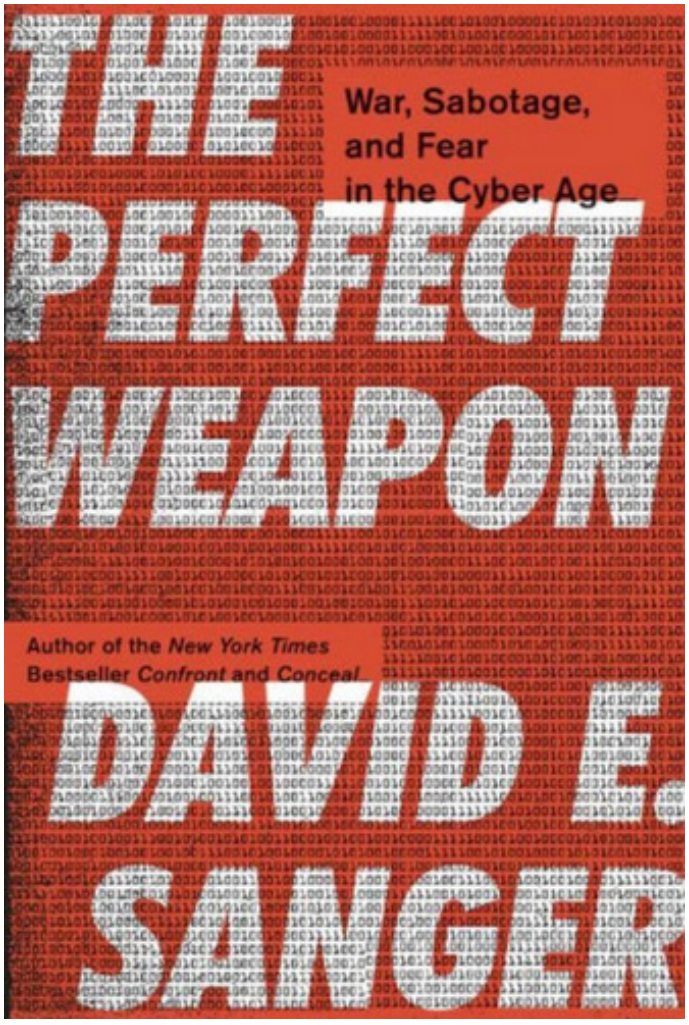
BOWLING GREEN DAILY NEWS

Cyber age tale may keep you up at night

Posted: Sunday, April 7, 2019

"The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age" by David E. Sanger. New York: Crown Publishing Group (an imprint of Penguin Random House), 2018, 354 pages, $28. (hardcover).



"In the cyber world today, we are somewhere around World War I," David E. Sanger explains near the beginning of "The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age," his new treatise on the new world we now occupy. "A decade ago there were three or four nations with effective cyber forces; now there are more than 30. The production curve of weapons produced over the last 10 years roughly follows the trajectory of military aircraft.

"As of this writing, the best estimates suggest there have been upward of 200 known state-on-state cyberattacks over the past decade or so – a figure that describes only those that have become public," he continues. "And, as in World War I, this glimpse into the future has led nations to arm up, fast. The United States was among the first, building 'Cyber Mission Forces,' as they call them – 133 teams, totaling more than 6,000 troops, were up and running by the end of 2017."

Sanger researched his subject matter extensively, as evidenced by the 28 pages of source notes at the conclusion of the prologue, 12 chapters and afterword that comprise the main narrative. The prose can get a bit dense as the reader makes his or her way through this inherently enlightening, yet thoroughly frightening foray into the fragile nature of today's interconnected digital architecture, although anyone with a rudimentary background in advanced communications technologies should have minimal difficulty navigating the manuscript.

One consideration that struck me repeatedly as I made my way through "The Perfect Weapon" was the unmistakable aura of paranoia that seemed to envelop the government's efforts to keep us safe from foreign hackers determined to disrupt our way of life. In the environment described by Sanger, every new piece of intelligence seemed to precipitate a debate regarding whether it would be prudent to disclose it to a wider audience – including those who could be most affected should the attack prove effective.

For instance, witness the following excerpt from "Pandora's Inbox," the second chapter and one of my personal favorites: "America's secrecy about offensive cyber, and its fear of revealing sources and

methods, meant that the government never really warned American banks and businesses that they were ripe targets for the new Iranian cybercorps. Instead, the United States issued general cautions about the need for cyber defenses and information-sharing – the digital equivalent of telling people to seek shelter in their basements in the case of a nuclear exchange without mentioning that it would be the radiation, as much as the blast, that was likely to wipe them out."

Sanger is a national security correspondent for The New York Times and has been a member of three teams that won the Pulitzer Prize for international reporting. A graduate of Harvard College, where he majored in government, he is a member of the Council on Foreign Relations and the Aspen Strategy Group. His previous books include "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power" and "The Inheritance: The World Obama Confronts and the Challenges to American Power."

It is obvious from the very first page that Sanger is an insider; i.e., he has been privy to meetings and exchanges that most of us will never be privileged to attend or overhear. As an insider, he is able to address his subject matter in an authoritative manner – certainly he has much more credibility in this arena than many of his counterparts exploring the same universe. Moreover, he tells the story on two levels. First, he provides a technical explanation – in relatively elementary terms – of how cyberattacks are developed and employed. This is where an understanding of computer basics will no doubt help the reader decipher exactly what he is articulating. What I found much more captivating, however, was the deeper level in which he explores the often-convoluted decision-making process the key players in the cybersecurity game often engage in to arrive at what course of action to take in light of the realities they uncover.

The author goes to some lengths, for example, to dissect how Presidents George W. Bush and Barack Obama managed to severely damage Iranian centrifuges by inserting malicious code into their operating systems in a quasi-successful attempt to thwart their fledging nuclear program. Yet, he also demonstrates convincingly how our defensive capabilities were not as comparatively developed as our offensive proficiency. This was evident when, during President Donald Trump's first year in office, the tools we had fashioned as a means of inflicting reciprocal damage on countries who threaten us were pilfered and targeted against us. It turned out we did not have adequate defenses to contend with our own creations.

"Until the cyber age came along, America's two oceans symbolized our enduring national myth of invulnerability," Sanger concludes near the end of the book. "The threat of nuclear attack preoccupied us during the Cold War, but generally the United States has assured it could take out dictators, conduct strikes on terrorists and blow up missile bases in faraway lands with relatively little fear of retaliation.

"And after some terrifying close calls, notably the Cuban Missile Crisis in 1962, we found an uneasy balance of power with our primary adversaries – mutually assured destruction – to deter the worst," he concludes. "It worked, or has worked so far, because the cost of failure is too high. In the cyber age, we have not found that balance, and probably never will. Cyberweapons are entirely different from nuclear arms, and their effects have so far remained relatively modest. But to assume that will continue to be true is to assume we understand the destructive power of the technology we have unleashed and that we can manage it. History suggests that is a risky bet."

If you want a book that will keep you up at night, you might want to consider adding this one to your reading list. Highly recommended.

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