Volume **4** (2) 2022 https://doi.org/10.5204/lthj.2658

Book Review

Nicole Perlroth (2021) *This is How They Tell Me the World Ends: The Cyberweapons Arms Race.* New York: Bloomsbury Publishing

Samuli Haataja
Griffith University, Australia

ISBN: 9781635576054

Nicole Perlroth's *This is How They Tell Me the World Ends: The Cyberweapons Arms Race* is a book by the former cybersecurity reporter for *The New York Times*. Its core focus is exploring the market for undisclosed vulnerabilities in computer software and systems. The author argues that these vulnerabilities are potentially valuable as they can be developed into cyber capabilities that give government agencies and other actors the ability to engage in a range of cyber operations, including espionage, law-enforcement activities and sabotage of critical infrastructure in other states.

Perlroth's book is written in a way that targets a general audience without a background in cybersecurity or international affairs. The author aims to shed light on the secretive 'cyberweapons industry'[1] by exploring questions about who is involved in it, whether there are any rules around it and whether there are limits to how so-called 'cyberweapons' are used.[2] This is a challenging undertaking as many involved in the industry are unwilling or unable to share details. Perlroth acknowledges that even after completing the book, 'much about the cyberarms trade remains impenetrable'.[3] Despite this challenge, the author draws on extensive material based on interviews conducted over seven years with over 300 individuals involved in or affected by the industry.[4] Perlroth also draws on confidential sources and documentary evidence[5] to provide an accessible account of the origins and development of this industry and its current state.

The book is structured into 23 chapters that are organised into seven parts. Part 1, 'Mission Impossible', serves as the introduction to the book, outlining its origins and the challenges of uncovering information about the industry. Parts 2–4, titled 'The Capitalists', 'The Spies' and 'The Mercenaries', provide accounts from various individuals working with or for companies and government agencies involved in purchasing, selling, developing or using undisclosed vulnerabilities and/or cyber capabilities. Here Perlroth captures the dilemmas many of these individuals face about whether vulnerabilities should be disclosed to vendors so that cybersecurity can be improved, sold for profit without knowing what purpose those vulnerabilities may be used for in the future, or used in pursuit of national security objectives.

[1] Perlroth, This is How They Tell Me the World Ends, xiv.
[2] Perlroth, This is How They Tell Me the World Ends, 17–18.
[3] Perlroth, This is How They Tell Me the World Ends, xiv.
[4] Perlroth, This is How They Tell Me the World Ends, xiii.
[5] Perlroth, This is How They Tell Me the World Ends, 411.

Part 5, 'The Resistance', details the efforts of companies—including Google, Facebook and Microsoft—to limit the availability of undisclosed vulnerabilities and other means to resist efforts by government agencies to undermine the cybersecurity of their products and services. In this part, the author highlights the important role played by private companies in implementing technical measures to make it more difficult for governments (whether foreign or their own) to obtain access to their customers' data or systems. Part 6, 'The Twister', outlines how a number of states have become actively involved in acquiring and using cyber capabilities in pursuit of their national interests, from Iranian cyber operations against Saudi Aramco in 2012 to Russian cyber operations against Ukraine's power grid in 2015. The 'twister' in this context refers to the escalatory spiral of cyber conflict between the US and its adversaries. Perlroth attributes this to the preparedness of the US to exploit vulnerabilities in its adversaries' systems and the failure of the US to effectively deter its adversaries from engaging in these activities.

Against this backdrop, Part 7, 'Boomerang', demonstrates the failure of US attempts to balance competing interests in deciding whether to disclose unknown vulnerabilities to vendors for patching or to use these capabilities for their national interests. This part of the book details how cyber capabilities developed by the US National Security Agency (NSA) were compromised and made publicly available online. Subsequently, some of these capabilities were repurposed and used by North Korea in the WannaCry ransomware incident in 2017 and by Russia in the NotPetya incident, which targeted Ukraine but spread globally, resulting in an estimated US$10 billion in damages.[6] These capabilities utilised an exploit the NSA referred to as 'EternalBlue', which made use of an undisclosed vulnerability in Microsoft Windows operating systems that the agency had known of for seven years before disclosing it to Microsoft only after it was compromised.[7] In this part, the author most effectively presents the book's underlying critique of the US' role in shaping the undisclosed vulnerability industry and its associated risks.

The book's central claim—alluded to in its provocative title—is that active efforts by the US and other governments (including Russia, India, Brazil, Singapore and Iran)[8] to stockpile undisclosed vulnerabilities and undermine the cybersecurity of computer systems globally increase the risk of a catastrophic cyber incident or 'Cyber Pearl Harbour' occurring.[9] While Perlroth is not a lawyer, and the focus of the book is not on law, the evident lack of sufficient legal restrictions on these activities underpins this claim. There are still glimpses of law throughout the book, from export agreements regulating the activities of companies involved in the trade,[10] lawyer involvement to ensure 'Stuxnet' (a US and Israeli cyber operation targeting an Iranian uranium enrichment facility) was targeted and that its effects were proportionate[11] and proposals for a 'Digital Geneva Convention' by Microsoft following the NotPetya incident in 2017.[12] But it is largely the lack of law—evident in the limited legal restrictions on these activities—that underpins Perlroth's argument. Regarding the industry, she writes that '[t]here were no norms—none that anyone could articulate anyway',[13] and in this absence of accepted rules, the US 'set the rules itself, making it permissible to attack a country's critical infrastructure in peacetime'.[14] It is correct that regulating the trade of these capabilities and limiting government agencies from acquiring them can be challenging. The European Union has, only after the publication of the book, sought to tighten export controls around dual-use 'cyber-surveillance' tools to limit their use for violations of human rights.[15] But the book largely disregards the fact that, since 2013, states have begun to reach some agreement about how international law does apply to the *use* of these capabilities (even if there continues to be debate about the specifics of this).[16]

One main concern regarding the book is the exaggerated threat of harm that underpins its argument. This is amplified by the imagery used to describe various cyber capabilities and their effects. For example, Perlroth describes how in 2015, 'Russian

[6] Perlroth, This is How They Tell Me the World Ends, 339–343.
[7] Perlroth, This is How They Tell Me the World Ends, ch 21.
[8] Perlroth, This is How They Tell Me the World Ends, 145.
[9] Perlroth, This is How They Tell Me the World Ends, xxv–xxvii.
[10] Perlroth, This is How They Tell Me the World Ends, 150–151.
[11] Perlroth, This is How They Tell Me the World Ends, 121.
[12] Perlroth, This is How They Tell Me the World Ends, 343.
[13] Perlroth, This is How They Tell Me the World Ends, 248.
[14] Perlroth, This is How They Tell Me the World Ends, 343.
[15] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), 2021 O.J. (L 206) 1.
[16] United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98 (June 24, 2013) 8; United Nations General Assembly, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, UN Doc A/76/136* (July 13, 2021).

hackers had been shelling Ukraine's computer networks with cyberattacks',[17] how NSA-developed tools 'had the power to inflict incalculable destruction' and could be transformed into a 'cyberweapon of mass destruction'[18] and how 'ransomware attacks were detonating across the globe' during the 2017 WannaCry incident.[19] While using this imagery is likely related to the book's broader target audience, it also functions to highlight the fear of a 'Cyber Pearl Harbour' looming throughout the book. Arguably this is an exaggerated threat of harm because, as the effects of the cyber incidents outlined in the book demonstrate, most cyber operations cause more limited technical effects, and it is extremely rare for destructive physical effects to occur, let alone on a large scale.

Overall, in light of Perlroth's aims in writing the book and its target audience, the book provides a great contribution. Despite its selected focus on a topic involving complex technical and political issues, it provides an accessible account of the development and use of cyber capabilities by states, the market for these capabilities that this has fostered and the risks it creates. But the threat it portrays should not be taken too literally.

Bibliography

Perlroth, Nicole. *This is How They Tell Me the World Ends: The Cyberweapons Arms Race*. New York: Bloomsbury Publishing, 2021.

Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), 2021 O.J. (L 206) 1.

United Nations General Assembly, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266*, UN Doc A/76/136* (July 13, 2021).

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/68/98 (June 24, 2013).

[17] Perlroth, This is How They Tell Me the World Ends, 294.
[18] Perlroth, This is How They Tell Me the World Ends, 331.
[19] Perlroth, This is How They Tell Me the World Ends, 333.