Intelligence in Public Media

Review Essay: Chips, Cyberweapons, and Larceny: Perspectives on Technological Risk

Yong Suk Lee

Chip War: The Fight for the World's Most Critical Technology
Chris Miller (Scribner, 2022), 464 pages, photos, illustrations, map.

This is How They Tell Me the World Ends: The Cyberweapons Arms Race
Nicole Perlroth (Bloomsbury, 2021), 528 pages.

The Lazarus Heist: From Hollywood to High Finance: Inside North Korea's Global Cyberwar
Geoff White (Penguin, 2022), 304 pages.

The revolution in information systems technology during the past 40 years has fundamentally changed how people live and relate to one another. Unfortunately, as with many innovations in history, human beings rapidly weaponized their latest discovery. The pace of innovation in weaponizing the computer-based technologies that form the fabric of our lives is moving as fast as the technology itself. Within 20 years, discussions about cutting edge automation in warfare went from GPS-guided munitions to artificial intelligence, swarms of autonomous drones, and quantum computing. Taken together, authors Chris Miller, Nicole Perlroth, and Geoff White offer a close examination of technological breakthroughs that made the computer revolution possible, how nation-states are competing against one another in a new cyberweapons arms race, and how one country is using these innovations to run a vast criminal enterprise.

Chris Miller, *Chip War*

War, *weapon*, *offense*, and *defense* are words often found in references to cybersecurity and advances in computing technology. Historian Chris Miller would say this is for good reason because, if nothing else, America's wars in the late 20th century provided the testing ground for innovation and spotlights the collaboration between early tech companies and the US military. *Chip War* is a paean to the US tech pioneers, such as Fairchild Semiconductors and Texas Instruments, that founded an industry and revolutionized the world, thanks in part to their Cold War partnership with the Department of Defense (only to later lose their competitive edge to Japan, South Korea, and Taiwan in the global consumer market).

Miller traces the history of a single technological innovation and its impact on modern geopolitical history: the microchip. The late Stephen Jay Gould, a renowned Harvard paleontologist, used the phrase *punctuated equilibrium* to describe periods of rapid change in evolutionary biology after a long period of stasis. This was the case in summer 1958 when a young Texas Instruments engineer, Jack Kilby, came up with an idea to assemble multiple transistor components on a single piece of semiconductor material. He called his invention an "integrated circuit," but it became colloquially known as a "chip." (14) Kilby did not know it at the time but he set the stage for a period of rapid evolution in the nascent computer industry and would receive the Nobel Prize in 2000. Gordon Moore, one of the early pioneering engineers in Silicon Valley, later coined the concept of Moore's Law to describe the exponential growth in computing power every two years that Kilby had unleashed. (15)

A few years after Kilby in 1965, another Texas Instruments engineer, Weldon Word, took on a Vietnam War–inspired challenge of producing a cheap precision weapon for the US Air Force. By 1972, Texas Instruments delivered the Paveway laser-guided bomb. As Miller writes, "Outside of a small number of military theorists and electrical engineers, hardly anyone realized Vietnam had been a successful testing ground for weapons that married microelectronics and explosives in ways that would revolutionize warfare and transform American military power." (60).

Microchips did more than make dumb bombs smart. The same chips made home computers possible, and Moore's Law of faster processing power and cheaper

All statements of fact, opinion, or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

manufacturing made them affordable. The Internet and email may have started as Cold War–inspired Pentagon programs, but rapid progress in integrated circuit technology brought them into our homes and into our hands. Global chip production and the supply chain that tied them together were beacons of hope for economic integration, with US companies, such as Apple, relying on chips made in Taiwan to be shipped to China to be assembled into devices that are shipped back across the Pacific and around the world. In theory, this level of integration and globalization is supposed to make the world more peaceful, with mutual dependence replacing mutually assured destruction. Today, age-old distrust among nations and political leaders who see their own people as a threat to their rule have formed a wall into which forces of globalization have collided.

When China's President Xi Jinping in 2014 said that "without Cybersecurity, there is no national security," Miller argues that he was not talking about hackers and phishing. (242) For Beijing, cybersecurity meant basic foundational technology that made computers possible. China's growing tech sector relied on data centers made possible only with US-produced components and "even the surveillance system that tracks China's dissidents and its ethnic minorities relies on chips from US companies like Intel and Nvidia." (245) China declared in its Made in China 2025 plan released in 2015 that it will be independent of US and foreign technologies in a decade and all components critical to China's global tech dominance will be made in China, signaling to the world its strategic intent and betraying the leadership's distrust of a Western rules-based economic order. As Miller eloquently argues, "From swarms of autonomous drones to invisible battles in cyberspace and across the electromagnetic spectrum, the future of war will be defined by computing power [and] the US military is no longer the unchallenged leader." (282)

Nicole Perlroth, *The Cyberweapons Arms Race*

As soon as computers and computer-based information management systems became indispensable, they also became vulnerabilities. The 1983 movie *War Games* first showed audiences what this vulnerability could look like, and, even if we are not yet near hackers being able to unleash global thermonuclear war, the ability of a non-state actor to hold a country hostage by threatening to turn off the lights is an ever increasing threat. *New York Times* reporter Nicole Perlroth dives into the dark world of hackers and a thriving underground market for bespoke cyberweapons and tools in *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*, and what she uncovers is as unnerving as the title of her book.

As military jargons litter the cybersecurity landscape, computer systems and their vulnerabilities borrow heavily from biology, using words such as a worm, virus, and infection to describe attacks against information systems as though they are an assault against the human body. The other term readers will learn from reading Perlroth is *zero-day*. Simply put, a zero-day is a previously unknown computer-software vulnerability an attacker can exploit.

A modern computer program has millions of lines of code and an innocuous error can open the door to a potential attacker. Perlroth shows that from the early days of computing, a select group of people have made a sport of trying to identify zero-day vulnerabilities in programs and operating systems, such as in Microsoft Windows. Some people do it to burnish their reputations within the hacker community, others do it for money and sell their discoveries to the highest bidders. Since the entire world has gone online, the stakes have increased and zero-day exploiters can now command hundreds of thousands of dollars for their discoveries.

For a long-time, the United States was the leader in zero-day exploits. It had the most active computer hacking community in the world, and the US Intelligence Community invested early in exploiting vulnerabilities in computer-based information systems for intelligence collection. This hidden capability came into the light as a new weapon in 2009. Perlroth claims the United States and its allies that year introduced a worm into the computers at the Iranian nuclear facility in Natanz, exploiting four zero-day vulnerabilities in Microsoft Windows. (122–23) Over the next weeks and months, the rotors controlling the uranium enrichment centrifuges spun out of control and wrecked themselves. The Iranians never acknowledged the destruction caused by Stuxnet, as this particular worm later became known. (130) The author quotes Michael Hayden, former director of CIA and NSA, as having said "this has a whiff of August 1945.

Somebody just used a new weapon and this weapon will not be put back in the box." (131).[a]

Perlroth argues the United States, in an attempt to prevent a possible Israeli raid against Iran and preserve peace in the Persian Gulf, crossed the "Rubicon," as she titled one of the chapters in her book. (117) If Perlroth is right, the US and its allies responsible for the operation against Natanz did more than cross the Rubicon against another nation state. She writes that, by the summer of 2010, security researchers around the world started picking up traces of the Natanz worm; the cyberweapon had escaped into the wild. (128) Although never officially confirmed, it wasn't long before intelligence exploits against Iran ended up as front-page news, and Perlroth says this was a wake up call for chief information officers everywhere: they were collateral damage in an escalating global cyberwar. (132)

Perlroth is focused on telling a good story and does not explicitly assign blame, but *This Is How They Tell Me the World Ends* is a harsh critique of the Intelligence Community. Her bottom line is that the US government developed a powerful cyber arsenal, the weapons leaked, and now the entire world is in danger. It is as if the US military lost control of the most powerful bombs in its nuclear arsenal and they are now for sale on the black market. Perlroth starts her book with a claim that "starting in 2016, the National Security Agency's own cyber arsenal—the sole reason the US maintained its offensive advantage in cyberspace—was dribbled out online by a mysterious group" that called itself the Shadow Brokers. The group started "trickling out NSA hacking tools and code for any nation-state, cybercriminal, or terrorist to pick up and use in their own cyber crusades."[b] (xx)

Stuxnet, Shadow Brokers, and revelations of US bulk-data collection have taken a toll on the level of trust between the US government and private industry, when government-industry cooperation is needed the most to defend the country's online infrastructure. Perlorth argues that US tech giants went to war against their own government, prioritizing protection of their users, and distancing themselves from Washington. (227–33) For the firms, this also made good business sense. Microsoft, for example, cannot be seen as cooperating with the US government against another country, and the government for its part lost credibility when it secretly exploited vulnerabilities in US-made computer products for intelligence collection and exploitation, leaving the businesses to scramble to contain the global fallout when these programs leaked.

Geoff White, *The Lazarus Heist*

One country that has benefited strategically from exploiting computer-security vulnerabilities is North Korea, where only a handful of elites go online outside the country's strictly controlled intranet. Geoff White, journalist and former BBC correspondent, chronicles North Korea's unlikely rise as a cybercrime kingpin in *The Lazarus Heist*. White claims what the North is doing in cyberspace is not warfare but larceny. Pyongyang has become the reverse Robin Hood, stealing from poor, impoverished nations to help fund the regime's one-family rule and its spending priorities, such as purchasing luxury goods and investing in its strategic weapons programs. White writes, "Whereas many country's cyber teams are focused on stealing information for strategic advantage, North Korea's online war is part of a battle for economic survival." (7)

There are no shortages of recent North Korean cyber exploits. but the heart of White's book is the breakdown of the attempted heist of $1 billion from Bangladesh's national bank in February 2016. The North's hackers, taking advantage of international time zones and the fact that the weekend starts on a Friday in most Muslim countries, attempted to transfer a billion dollars from Bangladesh's account at the US Federal Reserve in New York to the RCBC Bank in the Philippines. (106–107) In the end, the heist failed purely by chance when the word *Jupiter* raised a red flag. Of the many RCBC branches in Manila, the North Korean hackers picked the one on Jupiter Street as the receiving bank for the wire transfers from New York. It happens that M/V *Jupiter* is the name of a sanctioned Iranian ship and use of the word cost the hackers $951 million, after $101 million had been transferred. (109) Most, but not all, of the transferred funds were later recovered. A Gmail address on a phishing email that hackers used to gain entry into Bangladesh's banking

[a] See also Hayden Peake, review of *Countdown to Zero Day: STUXNET and the Launch of the World's First Digital Weapon*, by Kim Zetter, *Studies in Intelligence* 60, no. 1 (March 2016).

[b] See also Peake, review of *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, by Ben Buchanan, *Studies in Intelligence* 64, no. 2 (June 2020).

system, according to the FBI, was also used to phish Sony Pictures Entertainment in 2014, pointing to Pyongyang as the culprit. (118)

It turned out North Korea's attack against Sony Pictures Entertainment for producing *The Interview*, a comedy about two reporters hired to kill the North's leader Kim Jong Un, was just a practice run. Following its failed billion-dollar heist, the North launched the Wanna Cry ransomware attack in 2017, hitting targets like Great Britain's National Health Service. (194–97)

Bottom Line

Of the three books reviewed in this article, *Chip War* is the best-researched and most informative, *They Tell Me This is How the World Ends* is the best written and most entertaining, *The Lazarus Heist* is the weakest. Miller is a historian of Russia by training, and Perlroth and White are journalists who can spot good stories. The fact that the authors are not technicians steeped in the subject matter makes these books more approachable. For IC professionals looking for an introduction to technology and cybersecurity, Miller, Perlroth, and White offer excellent starting points.

❖ ❖ ❖

The reviewer: Yong Suk Lee is a former deputy associate director of CIA and a visiting fellow at the Hoover Institution, Stanford University.