The Washington Post
August 5, 2018

Book Review

The Perfect Weapon **War, Sabotage, and Fear in the Cyber Age**
by David E. Sanger, Crown, $28, 357 pp.

Our inadequate defense against cyberattacks

by Christian Caryl

Director of National Intelligence Daniel Coats, left, and Army Lt. Gen. Robert P. Ashley, director of the Defense Intelligence Agency, answer questions at a hearing held by the Senate Armed Services Committee in March. (Win McNamee/Getty Images)

Director of National Intelligence Dan Coats does not pull his punches. In a recent congressional hearing, while most of the media was preoccupied with the latest Mueller indictments and the disastrous Helsinki summit, Coats issued a stark warning. Russian cyberattacks on U.S. democracy are continuing, he said — and we are doing little to counter them. Drawing an explicit comparison with the situation before the 9/11 terrorist attacks, he declared: “The warning lights are blinking red again.”

Coats’s remarks probably came as little surprise to David E. Sanger, a national security correspondent for the New York Times. In his new book, “The Perfect Weapon,” Sanger offers a panoramic view of the rapidly evolving world of cyber-conflict. He covers incidents from the covert U.S. cyber-campaign to sabotage Iran’s nuclear program (a story we know about largely because of Sanger’s diligent reporting) to Edward Snowden’s epic heist of National Security Agency data. And yes, there’s also plenty of background on Russia’s active measures during the 2016 campaign.

But there’s also a wealth of gripping material on stories that have probably been missed by the broader public. Sanger reveals that Russian hackers penetrated super-secret Pentagon internal networks in 2008. How? By leaving USB drives spiked with malware lying around the public areas of a U.S. base in the Middle East. “Someone picked one up,” Sanger writes, “and when they put the drive in a laptop connected to [a Pentagon-White House-intelligence network], the Russians were inside.” (The Defense Department ultimately responded by sealing the USB ports on all of its computers with super glue.) Then-Deputy Defense Secretary William Lynn called it “the most significant breach of military computers ever.”

The Chinese get points for sheer subtlety. In 2010, Beijing hackers broke into a Google server that contained a database of orders to the company from the Foreign Intelligence Surveillance Court. The Chinese knew precisely what they were doing: By accessing the FISA orders, they could tell which of their spies in the United States was on the radar of the FBI. In 2008, the Justice Department informed presidential candidate Barack Obama that the Chinese had penetrated his campaign’s computers, apparently hoping to collect intelligence on his personality and future policies. Unlike the Russians in 2016, though, they kept the information for themselves.

And then there are the North Koreans, who, as Sanger notes, have devoted a significant portion of their gross domestic product to the development of a highly effective cyber-army — giving them powerful capabilities completely out of proportion to their tiny economy. The investment has clearly paid off. In 2016, their hackers broke into the central bank of Bangladesh, making off with $81 million. That was well short of the $1 billion they were hoping for. Even so, as Sanger notes, “if it had been a physical bank heist, it would have been considered one of the largest and most brilliant in modern times.”

It all adds up to a persuasive argument for the truth of the book’s title. Cyberthreats are so effective, in part, because they come in so many forms: One expert breaks them down into “vandals, burglars, thugs, spies, and saboteurs.” Cyberwarriors can steal cash or sensitive information, surveil their enemies from a comfortable distance, blacken reputations, tamper with real-world machinery, or troll their opponents into silence.

And they can do all this under the cover of anonymity. Attribution — the problem of figuring out who is behind that attack on your server or your bank account — remains one of the thorniest issues for defenders. When the movie studio Sony Pictures was devastated by hackers in 2014 after producing a film satirizing North Korea, the FBI immediately had good reason to suspect Pyongyang of orchestrating the attack. "But as President Obama's aides knew, suspecting was one thing. Proving it was another." Sanger says the intelligence community ultimately obtained the evidence it was looking for. The U.S. government hasn't publicly revealed what it knows — presumably because it doesn't want to betray its capabilities to the North Koreans.

You'd think, after all this, that we would have learned our lesson. Yet the most disturbing theme of Sanger's book is the degree to which policymakers and the public remain oblivious to the threat. Clinton campaign chairman John Podesta's willingness to click on a fake Google message — actually a spear phishing attack from Russian military intelligence — shows that even well-informed people are soft targets. Our profound dependence on cybertechnology makes us all the more vulnerable, yet the overall level of U.S. cybersecurity, in both the private and the public domains, remains pathetic.

Again and again, in Sanger's account, the United States experiences cybersecurity failures on a colossal scale. Take the catastrophic attack by the Chinese on the Office of Personnel Management that was discovered in 2015. The hack compromised a huge database containing a wealth of personal detail on some 22 million Americans, including those who had filed security clearances with the U.S. government, giving the Chinese valuable information on U.S intelligence operations. Yet the response was lackluster. The Obama administration never blamed Beijing.

The biggest comedy of errors, though, involves Putin's assault on the democratic process in 2016. Though Obama did ultimately impose some sanctions and expel Russian diplomats, those moves seem to have had little effect. That the Russians are apparently continuing the same campaign today, as Coats has said, clearly owes a great deal to Obama's failure to retaliate decisively. (Some of his advisers suggested publicizing the details of Putin's overseas assets, for example, but this option was rejected.)

Yet President Trump has now been in office for a year and a half, and he has shown little inclination to make up for Obama's mistakes. With Trump's blessing, Republicans in Congress have just refused to allocate additional funds to bolster the security of our electoral infrastructure ahead of the midterms. And The Washington Post recently reported that the National Security Agency and the Pentagon's Cyber Command have decided to join forces to prevent possible election tampering — despite the notable absence of any corresponding directive from the White House.

And this is the main message that Sanger is trying to get across with his book: Our country is a big, fat, juicy cyber-target for our enemies. Yet we seem determined to avoid changing our collective ways. When will we finally wake up?