely to violate the CFAA, we propose that the CFAA be amended to create a narrow safe harbor for cybersecurity research where the fruits of that research are offered to vendors through our transparent marketplace or a similar vehicle. These amendments to the CFAA could also include other liability limitations, restricting the extent to which a vendor could bring legal action against a good-faith security researcher.

The current vulnerability market is complicated by the recently enacted federal CISA. CISA is designed to facilitate the sharing of cyber threat indicators between the private sector and the government. If a vendor discloses information to the government about a vulnerability discovered by a freelance security researcher, the current wording of CISA is broad enough to permit the government to undertake an investigation of the security researcher, and potentially compel them to disclose the information for free. The vendor would thus be able to evade potential negotiations and obtain the information at no cost. By providing a transparent and legally recognized marketplace, our model could help avoid this outcome.

The transparency of the market may ultimately need to be a sliding scale. More sensitive systems, like programmable logic controllers used for industrial computers, may require greater delicacy than a consumer product. While harder to infect, industrial control systems are still vulnerable to human error if, for example, an employee puts an infected USB drive into one of the computers that would otherwise be "air gapped."

There are possible pitfalls to this proposal. Law enforcement and intelligence agencies around the world would likely protest the loss of grey markets. Unfixed vulnerabilities can help solve crimes by enabling law enforcement to hack into a suspect's computer, or even protect national security interests by making it easier to spy on terrorist organizations. We argue that these interests are important, but they do not outweigh the greater public interest in fixing security flaws instead of exploiting them.

Three other possible problems concern the derivative market side of our proposal. The first problem likely to be raised concerns the risk that investors might manipulate the market. For example, a software developer who invests in the market might insert backdoors intentionally that could be reported as critical

security flaws. But this concern is overstated, because that is already a hazard with the current market. This possible hazard is also why we have proposed a market organization scheme based on severity tier instead of the occurrence of specific events or the value of vulnerabilities associated with a particular vendor.

A second danger is the risk that over-speculation could lead to artificially high or low prices not justified by market realities. To address this possible risk, the derivative market should have guidelines for the acceptable ratios of speculators to potential buyers.

The third danger involves the potential for ill-intentioned third parties to obtain vulnerabilities during the options and auction phases. One possible way to address this downside is to eliminate third-party purchases. In this scenario, if negotiations between the researcher and vendor fail, the clearinghouse obtains the vulnerability and compensates the researcher with VFUs that they can trade in the market. This option would emphasize the clearinghouse's third purpose as a security-research organization.

As with any market, a successful vulnerability clearinghouse will need sufficient liquidity. It may be difficult to persuade initial investors, but one group in particular may be especially interested in a vulnerability research market: cyber insurance providers. Many standard insurance contracts are not broad enough to cover cyber risks, and customers are increasingly interested in cyber insurance policies. Unfortunately, the insurance industry is plagued by uncertainty because of the lack of actuarial data for cybersecurity risk management. An investment-based vulnerability market could enable insurers to hedge against some of the uncertainties of creating a market for cyber insurance. Ultimately, we are optimistic that our proposal could succeed, going a long way towards fixing the information security problems that plague modern society.

CONCLUSION

Information drives modern society, and nowhere is this clearer than cybersecurity, where information is the weapon, the shield, and the currency. Vulnerability markets allow the trading of information for personal gain, sometimes to the detriment of the public welfare.

When combating cyber threats, the regulatory response tends to emphasize punishment and detection. In this Article, we instead focus on rewards. If there are no carrots to improve the incentive to report flaws to vendors, the regulatory sticks of criminal enforcement will drive the prices up in questionable markets without actually improving security in the long run. We propose a model that we believe will create new incentives to sell vulnerabilities to vendors instead of to potentially malicious third parties.

One of our main goals is to create an efficient marketplace. Vulnerabilities and exploits are information goods vulnerable to the Arrow paradox. Too much disclosure destroys their value. They also can never be completely exclusive to any one buyer or seller, because vulnerability information is discovered, not created. Vulnerability information is currently traded secretively with an unknown end game. Security researchers attempting to sell their

discoveries may have prolonged periods of negotiation with a potential buyer, during which time the flaw might be discovered and patched.

Our proposal addresses these shortcomings by providing a largely self-funding nonprofit model that utilizes the price discovery benefits of derivative markets to establish a base fair market value for low-, medium-, and high-severity vulnerabilities, while also providing expert third-party intermediaries to certify vulnerabilities and facilitate transactions between vendors and security researchers.

Cyber threats could potentially affect every aspect of our daily lives. Governments are responding to these threats by debating disclosure requirements and export permits, but something more is needed. Government agencies around the world are stockpiling zero-day vulnerability information against the best interests of their constituencies. Regardless of their country of citizenship, people should demand more security, not clever ways of using computer insecurity against other countries. This is the new battlefield, and everyone is potentially collateral damage.