Journal of Strategic Security

Volume 14 | Number 2 Article 9

This is How They Tell Me the World Ends: The Cyber-Weapons Arms Race. By Nicole Perlroth. New York: Bloomsbury Publishing; 1st Edition, 2021. ISBN-13 : 978-1635576054. Pp. 528. $30.00.

Edward M. Roche , PhD, JD
Center for Cyber Arms Control

pp. 133-134

Recommended Citation
Roche, Edward M. , PhD, JD. "This is How They Tell Me the World Ends: The Cyber-Weapons Arms Race. By Nicole Perlroth. New York: Bloomsbury Publishing; 1st Edition, 2021. ISBN-13 : 978-1635576054. Pp. 528. $30.00.." *Journal of Strategic Security* 14, no. 2 (2020) : 133-134.
DOI: https://doi.org/10.5038/1944-0472.14.2.1958
Available at: https://scholarcommons.usf.edu/jss/vol14/iss2/9

This is How They Tell Me the World Ends: The Cyber-Weapons Arms Race. By Nicole Perlroth. New York: Bloomsbury Publishing; 1st Edition, 2021. ISBN-13 : 978-1635576054. Pp. 528. $30.00.

This is How They Tell Me the World Ends: The Cyber-Weapons Arms Race. By Nicole Perlroth. New York: Bloomsbury Publishing; 1st edition, 2021. ISBN-13 : 978-1635576054. Pp. 528. $30.00.

Review by Edward M. Roche, PhD, JD

The first cyber weapon was Stuxnet, discovered in 2010. It was a multi-billion dollar effort, built by a nation-state, using national laboratories, and deployed by intelligence services against a strategic national security target, the uranium centrifuges operating in Natanz, Iran. The discovery of this malware intensified a debate about cyberwar, cybercrime, cyberterrorism, cyberespionage, and a number of other disturbing acts that now have the word "cyber" attached as a prefix.

Here, Perlroth has focused on the emergence of a black market for cyber exploits. A large, but secretive and opaque industry has developed in the sale of malware, and governments are large purchasers of these unregulated goods because these snippets of code become components of cyber tools used to either conduct espionage, or develop the capability to launch cyber-attacks against opponents. Spelunking in the murky back rooms of cyber, the author had the cleverness (and also funding) to jump from one continent to another conducting interviews with leading personalities such as General Michael Hayden, as well as with others who appear content to remain in the shadows. And she repeats many famous quotes such as the one by Leon Panetta ("A Cyber Pearl Harbor").

There are a few weaknesses in this finely crafted work. The author has accepted the story about Russian interference being determinative in the 2016 U.S. Presidential election, when the Benkler, et al. (2018) book out of the Berkman Klein Center at Harvard, and the book Computational Propaganda out of Oxford, both of which actually use empirical measurements, disprove this uni-causal myth. In addition, Perlroth's description of Stuxnet, perhaps the most important cyber weapon ever, relies only on the first variant when there were several, but then talks about it escaping Natanz and infecting computers around the world, when that was actually a different variant designed for a completely different function. The failure of the United States to support a cyber weapons arms control convention is attributed to the U.S. desire to keep a perceived lead in the cyber arms race, when the idea actually floundered on different grounds (controls on exports of code would hinder cyber defense collaboration).

But those are nit-picking details. The overall theme of the book is correct, and the subtle infiltration of this underworld by what appears to be an intrepid journalist is a remarkable feat. Perlroth pulls back the cover on the shady dealers and creepy entrepreneurs that are not well known because many wish to remain anonymous and yet are so crucial for manufacturing of both offensive and defensive cyber technologies.

To understand the political, strategic, and legal challenges of cyber, one must follow the serious work being carried out in fora such as the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, the First Committee (Disarmament) of the United Nations, the European Network and Information Security Agency (ENISA), the Internet Engineering Task Force (IETF), the Internet Governance Forum, the Organization for Security and Co-operation in Europe, and in various leading think-tanks such as the Center for Strategic and International Studies (CSIS), particularly the work of James Andrew Lewis. All of these organizations publish informative works and recorded seminars covering different aspects of the cyber problem. Otherwise, your bookshelf will be awash with racy tabloid type analysis.

How They Tell Me is not a scholarly work, but instead is a type of chatty journalistic entertainment about a serious subject – very good reading for a flight, or lounging by a pool, although the use of foul language may put off some readers (it uses the word "f__k" 21 times). Perlroth comes to no serious conclusions, and does no serious analysis, but has produced a quick and entertaining read, sort of like an extended set of notes from a giant cocktail party punctuated with continual name-dropping and snarky observations. Fast-paced and exciting. Absolutely delightful reading. Yes, it will give a distorted and incomplete picture of the cyber arms race to many readers, but since only specialists and professionals actually make policy, it is unlikely to harm those serious efforts being pursued to develop a coherent national cyber defense, achieve cyber stability or formulate an international convention to limit the proliferation of this dangerous technology.

DOI: https://doi.org/10.5038/1944-0472.14.2.1958