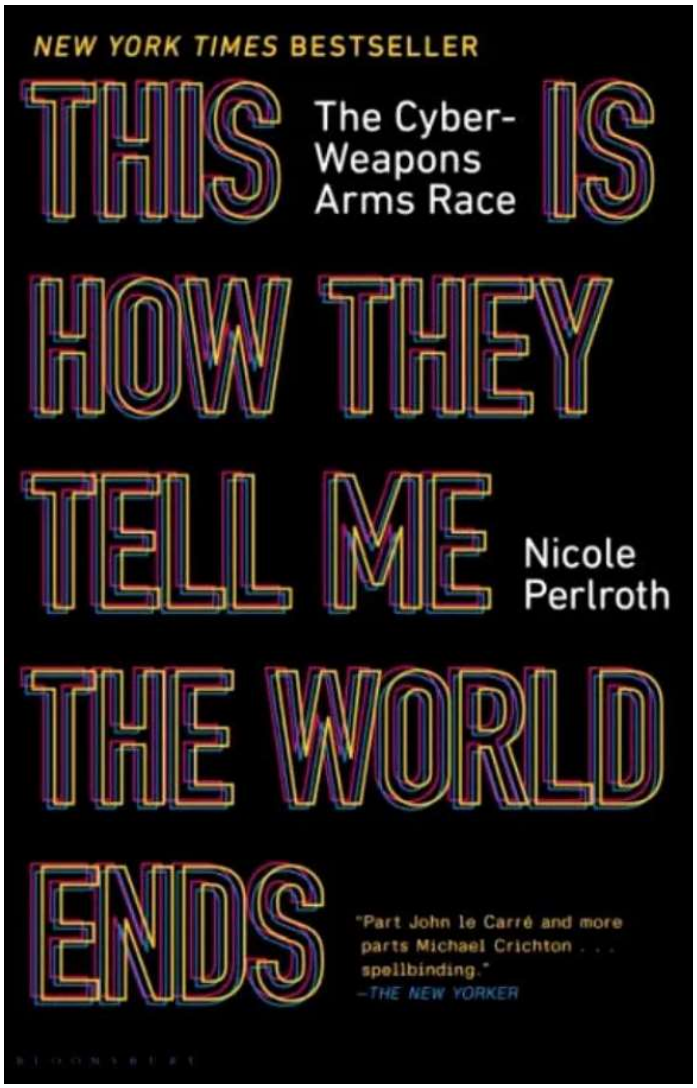
BOWLING GREEN DAILY NEWS

Even if you're tired of scary things, read this

Posted: Sunday, November 21, 2021

"This Is How They Tell Me the World Ends: The Cyberweapons Arms Race" by Nicole Perlroth. New York: Bloomsbury Publishing, 2021, 528 pages, $30 (hardcover).



"For years classified national intelligence estimates considered Russia and China to be America's most formidable adversaries in the cyber realm," Nicole Perlroth notes in "This Is How They Tell Me the World Ends: The Cyberweapons Arms Race," her treatise on an ever-escalating existential threat to our entire way of life. "China sucked up most of the oxygen, not so much for its sophistication, but simply because its hackers were so prolific at stealing American trade secrets. The Chinese were stealing every bit of American intellectual property worth stealing and handing it to their state-owned enterprises to imitate."

"But there was no question that in terms of sophistication, Russia was always at the top of the heap," she continues a little later. "Russian hackers had infiltrated the Pentagon, the White House, the Joint Chiefs of Staff, the State Department and Russia's Nashi youth group – either on direct orders from the Kremlin or simply because they were feeling patriotic – knocked the entire nation of Estonia offline after Estonians dared to move a Soviet-era statue. In one cyberattack Russian hackers, posing as Islamic fundamentalists, took a dozen French television channels off the air."

So begins the previously untold story of the cyber arms trade – a clandestine "cold war" that began in the 1990s and continues right up until the present moment. But unlike the version you may have heard about on the various news outlets, the United States actually has, according to Perlroth, been the primary perpetrator in the battle for ultimate control of the virtual world and all it increasingly controls. It was about 30 years ago that American defense contractors and intelligence agencies began shelling out six-figure payments to hackers for their help in exploiting vulnerabilities in code that would allow unprecedented access to previously secure databases and operating systems.

The book is extensively researched, with 60 pages of source notes at the conclusion of the prologue, 23 chapters and epilogue that form the main narrative. Structurally, the manuscript is arranged in seven major sections: "Mission Impossible," "The Capitalists," "The Spies," "The Mercenaries," "The Resistance," "The Twister," and "The Boomerang." The subtitles make additional sense as you make your way through the various episodes that eventually come together to form a complete

mosaic of the current state of affairs as they relate to the ongoing struggle for cyber supremacy that has been unfolding quietly since the dawn of the digital era. It is obvious Perlroth knows her stuff.

A core premise of the book is the progressively more difficult-to-deny emerging reality that the United States is not home to the expertise needed to keep our infrastructure safe from those who wish to do us harm from a safe distance. Our defensive capabilities have not kept pace with their offensive counterparts and, as a result, we often grossly underestimate the abilities and resourcefulness of our adversaries. To substantiate this claim, consider the following anecdote from "Perfect Storm," the 18th chapter and one I found particularly unsettling:

"Three years after the United States and the Israelis reached across Iran's borders and destroyed its centrifuges, Iran launched a retaliatory attack, the most destructive cyberattack the world had seen to date. On Aug. 15, 2012, Iranian hackers hit Saudi Aramco, the world's richest oil company – a company worth more than five Apples on paper – with malware that demolished 30,000 of its computers, wiped its data and replaced it all with the image of a burning American flag. All the money in the world had not kept Iranian hackers from getting into Aramco's systems. Iran's hackers had waited until the eve of Islam's holiest night of the year – 'The Night of Power,' when Saudis were home celebrating the revelation of the Koran to the Prophet Muhammad, to flip a kill switch and detonate malware that not only destroyed Aramco's computers, data and access to email and internet but upended the global market for hard drives."

A cybersecurity and digital espionage correspondent for The New York Times, Perlroth has covered Russian hacks of nuclear plants, airports and elections, North Korea's cyberattacks against movie studios, banks and hospitals, Iranian attacks on oil companies, banks and the Trump campaign, and hundreds of Chinese cyberattacks, including a months-long hack of The Times. The recipient of several journalism awards, including best technology reporting by the Society of Business Editors and Writers, her 2014 Times profile of security blogger Brian Krebs was optioned by Sony Pictures and a 2016 story of Chinese hackers in a welding shop server was optioned for a television series.

I was impressed both with the comprehensive scope as well as the corresponding level of detail Perlroth brings to her prose. The account she provides serves as both an exposé as well as a cautionary tale; it is also a stark reminder that the United States is not always the role model we like to project to the rest of the world. For instance, the author traces the spread of the cyber arms trade – an invisible, classified and highly lucrative enterprise – to foreign actors including the United Arab Emirates and Saudi Arabia, where former National Security Agency hackers were contracted to hack American allies. I was surprised to learn that one of the targets of these hackers was Michelle Obama, the former first lady. Apparently her communications were captured by these former NSA agents. I don't recall seeing that on the nightly news.

Perlroth concludes "This Is How They Tell Me the World Ends" with a scathing indictment of how the last administration failed to take the growing cyberthreat seriously – and even eliminated the White House cybersecurity coordinator. When Donald Trump initiated what many consider to be an ill-advised and unnecessary trade war with China, he effectively nullified the Obama-Xi agreement to cease cyberattacks for industrial trade theft – an agreement that, by all accounts, both sides were honoring. The bottom line seems to be that we are much more vulnerable today than we were in 2016. Evidently you need to be able to understand a technological threat before you can mount an effective response.

Admittedly, this was a scary one. And although I realize a lot of readers are probably tired of scary, our fatigue shouldn't negate the relevance of Perlroth's work or make the reasons we should be on edge any less visceral. Highly recommended.

Reviewed by Aaron W. Hughey, University Distinguished Professor, Department of Counseling and Student Affairs, Western Kentucky University.