2022

Book Review: This Is How They Tell Me the World Ends: The Cyberweapons Arms Race (2020) by Nicole Perlroth

Amy Gaudion
Penn State Dickinson Law, acg14@psu.edu

Book Reviews

DRAFT
Forthcoming in the *Dickinson Law Review* Volume 126 Issue 2 to be published early 2022. Please use the following citation until the review is published: Amy C. Gaudion, *Book Review: This Is How They Tell Me the World Ends: The Cyberweapons Arms Race (2020) by Nicole Perlroth*, 126 DICK. L. REV. (forthcoming 2022).

Book Review: This Is How They Tell Me the World Ends: The Cyberweapons Arms Race (2020) by Nicole Perlroth

Amy C. Gaudion*

In May of 2017, the WannaCry attack, later attributed to North Korea and Russia respectively, resulted in the loss of billions of dollars for governments and private companies across the globe. Only one month later, the NotPetya attack, later attributed to Russia, wreaked additional and more devastating havoc, again on a global scale. Both attacks exploited a vulnerability found in the Microsoft Windows operating system. The U.S. government had discovered that same vulnerability several years earlier. However, rather than notifying Microsoft of the vulnerability so that it could be patched, the U.S. government decided to keep the discovery of the vulnerability a secret, and to retain it for intelligence collection and national security purposes.[1]

* Associate Dean for Academic Affairs and Professor of Lawyering Skills, Penn State Dickinson Law.

1. Lily Hay Newman, *The Leaked NSA Spy Tool That Hacked the World*, WIRED (Mar. 7, 2018, 8:00 AM), https://bit.ly/3GkveVi [https://perma.cc/G2KU-3ZPQ]. After discovering the vulnerability, the National Security Agency developed a set of hacking tools called Eternal Blue designed to exploit the software

In October of 2021, the media reported that the FBI "refrained for almost three weeks from helping to unlock the computers of hundreds of businesses and institutions" impacted by the July 2021 ransomware attack conducted by REvil, a Russia-based criminal gang, even though the FBI had acquired the digital key needed to do so.[2] The FBI decided against sharing the key with the companies affected, so that it could be utilized as part of an on-going operation to investigate and take down REvil's criminal network.[3]

These incidents highlight the trade-offs implicated in the U.S. government's use of cyber tools and capabilities, and especially its purchasing, use, and stockpiling of zero-day vulnerabilities. At the general level, a vulnerability is a "weakness in an information system or its components (e.g., system security procedures, hardware design, internal controls) that could be exploited or impact confidentiality, integrity, or availability of information,"[4] and a zero-day vulnerability is "a software or hardware flaw for which there is no existing patch."[5] A small group of legal and information security scholars and commentators have examined this subject, carefully recording the competing interests at stake, the governing legal and policy frameworks, and the consequences both anticipated and

vulnerability for intelligence collection and defense purposes. The hacking tools were later leaked by a group known as Shadow Brokers, and led to the development of WannaCry, NotPetya, and other malware. While the NSA has not officially acknowledged its role or use of Eternal Blue, other reports and Microsoft have corroborated its NSA origins. For a detailed history of this episode, see NICOLE PERLROTH, THIS IS HOW THEY TELL ME THE WORLD ENDS: THE CYBER WEAPONS ARMS RACE 308–09, 340–41, 347–49 (2020); see also ANDY GREENBERG, SANDWORM: A NEW ERA IN CYBERWAR AND THE HUNT FOR THE KREMLIN'S MOST DANGEROUS HACKERS 164–65, 182–83 (2020); BEN BUCHANAN, THE HACKER AND THE STATE: CYBER ATTACKS AND THE NEW NORMAL OF GEOPOLITICS 253–54 (2020). No U.S. law prohibited this decision. Rather, in assessing whether to disclose or to retain a vulnerability, the U.S. government follows an internal executive branch policy called the Vulnerabilities Equities Process (VEP). The VEP is an interagency mechanism that seeks to balance

> whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched, or to temporarily restrict the knowledge of the vulnerability to the USG, and potentially other partners, so that it can be used for national security and law enforcement purposes, such as intelligence collection, military operations, and/or counterintelligence.

THE VULNERABILITIES EQUITES POLICY AND PROCESS FOR THE U.S. GOVERNMENT 1 (2017), https://bit.ly/3x7OxDC [https://perma.cc/8JC8-W4SC] [hereinafter VEP].

2. Ellen Nakashima & Rachel Lerman, *FBI Held Back Ransomware Decryption Key from Businesses to Run Operation Targeting Hackers*, WASH. POST (Sept. 21, 2021), https://wapo.st/3BAfYqy.

3. *Id.*

4. This is the definition included in the VEP, *supra* note 1, at 12.

5. PERLROTH, *supra* note 1, at 7.

unintended.[6] In many ways, however, the U.S. government's engagement in the vulnerability market has remained a practice in the shadows, and its impacts are understood by few people inside or outside the U.S. government. In *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*, published at the end of 2020, author Nicole Perlroth attempts to bring this practice out of the shadows.

In the book, Perlroth traces the development and use of cyber capabilities, focusing on the U.S. government's unintended role in creating a market for these cyber goods. Her purpose is a straightforward one: to illuminate. Perlroth explains that her goal is to "help shine even a glimmer of light on the highly secretive and largely invisible cyberweapons industry so that we, a society on the cusp of this digital tsunami called the Internet of Things, may have some of the necessary conversations now, before it is too late."[7] She seeks to accomplish this purpose by offering a treatise-like treatment of the subject, defining terms, tracking the historical development of governmental cyber capabilities and the parallel growth of a vulnerability broker industry, identifying key players and entities in the market, and profiling a slew of cyber operations and events. Despite the length and breadth of the book, her thesis is precise and blunt: the U.S. government's practice of purchasing vulnerabilities for use in law enforcement, intelligence collection, and military operations led to a black market for these tools and an arms race between governments and an array of questionably-motivated private actors. She argues that the U.S. government's myopic focus on the offensive use of these cyber tools, and its corresponding failure to anticipate or consider the consequences of that offensive focus, led to unexpected and negative results for the United States and the world.

6. *See, e.g.*, Tristian Caulfield et al., *The U.S. Vulnerabilities Equities Process: An Economic Perspective*, UCL DISCOVERY, https://bit.ly/3oSaNO2 [https://perma.cc/YX7X-VV99] (last visited Nov. 21, 2021); Sharon Bradford Franklin, *The Need for Countries to Establish Robust and Transparent Vulnerabilities Equities Processes*, 6 FLETCHER SEC. REV. 46, 46–47 (2019); SVEN HERPIG, GOVERNMENTAL VULNERABILITY ASSESSMENT AND MANAGEMENT: WEIGHING TEMPORARY RETENTION VERSUS IMMEDIATE DISCLOSURE OF 0-DAY VULNERABILITIES (2018), https://bit.ly/3x9DIRC [https://perma.cc/CTK2-ASBF]; Stephanie Pell *The Ethical Imperative for a Vulnerability Equities Process and How the Common Vulnerability Scoring System Can Aid that Process*, 48 CONN. L. REV. 1549–90, (2017); Ari Schwartz & Rob Knake, *Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process* (Harv. Kennedy Sch. Belfer Ctr., Discussion Paper 2016-04, 2016).

7. PERLROTH, *supra* note 1, at xiv.

The book unabashedly is written for the layperson. As Perlroth notes in the first chapter, "Not only did I not know anything about cybersecurity, I had actively gone out of my way to not know anything about cybersecurity."[8] Her realization, of course, is that she should know—and that we all need to know more about cybersecurity. This is a book designed for that task, to raise awareness among the non-cyber crowd of a phenomenon that has occurred mostly out of public view.[9] She identifies this phenomenon as the acceleration in use and increase in potency of government hacking tools. Other authors also have lamented the public's ability to appreciate or grasp how this phenomenon impacts day-to-day life. Ben Buchanan writes that although,

> everyone on the internet is caught in the crossfire . . . this struggle does not manifest itself in public debates at the United Nations or even the discreet summits of international leaders. It does not rely on conspicuous military mobilizations or troops that serve as human trip wires. Instead, it flows through vast server farms, ad hoc networks of unwitting participants, third-party states, and homes and workplaces nearly everywhere.[10]

Perlroth's aim is to illuminate for the general public this phenomenon, to identify its participants, and to draw the contours of the battlefield in which it is taking place. As such, the book provides an imminently satisfying and fast read, almost achieving the page-turner status of fictional political thrillers. If you are listening to it as an audio book, you will want simultaneously to increase the speed to 1.5 to see what happens next, and then slow the speed to 0.5 to ensure you do not miss an important detail. Many of the events and actors will be familiar to those in the national security and cyber fields, but the author weaves the threads together in a way that even an individual steeped in the subject will learn something new and will appreciate the temporal and substantive connections she delivers.

The book's structure operates on several levels. The first level divides the book by the type of cyber actor, as Perlroth profiles government entities of both intelligence and military varieties, private companies engaged in both the development and use of cyber tools and in providing cybersecurity (or defensive) services,

8. *Id.* at 3.

9. *Id.* at xvii ("But had we all been paying closer attention, we might have seen the blaring red warning lights, the compromised servers in Singapore and Holland, the blackouts, the code spiking out in all directions. We might have seen the end game wasn't Ukraine. It was us.").

10. BUCHANAN, *supra* note 1, at 9.

hackers of all stripes from across the black, grey, and white hat worlds, and vulnerability brokers. Within each part, she offers three or four chapters, which are generally organized by cyber event, operation, or tool. The double-layered structure takes the reader skipping across decades as Perlroth chronicles real world case studies and offers in-depth profiles of the key players, both individuals and organizations, in the cyberweapon marketplace. What makes the book such a compelling read, however, is the author's ability to draw the reader in through the use of personal vignettes in which Perlroth is a character in the action as it unfolds, anticipating the reader's questions.

Before turning to an evaluation of the book's contributions and weaknesses, it is helpful to consider where this work sits among others. Perlroth joins an ambitious group of journalists, scholars, and former government officials who have attempted to outline the contours of the shadowy world of vulnerability brokers and the growth of the zero-day vulnerability market. These include, most notably Ben Buchanan's *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (2020) and Andy Greenberg's *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (2019), as well as incisive reporting efforts by Chris Bing and Ellen Nakashima.[11] The book also complements those that have explored the U.S. government's efforts to develop and use cyber weapons, including David Sanger's *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (2018), and Kim Zetter's *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (2014).

Perlroth's contributions with this work are the most significant in four areas: (1) describing the current state of affairs in the cyberweapons marketplace; (2) providing comprehensive descriptions of instances where the state actors (or state-sponsored actors) have deployed their cyber capabilities; (3)

11. *See, e.g.*, Joseph Menn & Chris Bing, *Governments Turn Tables on Ransomware Gang REvil by Pushing It Offline*, REUTERS (Oct. 21, 2021, 6:45 PM), https://reut.rs/3GDzLZX [https://perma.cc/WWY8-4LBY]; Chris Bing, *U.S. Moves to Control Sales of Hacking Tools Abroad*, REUTERS (Oct. 20, 2021, 1:11 PM), https://reut.rs/3mBdOCC [https://perma.cc/5NW7-E4J3]; Chris Bing & Joel Schectman, *Inside the UAE's Secret Hacking Team of American Mercenaries*, REUTERS (Jan. 30, 2019), https://reut.rs/3EH5mrT [https://perma.cc/SC3W-T5LV]; Ellen Nakashima & Craig Timberg, *NSA Officials Worried About the Day Its Potent Hacking Tool Would Get Loose. Then it Did*, WASH. POST (May 16, 2017), https://wapo.st/3BClhFV [https://perma.cc/6DUW-9RQQ]; Ellen Nakashima, *The Cybersecurity 202: Here's Why NSA Rushed to Expose a Dangerous Computer Bug*, WASH. POST (Feb. 6, 2020, 7:55AM), https://wapo.st/2Zl3ekP [https://perma.cc/M4LR-G5TJ].

exploring how the U.S. government's actions in cyberspace may have contributed to the current cyberweapons marketplace; and (4) supplying a well-researched, and helpfully indexed, primer for the cyber layperson.

The book's first contribution is its gripping and thorough account of the cyberweapons industry and in particular the zero-day vulnerabilities market. The author describes its origins, its pricing structure, its codes of professional conduct and deal-making norms, its sellers, its buyers, and the cybersecurity firms and researchers that attempt to study it. For example, she explains how the price of a vulnerability went from $400 in the early days of the market to $4,000 only 3 years later to around $50,000 5 years on.[12] She also explains the practice of stockpiling vulnerabilities, and unearths the U.S. government's practice of doing so. While other scholars and journalists have profiled this market,[13] Perlroth brings it into sharp focus through her personal encounters with many of the central figures in the market. These include deep character sketches, most notably of John P. Watters,[14] Alfredo Ortgega,[15] Adriel Desautels,[16] Dave Aitel,[17] Chaouki Bekrar,[18] and John Hultquist.[19] Recognizing the ambitiousness of the task before her, Perlroth writes that "getting to the bottom of the zero-day market was a fool's errand."[20] While she might not make it to the bottom, she takes the reader on a rollicking ride well-beneath the surface.

The book's second contribution is its comprehensive descriptions of instances where state actors (or state-sponsored actors) have deployed their cyber capabilities, with a particular

12. PERLROTH, *supra* note 1, at 39–40. The owner of iDefense told the author that "the first thousand bugs iDefense paid $200,000 for in the first [18] months of the program would have cost $10 million today." *Id.* at 40.

13. *See* SVEN HRAPIG ET AL., MARKETS FOR CYBERCRIME TOOLS & STOLEN DATA (2014), https://bit.ly/3BAAw1W [https://perma.cc/T8BW-4NT2].

14. PERLROTH, *supra* note 1, at 22–35, 289–90. Watters is the owner of iDefense, an early corporate player in the cybersecurity field, and one of the first companies to hire hackers and "start paying bounties for zero-day bugs." *Id.* at 29.

15. *Id.* at 259–62. Alfredo Ortgega is an Argentinian hacker known to many as the Cyber Gaucho.

16. *Id.* at 165–75. The author describes Adriel Desautels as "a cyberweapon merchant who looked like a milkman," and someone who brought a moral compass sniff test to his work. *Id.* at 165.

17. *Id.* at 259–62. Dave Aitel is a former NSA hacker, arguably disgruntled, who went on to author *The Shellcoder's Handbook: Discovering and Exploiting Security Holes* and to establish Immunity Inc.

18. *Id.* at 218–19. Chaouki Bekrar is known as the "Wolf of Wuln Street."

19. *Id.* at 290–93. Hultquist is a former army reservist and one of the key cybersecurity researchers tracking the origins of the BlackEnergy malware.

20. *Id.* at 21

focus on U.S. cyber operations. The book provides rich descriptions of each operation's origin and development, its intended purpose, and its actual (occasionally unintended) impact and effect. For example, the author guides the reader through China's cyber operations against Google (2009–2010) [labeled "Aurora" by cybersecurity researchers] and the U.S. Office of Personnel Management (2014); Iran's cyber activities against Aramco, the Sands Casino, and the U.S. banking industry; Russia's efforts with NotPetya (2017), Black Energy/Sandworm and, of course, the 2016 hack of the DNC servers; and North Korea's cyber operation against Sony Pictures and its development of the WannaCry ransomware attack. She offers a deeper dive on the U.S. government's cyber activities, focusing particular attention on Olympic Games, an operation that utilized the Stuxnet worm to slow Iranian nuclear capabilities, and the Eternal Blue tool/exploit.

The third contribution this book makes to the field is its effort to draw a causal connection between the U.S. government's actions and the frenzied and precipitous state of the cyberweapons marketplace. According to Perlroth, the U.S. government's decision to focus on the offensive side of the cyber house, while ignoring the defensive effort, led to two types of problems. First, the United States slipped from being a state with dominating cyber powers to only one player among many with comparable capabilities. This hubris is reflected best in the Nobody But Us or "NOBUS" framework:

> The premise behind NOBUS was that low-hanging fruit—vulnerabilities that could easily be discovered and abused by American adversaries—should be fixed and turned over to vendors for patching. But more advanced exploitation— the kind of advanced zero-days the agency believed only it had the powers, resources and skills to exploit—would remain in the agency's stockpile and be used to spy on American enemies or degrade their systems in the case of cyberwar.[21]

Second, she argues that the myopic focus on developing offensive cyber tools caused the U.S. government to fail to see the asymmetry challenge coming around the bend.[22] While not agreeing with the cause, others have described the asymmetry problem as well. In a 2018 article, Jack Goldsmith & Stuart Russell explained how the strengths of American society—including commitments to free speech, privacy, and the rule of law, innovative

21. *Id.* at 136–37.
22. Perlroth, *supra* note 1, at xxv.

technology firms, relatively unregulated markets, digital sophistication—would "create asymmetrical vulnerabilities in the digital age that foreign adversaries" could increasingly exploit.[23] Perlroth's contribution is to connect the timing dots for this causal link. For example, she walks in painstaking detail through the NSA's acquisition (or purchase) of the EternalBlue exploit, its development into a tool, the government's decision to use it for seven years for intelligence collection and other national security purposes (rather than disclosing it to Microsoft), its eventual disclosure to the vulnerability marketplace by the ShadowBrokers dump, and then its adapted revision by North Korea and Russia in the WannaCry and NotPetya operations, respectively.[24] Through this and other examples, she illustrates that the U.S. government's failure to disclose certain vulnerabilities created a "boomerang effect" whereby cyber tools utilized by the U.S. government agencies for intelligence collection, law enforcement, or national security purposes, often came back to wallop U.S. companies and individuals, and even other agencies within the U.S. government agencies.

The fourth contribution Perlroth makes is her service as a lantern-holding guide through a treatise-like and comprehensive primer for the cyber layperson. The author decodes technologically challenging concepts and material, bringing her journalist toolkit to the task of making the topic accessible. She humbly places herself in the book in the role of the confused novice trying to understand the topic and the landscape. This device works quite effectively as she navigates the reader through major cyber events, while offering profiles of the entities responsible for those events. She covers the well-known operations and players, while also covering several lesser-known but equally important ones. By the end of the book, the reader has a solid understanding of the characteristics that define the Russian hacking groups[25] (including the Internet Research Agency, Cozy Bear, Energetic Bear, and Fancy Bear),

23. JACK GOLDSMITH & STUART RUSSELL, STRENGTHS BECOME VULNERABILITIES: HOW A DIGITAL WORLD DISADVANTAGES THE UNITED STATES IN ITS INTERNATIONAL RELATIONS 1–17 (2018), https://hvr.co/3jWyZxr [https://perma.cc/9WU9-CU6V] ("These asymmetrical vulnerabilities, in turn, might explain why the United States so often appears to be on the losing end of recent cyber operations and why US attempts to develop and implement policies to enhance defense, resiliency, response, or deterrence in the cyber realm have been ineffective.").

24. PERLROTH, *supra* note 1, at 308–09, 347–49.

25. *Id.* at 292, 306, 310–11, 312, 361–62.

the ShadowBrokers,[26] the NSO Group,[27] as well as the Chinese[28] and North Korean[29] cyber units. Her book is thoroughly researched drawing from a number of empirical data sets as well as sources including hackers, vulnerability brokers, cybersecurity researchers, journalists, employees of social media and technology companies, and current and former government officials. Indeed, the word "They" in the title references this host of sources. Adhering to her role as a guide, and her stated intention to "help shine even a glimmer of light on the highly secretive and largely invisible cyberweapons industry,"[30] Perlroth is candid in pointing out what she doesn't know.

While the book is an excellent contribution to this field and fulfils its goal of raising awareness among the non-cyber crowd, it suffers from weaknesses in three general areas: (1) it gives too little attention to the debates within the U.S. government regarding the use of cyber capabilities; (2) it fails to effectively incorporate the legal and policy authorities that shape and constrain the U.S. government's actions in the cyberspace; and (3) it overstates the danger in certain areas ("the world ends") at the expense of recognizing the more likely low-grade and pressing threats.

First, the book fails to discuss the complexity, nuance, and evolution of the U.S. government's cyber strategy and approach to the cyber domain. Perlroth creates the impression that the U.S. government, from the Bush to Obama to Trump administrations, unabashedly endorsed an aggressive posture in cyberspace, focused only on the offensive side of the equation. In practice, however, there were continuous, robust, and difficult debates—within each of the administrations—on how to strike the appropriate balance between the use of cyber tools for offensive purposes and the need to adequately engage in cyber defense of both government and private sector networks. The contours of these debates can be found in Richard Clarke and Robert Knake's book *Fifth Domain*,[31] and in a series of competing articles between Jason Healey and Dmitri Alperovitch.[32] For example, the Bush

26. *Id.* at 320–32.
27. *Id.* at 177–85.
28. *Id.* at 200–01, 205–09.
29. *Id.* at 333–37.
30. *Id.* at xiv.
31. *See generally* RICHARD CLARKE & ROBERT KNAKE, THE FIFTH DOMAIN: DEFENDING OUR COUNTRY, OUR COMPANIES, AND OURSELVES IN THE AGE OF CYBER THREATS (2019).
32. *See, e.g.*, *Great Power Cyber Party*, WAR ON THE ROCKS (Apr. 19, 2021), https://bit.ly/3ECqeQY [https://perma.cc/8Q2Y-764L] (containing the conversation

administration did not easily come to the decision to approve the use of the Stuxnet virus in the Olympic Games operation.[33] A second example can be found in the policy directives that outline the executive branch's approval process for military cyber operations. The Obama administration was often criticized for making the inter-agency process for the approval of military cyber operations too cumbersome and time-consuming, one which left U.S. Cyber Command looking feeble. Presidential Policy Directive 20 (PPD-20)[34] was an 18-page classified directive that laid out an extensive interagency process for the approval of military cyber operations, and required presidential approval for offensive and defensive cyber operations with effects outside U.S. government networks. In August of 2018, the Trump Administration significantly revamped the Obama-era approval process for high-level cyber operations, describing it as an "offensive step forward."[35] A third example of the complexity and nuance of the U.S. government's approach can be found in the development and eventual publication in 2017 of Vulnerabilities Equities Policy Process (VEP).[36] The VEP guides the decision-making process when the U.S. government discovers exploitable weaknesses, or vulnerabilities, in information systems. It is the process by which the government decides whether to disclose the security flaws it discovers or to keep the

between Healey and Alperovitch); Dmitri Alperovitch & Ian Ward, *How Should the U.S. Respond to the SolarWinds and Microsoft Exchange Hacks?*, LAWFARE (Mar. 12, 2021, 10:59 AM), https://bit.ly/3btly3n [https://perma.cc/L4QD-DPVQ]*; Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience: Hearing Before the H. Comm. on Homeland Sec.*, 117th Cong. (2021) (statement of Dmitri Alperovitch, Exec. Chairman, Silverado Pol'y Accelerator); Jason Healey & Robert Jervis, *The Escalation Inversion and Other Oddities of Situational Cyber Stability*, 3 TEX. NAT'L SEC. REV. 30 (2020).

33. *See* DAVID SANGER, CONFRONT & CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER 188–225 (2012).

34. Dustin Volz, *Trump, Seeking to Relax Roles on U.S. Cyberattacks, Reverses Obama Directive*, WALL ST. J., https://on.wsj.com/2Y6uKaN [https://perma.cc/J8H9-GQFV] (Aug. 15, 2018, 11:36 PM).

35. *Id.* Although National Security Presidential Memorandum 13 (NSPM 13) remains classified, media reporting indicates that it accomplished three significant changes. First, it loosened the interagency approval process. Second, it shortened the approval timeline to allow for more responsive actions. Third, it removed the presidential approval requirement for cyber operations that fell below the use of force (or similar) thresholds, and delegated that decision-making authority to others within the chain of command. *See* Robert Chesney, *The Pentagon's General Counsel on the Law of Military Operations in Cyberspace*, LAWFARE (Mar. 9, 2020, 12:33 PM), https://bit.ly/3mA9ROL [https://perma.cc/P4VP-5RCM]; Ellen Nakashima, *White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries*, WASH. POST (Sept. 20, 2018), https://wapo.st/3Bw14RT [https://perma.cc/GC2E-JVLJ]; Volz, *supra* note 34.

36. PERLROTH, *supra* note 1, at 401–03 (describing the VEP, *supra* note 1).

flaws secret for national security, intelligence, or law enforcement purposes. According to the charter, the VEP provides an interagency mechanism that seeks to balance

> whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched, or to temporarily restrict the knowledge of the vulnerability to the USG, and potentially other partners, so that it can be used for national security and law enforcement purposes, such as intelligence collection, military operations, and/or counterintelligence.[37]

The VEP was initiated in the Bush Administration, tacitly acknowledged in the Obama administration, and formally published (at least in part) in the Trump Administration. Perlroth's portrayal of Michael Daniel[38] comes closest to recognizing the complexity and nuance of the U.S. government's attempts to balance the offensive and defensive considerations. Daniel was serving as the cybersecurity czar in the Obama administration when Perlroth met with him in 2015. His haggard appearance and tired but earnest responses to her questions reveal the difficulty of the debates, and his own concerns about whether the government was striking the balance appropriately. Daniel is one of the few government officials that Perlroth identifies as having concerns; however, he was not alone.[39] By giving less attention to the voices that counseled against an overly offensive approach, she creates the impression that the U.S. government has been particularly careless, bordering on reckless. The book fails to appreciate that many officials in the U.S. government were calling for a more defensive posture, and for recognition of the reciprocity (what Perlroth refers to as the "boomerang effect") problem.

The book's second oversight is its failure to adequately discuss the existing legal and policy frameworks governing the U.S. government's development and use of cyber capabilities. One may come away from the book with the impression that this is a lawless domain. While there are certainly debates as to which laws apply and in what way, there are indeed laws, both domestic and international, that govern state conduct in cyberspace.[40] In addition,

37. VEP, *supra* note 1, at 1.

38. PERLROTH, *supra* note 1, at 302–09.

39. *See generally* CLARKE & KNAKE, *supra* note 31; BUCHANAN, *supra* note 1.

40. A sample of relevant U.S. legal authorities include: War Powers Resolution, 50 U.S.C. §§ 1541–1550; the covert action reporting requirements, 50 U.S.C. § 3093; the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1885; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. For example, 10 U.S.C.

the book gives only scant attention to the slew of executive branch strategy and policy documents, published in 2018, which reflected a shift from a deterrence-based strategy in cyberspace to a "defend forward" concept, and the embrace of a more aggressive posture in the cyber domain.[41] The DoD Cyber Strategy provided: "We will

Section 394(a), initially enacted in 2015 and amended in 2018 by the National Defense Authorization Act for Fiscal Year 2019, provides general authorization for military cyber operations. Specifically, it authorizes the Secretary of Defense to prepare for, and when appropriately authorized, to conduct "military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the United States and its allies, including in response to malicious cyber activity carried out against the United States or a United States person by a foreign power." 10 U.S.C. § 394(a). Section 394(b), which was added in 2018 as part of the National Defense Authorization Act for Fiscal Year 2019, affirmed an expansive reading of these authorities, providing the U.S. military was authorized to conduct cyber activities or operations "short of hostilities" and to conduct such operations outside areas of active hostilities. 10 U.S.C. § 394(c). In addition, and most notably, the National Defense Authorization Act for Fiscal Year 2019 included specific pre-authorization for U.S. military cyber and information operations in response to certain types of cyber actions by certain state actors. Section 1642, included in the notes to 10 U.S.C. § 394, is labeled "Active Defense Against the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, and Islamic Republic of Iran Attacks in Cyberspace." The provision authorizes the Secretary of Defense, acting through U.S. Cyber Command, to take "appropriate and proportional action in foreign cyberspace" against Russia, China, North Korea, or Iran if the National Command Authority determines that one of those states "is conducting an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace." According to reports, U.S. Cyber Command has not been hesitant in deploying its capabilities pursuant to this authority. Mark Pomerleau, *New Authorities Mean Lots of New Missions at Cyber Command*, FIFTH DOMAIN (May 8, 2019), https://bit.ly/3EDHyEG [https://perma.cc/34B2-QDMY].

A sample of relevant international legal authorities and other sources of guidance include: U.N. Charter art. 2, ¶ 4 (prohibition on the use of force); *id.* (sovereignty); *id.* ¶¶ 4, 7 (prohibition on intervention); DEP'T OF DEF., LAW OF WAR MANUAL § 16.2.1. (2016); TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (2d ed. 2017); Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report, U.N. Doc. A/AC.290/2021/CRP.2 (2021); Paul C. Ney, Jr, General Counsel, Dep't of Def., Remarks at the U.S. Cyber Command Legal Conference (Mar. 2, 2020); Brian J. Egan, International Law and Stability in Cyberspace, Remarks at Berkeley Law School (Nov. 10, 2016); Harold H. Koh, Legal Advisor, U.S. Dep't of State, International Law in Cyberspace, Remarks at USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012).

41. In April of 2018, the executive branch published the Command Vision for U.S. Cyber Command, U.S. CYBER COMMAND, ACHIEVE AND MAINTAIN CYBERSPACE SUPERIORITY: COMMAND VISION FOR US CYBER COMMAND (2018), https://bit.ly/3w7YcKb [https://perma.cc/F7NK-P7FX], followed in September of 2018 by the Department of Defense Cyber Strategy, DEP'T OF DEF., CYBER STRATEGY 2018 (2018), https://bit.ly/2Y9olvu [https://perma.cc/T46K-K9RJ] (the unclassified summary) and the White House National Cyber Strategy, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA (2018) https://bit.ly/3kXlqho [https://perma.cc/HA4U-NBNS].

defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[42] In a more recent articulation of the defend forward concept, General Paul M. Nakasone described it as an approach that acknowledges "that defending the United States in cyberspace requires executing operations outside the U.S. military's networks and that the country cannot afford to wait for attacks to come its way."[43]

The failure to incorporate the legal and policy frameworks into the book's thesis contributed to a related oversight: the failure to distinguish between cyber activities conducted for different purposes and by different U.S. governmental entities. For example, the balance between offensive and defensive resources may be struck differently when the cyber tool is used for law enforcement purposes (by entities like the FBI or local entities), for intelligence collection (by agencies like the CIA or NSA), for covert cyber operations (conducted by the CIA), or for clandestine cyber operations (conducted by the U.S. military, usually U.S. Cyber Command). While it would be beyond the book's scope (and more appropriately suited to a law review article) to offer an in-depth analysis of these authorities, it would be helpful for the reader to appreciate that the legal and policy authorities exist, and that the constraints on government action will differ dependent on the cyber tool's purpose and the cyber actor.

Reviewers within the cybersecurity community have noted factual errors in the book, leading to inaccurate timelines, misunderstanding as to the technical capabilities of foreign adversaries, and overstatements as to the threat posed.[44] While I leave the technical critique to those more familiar and appropriately trained, I agree that the author overstates the danger in certain areas at the expense of recognizing the more likely and pressing threats presented by the rapid and often un-watched development of cyber capabilities. Although minor, this is the book's third

42. DEP'T OF DEF., CYBER STRATEGY 2018 (2018), https://bit.ly/2Y9olvu [https://perma.cc/T46K-K9RJ].

43. Paul M. Nakasone & Michael Sulmeyer, *How to Compete in Cyberspace: Cyber Command's New Approach*, FOREIGN AFFS. (Aug. 25, 2020), https://fam.ag/3xhZtPm [https://perma.cc/X74F-CBBM].

44. *Book Review: This Is How They Tell Me the World Ends by Nicole Perlroth*, DALE PETERSON (Apr. 13, 2021), https://bit.ly/3pSb1XQ [https://perma.cc/B7KA-QN6T] (criticizing Perlroth for overstating Wolf Creek and Dam examples); Edward M. Roche, *This Is How They Tell Me the World Ends: The Cyber-Weapons Arms Race*, 14 J. STRATEGIC SEC. 133, 134 (2020) ("[I]t will give a distorted and incomplete picture of the cyber arms race to many readers.").

weakness. An example of this is found in the book's title, which indicates the world may end tomorrow. On closer read, however, it overstates the problem, which is a significant one but not likely leading to the end of the world. In this sense, the author fails at times to give a wholistic treatment to the tradeoffs implicated and the realities of the cyber domain.

In sum, Perlroth's book is a valuable contribution to the debates and discussions surrounding the vulnerabilities market. She achieves the purpose she set forth: to illuminate and educate the layperson about the existence of the market, and how decisions by governments can influence—and possibly even create—the cyber weapons market. Indeed, a recent RAND Report indicates the U.S. population is growing increasingly concerned about ransomware.[45] Some have criticized Perlroth for providing a list of muddled recommendations in the epilogue, and for failing to identify specific solutions to the problems she identifies. However, she comes by the muddle-ment honestly, and is most certainly not the only commentator to conclude that this is an area without easy solutions. Indeed, she recognizes this challenge throughout the book, explaining that her objective is not to chart a course forward but to raise awareness of the problem and to pose the important questions.

Did the U.S. government's use of Stuxnet cause the development of the vulnerabilities market? Did the U.S. focus too much on offensive cyber capabilities and fail to appreciate the reciprocal consequences? I am not convinced Perlroth gets the answers to these questions correct, however, she earns praise for raising the questions. The book's ultimate contribution is in synthesizing the information and framing the questions that require the attention of those government officials and corporate actors responsible for their study and resolution.

45. Alan Suderman, *Cyberattacks Concerning to Most in US: Pearson/AP-NORC Poll*, AP NEWS (Oct. 11, 2021), https://bit.ly/2ZDIGcG.