This is How They Tell Me the World Ends: The Cyber-Weapons Arms Race | Nicole Perlroth

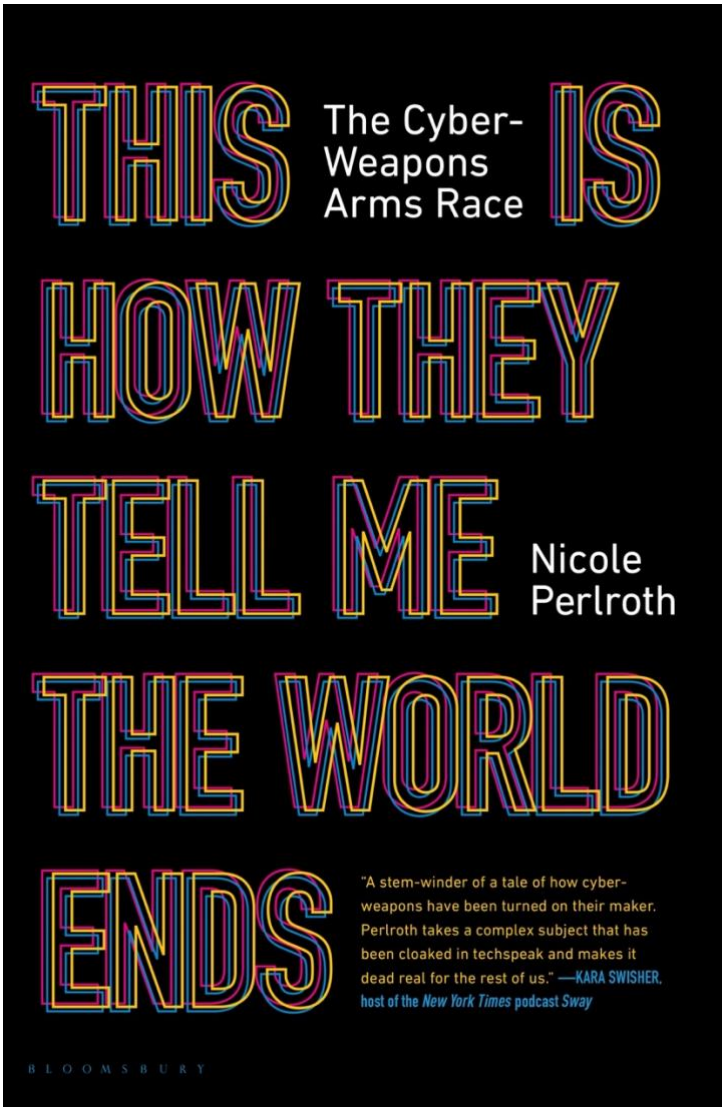
March 2nd, 2021

INTRODUCTION

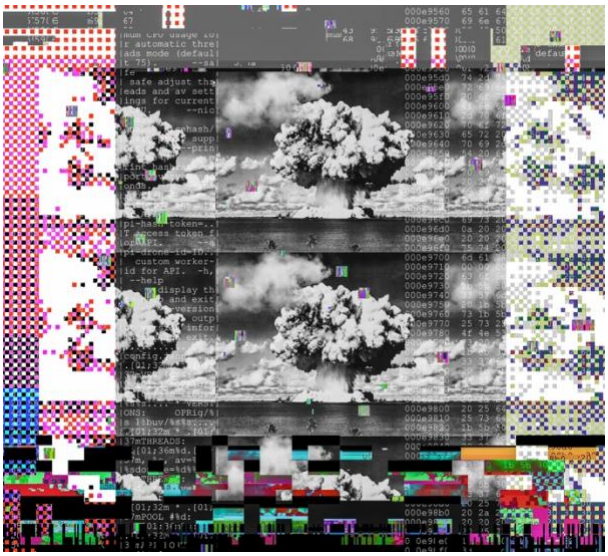
Nicole Perlroth is an award-winning cybersecurity journalist for The New York Times, where her work has been optioned for both film and television. She is a regular lecturer at the Stanford Graduate School of Business and a graduate of Princeton University and Stanford University. She lives with her family in the Bay Area, but increasingly prefers life off the grid in their cabin in the woods.

WHY DO I CARE?

I don't have a particularly confident view on how most people think about cybersecurity and the cyberattack, threat landscape. If I had to guess, I'd say most people think of cyber in much the same way as they think about land, sea, and air attacks. That is to say, they see it as just another extension of a battlefield where adversaries can engage in attacks and counterattacks. On a deeper level, I don't think people really understand that one of the major differences between analogue battlespace and cyberspace, is that the latter has no boarders and is organized in a fundamentally different way. Even if you tell someone that "cyber has no boarders," they are likely to think "yea, I get it…you can attack anyone, anywhere." But that's not it, or at least, that's not the borderless nature of cyberwar that is so horrifying. Not only does our world run on software, much of which was never meant to be connected to the Internet (SCADA control systems, hospital medical equipment, etc.), but we are all more or less using the *same* software. This means that not only are there no boarders; there are no countries. It's all one giant, open space. The vulnerabilities are within us. Each and every one of us who uses digital devices, runs windows machines, has an iPhone, goes on a web browser, etc., is vulnerable to being hacked and attacked using the same vulnerabilities and exploits irrespective of citizenship or motive. There is a thriving black-market that sells information about vulnerabilities and access to exploits to the highest bidder. Many of these sellers do not discriminate between a North Korean government arms buyer, an ISIS fighter, or the NSA. What this means in practical terms is that we are all using the same weapons, or at the very least, targeting the same vulnerabilities. When the US developed and tested the atomic bomb in 1945,



it was one of only two countries that had the resources and capabilities to create and deploy such a weapon. Even to this day, nuclear programs are luxuries available to only the most well-funded or highly ambitious nation states. This is not the case in cyberspace.



So, the question is, *what do we do about it*? At the individual and business level, people should be steering away from connected devices, buying and using them only in cases where they really are vital, or where the benefits greatly outweigh the harms. In our rush to connect everything, we have put things online with little or no benefit, while at the same time exposing enormous vulnerabilities that could leave us badly damaged or even dead and out of business. At the government level, I'm less confident about what steps can be taken, though Bruce Schneier discussed a number of them in our last episode together. I think, overtime, you are going to see more and more collaborate between government and the private sector, as well as a "Chinese wall" of sorts between various allies who are able to agree on certain "rules of the road." (e.g. perhaps a transatlantic software alliance).

BACKGROUND QUESTIONS:

Background — **Q:** How did you get started in journalism? **Q:** What got you on the beat of writing about cybersecurity? **Q:** How long have you been doing it? **Q:** What do you like about it? **Q:** What are the characters like that you encounter? **Q:** How different are they than other types of technically minded individuals?

Your Book — **Q:** When did you begin to write this book? **Q:** Why did you decide to write it? **Q:** Is there some angle to this story that other authors aren't covering or that you think you could do better? **Q:** So, how does the world end?

Missing Coverage — **Q:** What's missing from the coverage around cyber security and the cyber weapons industry?

Key Insight & Action — **Q:** What is the key insight you want people to take away from this book? **Q:** What do you want them to do after they are done reading it?

WTF is a Cyber Weapon? — **Q:** WTF is a cyber weapon? **Q:** For someone who doesn't have a sophisticated, let alone basic understanding of how software is created and code is generated, how can he/she appreciate (1) why software is inherently porous and vulnerable and (2) how exploits are written and how they work? (i.e. how are these weapons made and what is it that makes them work?)

Deterrence vs. Attack — **Q:** Why is it harder to deter cyberattacks than it is to deter conventional ones?

Attribution — **Q:** What kind of headway has been made in the area of attribution?

Evolution of Cyber Arms Trade — **Q:** How has the cyber arms trade evolved over time? **Q:** When did the market first develop? **Q:** How international is this marketplace (both sellers and buyers) and has it become more international over the years? **Q:** Has this made it more difficult for the US to control the spread of knowledge about zero-day vulnerabilities so that it can be the only one to exploit them?

Zero-Day — **Q:** Why are zero-day vulnerabilities and exploits so important? **Q:** Do major intelligence agencies bother with exploiting non-zero-day vulnerabilities?

Stuxnet — **Q:** What was the impact of Stuxnet on the rest of the world? **Q:** Was it something akin to the US invasion of Iraq in Gulf War I, where the rest of the world could witness the technical superiority of America's armed forces on full display?

Cyber Pearl Harbor — **Q:** Is the analogy of a "cyber pearl harbor" an accurate one for thinking about the types of threats we face?

Solar Winds — **Q:** What was the Solar Winds hack? **Q:** What was so alarming about it? **Q:** What lessons can we draw from it?

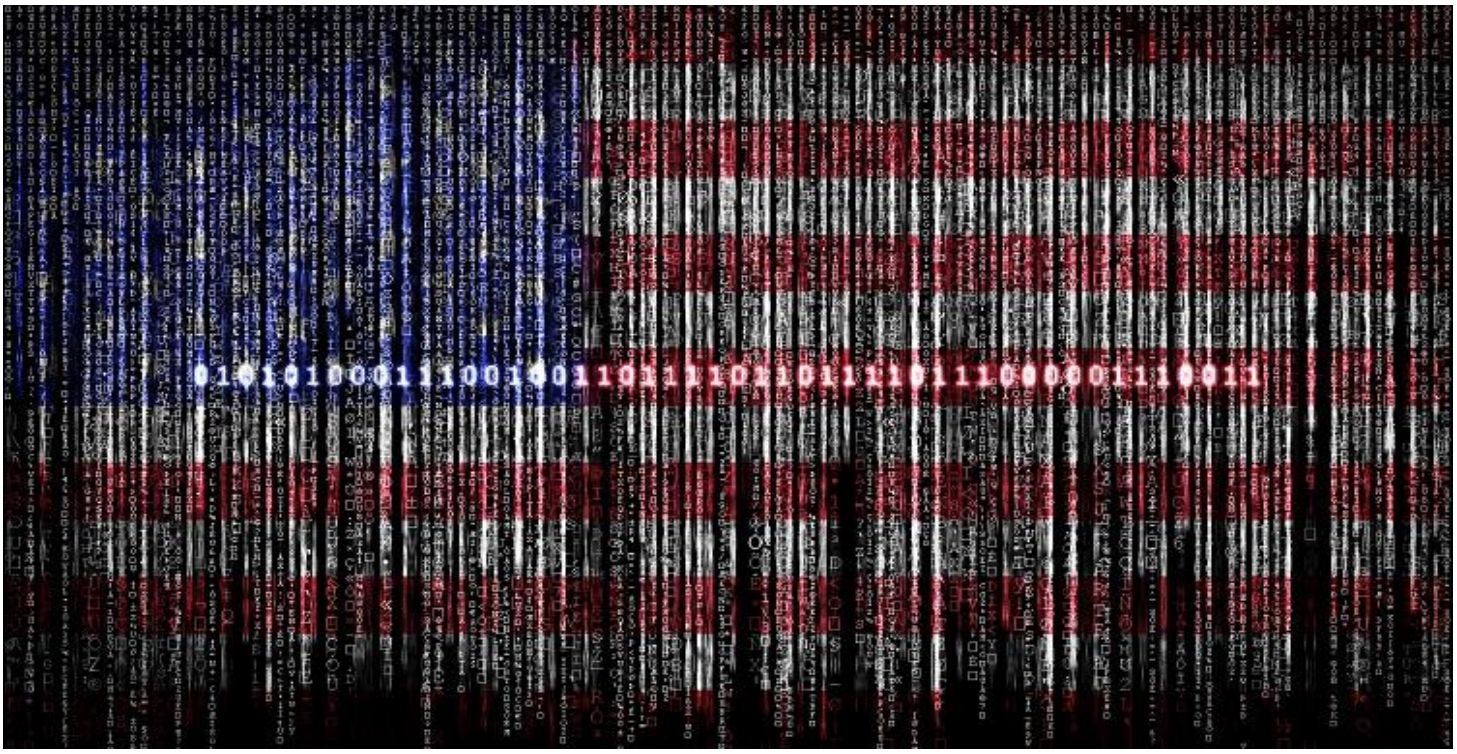
Biden Admin — **Q:** What is the Biden administration's attitude towards cyber? **Q:** How are they approaching this?

Twitter Account — **Q:** How come you deleted your twitter account?

India-China — **Q:** What can you tell us about the NYTimes article suggesting that China infiltrated and conducted cyber-attacks against the Indian electric grid?

QUOTES:

Solar Winds may have been the biggest cyberattack on the United States in years, if not ever. But it was hardly a singular event. In the last half decade or so, American corporations have suffered billions of dollars of losses in similar incursions. Between 2019 and 2020, more than 600 towns, cities and counties were hit by ransomware attacks, shutting down hospitals, police departments and more. America's adversaries—Russia, China, Iran and North Korea—have by now thoroughly infiltrated the computer systems that run some of the United States' most important infrastructure, including not just power grids and dams but also nuclear plants. All of which raises the question: Why does this keep happening? After all, the United States isn't just the most formidable and intimidating military power in the world; it's also the most sophisticated cyber power. The country's conventional arsenal has proved remarkably effective at scaring off any would-be attackers; these days, no nation on the planet would dream of going toe-to-toe with the United States military. So



why doesn't the same logic work in the cyber realm, where Washington could just as easily inflict biblical vengeance on anyone who messed with it? — Jonathan Tepperman

Deterring cyberattacks turns out to be much, much harder than deterring conventional ones, for a long list of reasons. Among them: Despite all its offensive power, the United States, as one of the most wired nations on earth, is also more vulnerable to such attacks than many of its less- connected enemies. Cyberattacks are also relatively cheap, while cyberdefense is expensive and painstaking. And then there's the problem of attribution: Given how hard it often is to spot digital incursions in the first place (remember, the Solar Winds hack went undetected for months), and the tendency of countries to rely on private hackers only loosely connected to the government to do their dirty work, figuring out whom to retaliate against can be very difficult. Unlike nuclear missiles, hacks rarely come stamped with a clear return address. — Jonathan Tepperman

This book is the story of our vast digital vulnerability, of how and why it exists, of the governments that have exploited and enabled it and the rising stakes for us all. — Jonathan Tepperman

The hackers who actually create all those nasty little tools and then sell them to whatever government will pay the most — no questions asked — bear primary responsibility. And sure, the foreign states who use these tools against us or their own people are guilty too. But none of this would have happened, Perlroth argues, if Washington hadn't decided years ago to neglect cyberdefense and focus instead on paying programmers around the world to find and weaponize vulnerabilities in existing software — gaps known as "zero days" in the industry — that grant those that wield them "digital superpowers." If enabling this market was Washington's original sin, its second catastrophic blunder, according to Perlroth, was Stuxnet: the computer worm the United States allegedly used to destroy a fifth of the centrifuges at Iran's Natanz nuclear enrichment plant in 2009-10. While the worm, a stunning technological breakthrough, may have forestalled an Israeli attack on Iran, set back Tehran's weapons program and driven the mullahs to the bargaining table, it also shattered a basic norm: It was the first time one government had digitally infiltrated the networks of another and used its access not for spying — which everyone does — but to wreak physical havoc. Once that gentlemen's rule was broken, Perlroth argues, it became open season for America's enemies to try to do the same to it; and now it's only a matter of time, she concludes, till we face a digital Pearl Harbor. — Jonathan Tepperman

The decision by the United States and Israel to develop and then deploy the Stuxnet computer worm against an Iranian nuclear facility late in George W. Bush's presidency marked a significant and dangerous turning point in the gradual militarization of the Internet. Washington has begun to cross the Rubicon. If it continues, contemporary warfare will change fundamentally as we move into hazardous and uncharted territory. — Misha Glenny

Stuxnet has effectively fired the starting gun in a new arms race that is very likely to lead to the spread of similar and still more powerful offensive cyberweaponry across the Internet. Unlike

nuclear or chemical weapons, however, countries are developing cyberweapons outside any regulatory framework. — Misha Glenny

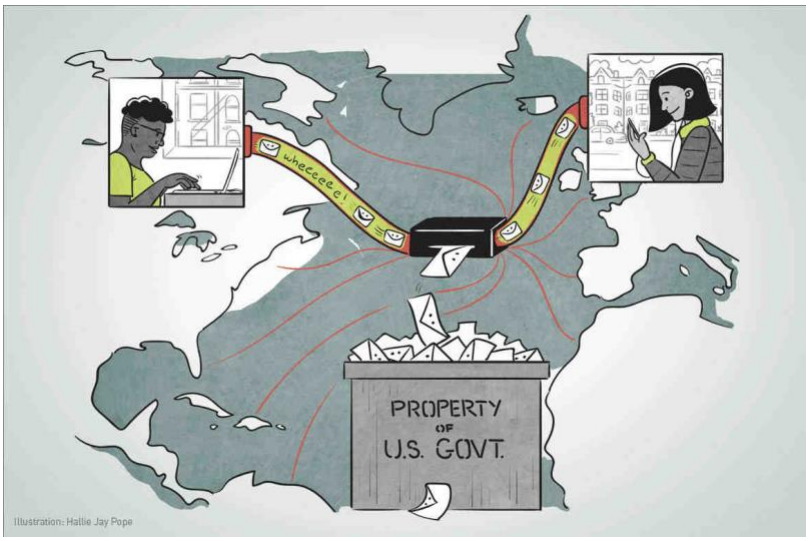
During the cold war, countries' chief assets were missiles with nuclear warheads. Generally their number and location was common knowledge, as was the damage they could inflict and how long it would take them to inflict it. Advanced cyberwar is different: a country's assets lie as much in the weaknesses of enemy computer defenses as in the power of the weapons it possesses. So in order to assess one's own capability, there is a strong temptation to penetrate the enemy's systems before a conflict erupts. It is no good trying to hit them once hostilities have broken out; they will be prepared and there's a risk that they already will have infected your systems. Once the logic of cyberwarfare takes hold, it is worryingly pre-emptive and can lead to the uncontrolled spread of malware. — Misha Glenny

Until now, America has been reluctant to discuss regulation of the Internet with Russia and China. Washington believes any moves tow ard a treaty might undermine its presumed superiority in the field of cyberweaponry and robotics. And it fears that Moscow and Beijing would exploit a global regulation of military activity on the Web, in order to justify and further strengthen the powerful tools they already use to restrict their citizens' freedom on the Net. The United States must now consider entering into discussions, anathema though they may be, with the world's major powers about the rules governing the Internet as a military domain. — Misha Glenny

Nobody can halt the worldwide rush to create cyberweapons, but a treaty could prevent their deployment in peacetime and allow for a collective response to countries or organizations that violate it. — Misha Glenny

Early last summer, Chinese and Indian troops clashed in a surprise border battle in the remote Galwan Valley, bashing each other to death with rocks and clubs. Four months later and more than 1,500 miles away in Mumbai, India, trains shut down and the stock market closed as the power went out in a city of 20 million people. Hospitals had to switch to emergency generators to keep ventilators running amid a coronavirus outbreak that was among India's worst. Now, a new study lends weight to the idea that those two events may well have been connected — as part of a broad Chinese cybercampaign against India's power grid, timed to send a message that if India pressed its claims too hard, the lights could go out across the country. The study shows that as the standoff continued in the Himalayas, taking at least two dozen lives, Chinese malware was flowing into the control systems that manage electric supply across India, along with a high-voltage transmission substation and a coal-fired power plant. — David E. Sanger and Emily Schmall

Until recent years, China's focus had been on information theft. But Beijing has been increasingly active in placing code into infrastructure systems, knowing that when it is discovered, the fear of an attack can be as powerful a tool as an attack itself. — David E. Sanger and Emily Schmall



The issue is we still haven't been able to get rid of our dependence on foreign hardware and foreign software. — General Hooda

"A good defense isn't enough; we need to disrupt and deter our adversaries from undertaking significant cyberattacks in the first place," Mr. Biden said, adding, "I

will not stand idly by in the face of cyberassaults on our nation." — David E. Sanger and Nicole Perlroth

"I want to be clear: My administration will make cybersecurity a top priority at every level of government — and we will make dealing with this breach a top priority from the moment we take office," Mr. Biden said, adding that he plans to impose "substantial costs on those responsible." — David E. Sanger and Nicole Perlroth

The hubris of American exceptionalism — a myth of global superiority laid bare in America's pandemic death toll — is what got us here. We thought we could outsmart our enemies. More hacking, more offense, not better defense, was our answer to an increasingly virtual world order, even as we made ourselves more vulnerable, hooking up water treatment facilities, railways, thermostats and insulin pumps to the web, at a rate of 127 new devices per second. — Nicole Perlroth

At the N.S.A., whose dual mission is gathering intelligence around the world and defending American secrets, offense eclipsed defense long ago. For every hundred cyberwarriors working offense — searching and stockpiling holes in technology to exploit for espionage or battlefield preparations — there was often only one lonely analyst playing defense to close them shut. — Nicole Perlroth

America remains the world's most advanced cyber superpower, but the hard truth, the one intelligence officials do not want to discuss, is that it is also its most targeted and vulnerable. — Nicole Perlroth

When Leon Panetta, then secretary of defense, warned of a coming "Cyber Pearl Harbor" in 2012, he was dismissed as stoking FUD. The Cyber Pearl Harbor analogy is, indeed, flawed: The U.S. government did not see the Japanese bombers coming, whereas it has seen the digital equivalent coming for decades. And the potential for a calamitous attack — a deadly explosion at a chemical plant set in motion by vulnerable software, for example — is a distraction from the predicament we are already in. Everything worth taking has already been intercepted: Our personal data, intellectual property, voter rolls, medical records, even our own cyberweaponry. — Nicole Perlroth

This threat often feels too distant to combat, but the solutions have been there for decades: Individuals just decided that access and convenience, and in governments' case, the opportunities for espionage, were worth leaving windows open, when we would have all been better off slamming them shut. — Nicole Perlroth

There's a reason we believed the fallacy that offense could keep us safe: The offense was a bloody masterpiece. — Nicole Perlroth

As the market expanded outside the N.S.A.'s direct control, the agency's focus stayed on offense. The N.S.A. knew the same vulnerabilities it was finding and exploiting elsewhere would, one day, blow back on Americans. Its answer to this dilemma was to boil American exceptionalism down to an acronym — NOBUS — which stands for "Nobody But Us." If the agency found a vulnerability it believed only it could exploit, it hoarded it. — Nicole Perlroth

In modern warfare, “active defense” amounts to hacking enemy networks. It’s mutually assured destruction for the digital age: We hacked into Russia’s troll networks and its grid as a show of force; Iran’s nuclear facilities, to take out its centrifuges; and Huawei’s source code, to penetrate its customers in Iran, Syria and North Korea, for espionage and to set up an early warning system for the N.S.A., in theory, to head off attacks before they hit. — Nicole Perlroth

To understand how we got here, facing one escalating attack after another, and how we might possibly claw our way out, it’s useful to look back at the Russian attack that put us on this offensive course. That year, 1983, workers at the American embassy in Moscow came to believe that everything they said and did was being captured by the Soviets. They suspected a mole, and had it not been for a tip from the French, who discovered a bug in their teleprinters, they might have never discovered the mole was in their machines. In 1984, President Ronald Reagan personally approved a classified project, code-named Gunman, to find and eradicate any Soviet bugs in embassy equipment. It took 100 days just to get every last piece of equipment back to Fort Meade and nearly 100 more days to uncover the most sophisticated exploit the agency had ever seen. Sitting in the back of an embassy typewriter was a tiny magnetometer, a device that measured the slightest disturbance in the earth’s magnetic field. It had been recording the mechanical energy from every last typewritten stroke and transmitting the results via radio to a nearby Soviet listening unit, hidden in the embassy’s chimney. By the time Gunman was complete, and more implants were discovered, it was clear that the Soviets had been siphoning American secrets from our typewriters for eight years. “That was our big wake up call,” James R. Gosler, the godfather of American cyberwar, told me. “Or we’d still be using those damn typewriters.” — Nicole Perlroth

Finding every Russian back door could take months, years even. And climbing out of our current mess will entail a grueling choice to stop leaving ourselves vulnerable. For individuals, this means making life less convenient. It’s not ignoring password prompts and software updates, turning on two-factor authentication, not clicking malicious links. For businesses, it requires testing code as engineers write it, not after it has made its way into consumer hands. It requires adding moats around the crown jewels: using hand-marked paper ballots, removing the controls that govern our nuclear plants, medical equipment and air traffic from anything else. — Nicole Perlroth