2021

A Critical Review of: The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age

Steven Cauthron
Augusta University, scauthro@augusta.edu

A Critical Review of: The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age

Cover Page Footnote

A CRITICAL REVIEW OF: *THE PERFECTN WEAPON: WAR SABOTAGE AND FEAR IN THE CYBER AGE*

Steven T. Cauthron

Chemical Officer, United States Army

First Lieutenant Steven T. Cauthron is a U.S. Army Chemical Officer assigned to Fort Leonard Wood, Missouri. He is currently a Master of Intelligence and Security Studies student at Augusta University. His research interests include the study of terrorism, counterterrorism, intelligence disciplines, weapons of mass destruction, and national security. He holds a BS in Chemistry with a Nuclear Science Concentration from Augusta University.

Email: steven.t.cauthron.mil@mail.mil

David Sanger, the *New York Times*' national security correspondent, provides an expert glimpse into the impact of contemporary cyber technology in his book, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. His writing brings insight from the unique, rarely seen, perspective of several high government and corporate officials. This unusual opportunity results in a captivating book that continuously draws the reader in for more. Despite being a technical topic, Sanger has written in a way that makes it easy for the reader to follow the intense developments in cyber operations regardless of their level of technical experience in the realm of cyber warfare.

Sanger's premise, although delivered in a way that could be considered alarming, falls short of the common sensationalizing that other authors fall victim to when writing about weapons and warfare. Up until now, nuclear weapons and similar weapons of mass destruction have been viewed as the key weapon that could be used if the situation ever called for a serious option. Sanger instead argues that, as a result of recent advancements in cyber technology, cyber weapons are in fact the perfect weapons. He supports this argument through displays of recent occurrences against the United States in both the corporate and political spheres. His focus on recent cyberattacks and cyber espionage in multiple areas demonstrate just how effective current cyber technology can be when serving as a weapon.

The breadth of scenarios discussed in detail by Sanger only strengthen his thesis. Beginning with the high note of discussing Russian cyberattacks that were used to target American infrastructure, Silicon Valley, and the Democratic National Committee set the ground work for demonstrating the capabilities the United States needs to be prepared to defend itself from. Continued reading expresses that national security implications in relation to cyber warfare have a plethora of constitutional rights implications that must be considered when making policies and decisions. His chapter, *Man in the Middle*, focuses greatly on these privacy concerns and the long-lasting impacts that decisions can have. Candid conversations with influential cyber players such as Apple CEO, Tim Cook, enable readers to better understand the importance of utilizing proper privacy settings as well as encrypted messages and devices to limit the likelihood of being an easy target.

Throughout his book, Sanger continuously identifies similar flaws in the United States that can be exploited by potential cyber attackers. These weaknesses range from individual responsibilities, such as privacy settings for electronics and social media, to organizational responsibilities, such as has been the case in multiple hacks. In 2014, a North Korean hack caused Sony Pictures to realize it was not immune to cyberattacks by foreign entities. This incident showed the world that corporations were subject to being attacked and that states could use cyber operations as a way to even the playing field between themselves and a much larger opponent. If that was not enough to convince the US government that cybersecurity needed to become a priority they would soon learn. In 2015 the Office of Personnel Management learned just how damaging and useful cyber weapons could be when it fell victim to a hack by the Chinese government that resulted in the release of millions of personnel records in the form of a security clearance questionnaire.

These chapters by Sanger are important because they show the true dangers of the future of cyber warfare and that nobody is immune to them. It is easy to imagine a kinetic battlefield and believe you are safe and not at risk because you are not there. Sanger's powerful writing shows that the same is not true for a cyber battlefield and that those of us trying to defend ourselves from these attacks have an uphill battle. It is repeatedly argued and demonstrated that as technological advances are made, the capacity for offensive cyber operations will continue to grow at a faster

pace than the capacity for defensive operations. As a result, it is necessary for both government and corporate entities to take cybersecurity as a serious threat that can have damaging effects, not only in the present but also for years to come.

I highly recommend *The Perfect Weapon* to anyone with an interest in learning more about cybersecurity and cyberwarfare. Sanger's thorough and enlightening writing is extremely enjoyable. Although technical, the simplicity of his explanations make it a readable option for those seeking to learn more about America's competition in cyberspace. The enthusiasm and candor portrayed through his writing give reason to take cybersecurity more seriously and his variety in examples of attacks in recent years show that cyber capabilities are obviously "The Perfect Weapon".

References:

Sanger, David. 2018. *The Perfect Weapon: war, Sabotage and Fear in the Cyber Age".* New York, NY: Penguin Random House LLC.