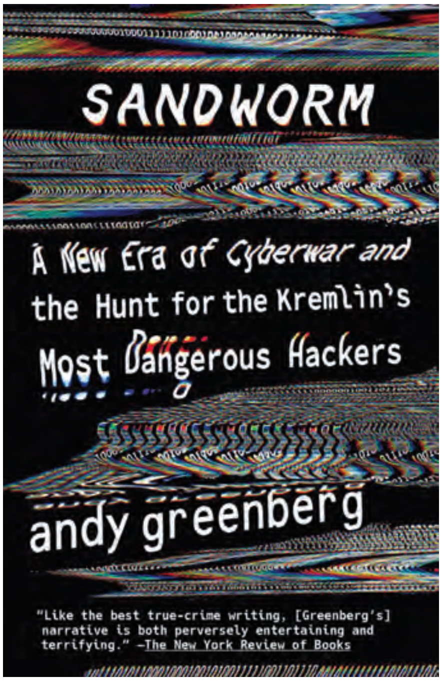
> *with divergent behaviors . . . the risk is significant; and the definition of success is cloudy at best.*

Aycock and Glenney find no evidence that any existing system is going to produce a war-winning advantage for a fleet commander soon. What they do find is a lot of narrow or task-specific AI products that can support tactical tasks, but they contend these do not aggregate into operational success or support decision-making at the operational level of war. Rather than ignore the potential or limit AI systems to tactical tasks, the authors recommend that the defense establishment stop thinking about commercial games and initiate the development of operationally relevant AI-based military decision systems to support Navy or geographic commanders.

AI at War is a balanced product with several chapters ideal for professional military education curricula on the changing character of warfare and the role of technology. The future is uncharted, but the editors note the continuities facing the use of AI, including "the painstaking work required to achieve innovation, the need for rigorous policy analysis, the friction of implementation, ethical concerns, and the ever-present dilemma of how to trust new technologies." Although produced for a naval audience, the book is just as valuable for the joint warfighting community.

All told, *AI at War* is the most important book-length contribution on this topic since Scharre's highly regarded *Army of None: Autonomous Weapons and the Future of War* (Norton, 2019). It is practical, insightful, and replete with the kind of healthy skepticism and openness that the defense community should embrace as we enter the fourth industrial revolution. It is a highly commendable product for navigating the challenges and the opportunities of artificial intelligence. **JFQ**

Dr. Frank Hoffman is a Distinguished Research Fellow in the Center for Strategic Research, Institute for National Strategic Studies, at the National Defense University.


SANDWORM
A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers
andy greenberg
"Like the best true-crime writing, [Greenberg's] narrative is both perversely entertaining and terrifying." —The New York Review of Books

Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers

By Andy Greenberg
Anchor Books, 2020
368 pp. $18.00
ISBN: 978-0525564638

Reviewed by Janine Lafortune

Sandworm reads like a fiction crime thriller but raises the alarm about a looming nonfiction threat: unrestricted cyber war. Andy Greenberg, the author and a senior writer for *Wired*, cautions readers that the world is in the midst of a global cyber arms race. He forewarns that civilian critical infrastructure remains highly vulnerable to cyber attacks by aggressive state and nonstate actors. He identifies malicious cyber attacks, as part of a new tit-for-tat, with escalation mirroring that of the Cold War, with increasingly sophisticated cyber attack methods and capabilities constituting a new, modern arms race. He concludes with an ominous message: that the next cyber doomsday is not a matter of *if* but *when*.

The main narrative follows the aggressive and unrelenting cyber attacks that have been bombarding Ukraine since 2015. For 5 years, Ukraine served as a petri dish for cyber operations by Russian state and nonstate actors, who were testing the limits of deniability, attribution, proportionality, and discrimination. Each time they conducted an attack—BlackEnergy in 2015, Industroyer in 2016, NotPetya and Bad Rabbit in 2017—these cyber hackers walked away unscathed and free to strike again. Intertwined with this narrative is a second one, detailing Greenberg's quest to find and oust the masterminds behind many of these attacks, accompanied by civilian cyber security professionals. Together, the two accounts illuminate the new and evolving world of cyber conflict.

Greenberg traces the history of state-sponsored cyber attacks and offers a critique of U.S. cyber activities. Once Stuxnet, the computer worm identified in 2010, was compromised, it opened a Pandora's box. Cyber gurus, aggressors, and defenders have been playing an escalating game of cat and mouse ever since. Greenberg warns that this is no game, however, and that it comes with real consequences—millions of dollars in economic losses, physical damage to property, and potential loss of life. He points to NotPetya as the perfect case study. The malware spread to more than 65 countries and caused an estimated $10 billion in damages, demonstrating unprecedented scope. Greenberg argues that malicious cyber attacks are becoming more dangerous, and indiscriminate attacks on civilian critical infrastructure, spreading beyond traditional notions of state sovereignty, should serve as a warning to the global order.

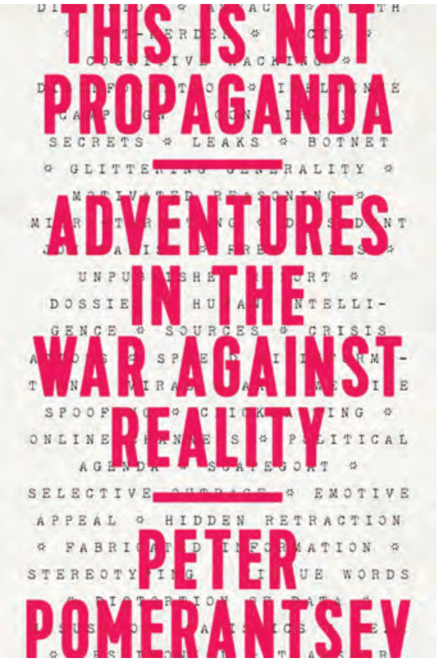
Greenberg's ability to present complex and dry technical jargon with fluidity and accessibility aids readers in navigating the more challenging elements of his argument. However, at times, *Sandworm* jerks the reader around in its six sections. Greenberg interrupts his main narratives with branch narratives, biographies, and fascinating but superfluous history. For instance, instead of presenting mysterious cyber hackers such as Fancy Bear, FSociety, and Shadow Brokers in "Part V: Identity," he introduces the former two in "Part III: Evolution" and the last in "Part IV: Apotheosis." Similarly, he presents a new cyber attack called Bad Rabbit/Olympic Destroyer, followed by a chapter on false attribution, all in "Section V: Identity." These interruptions create confusion and tangents that detract from his fundamental question: Who is Sandworm? Nevertheless, Greenberg's research, analysis, and impressive sources provide credibility, and a sense of urgency and mystery, making it an exciting read.

Sandworm makes a convincing case about the threats of unrestricted cyber war and the vulnerability of civilian critical infrastructure. The book is thorough, with rich accounts from cyber security specialists and cyber attack victims adding weight and perspective to the main argument. Greenberg's focus on Ukraine as the test bed for Russian malicious cyber activities provides the greatest example of cyber conflict's complexity. Offensive cyber attacks to support tactical military operations, as seen in Ukraine, are just a tiny facet of the cyber influence that strategic competitors leverage to obtain combat advantage. There is also a psychological component to cyber war, manifesting as harassment, extortion, and even destruction—all aimed at eroding civilians' trust in their governments and their ability to protect its people.

Although Greenberg is careful to question U.S. cyber security policy in the wake of NotPetya, his efforts in this regard fall short. Despite interviewing top cyber security officials from the administrations of Barack Obama and Donald Trump, Greenberg never critically examines U.S. cyber security policy, U.S. Federal cyber security operations teams (national roles, authorities, and responsibilities), or the ways international humanitarian law applies to cyber activities. He fails to address the U.S. creation and alignment of responsible cyber security organizations, such as the Cybersecurity and Infrastructure Security Agency, and the policies that govern their activities—a notable omission. The Department of Defense's official policy states that the law of war will apply to cyberspace operations; however, *Sandworm* chronicles malicious activity that occupies the gray zone—below the threshold of armed conflict. In a missed opportunity, *Sandworm* pirouettes around the most significant issue the United States faces in the wake of the Ukrainian case study: How does the Nation conduct cyber operations consistent with domestic law, applicable international law, and rules of engagement, when the same rules do not constrict our competitors and adversaries?

Despite failing to address some of the most significant legal considerations the United States faces to cyber operations, *Sandworm* is one of the most comprehensive chronicles of cyber warfare available over open-source platforms. The book forces self-reflection—which at times triggers vulnerability—and challenges our underlying assumptions of U.S. cyber security policy, methods, and capabilities, as well as those belonging to actors within the strategic environment. Its warnings and insights on cyber's "gray areas" make it a formidable resource for those in the joint force and the national security community charged with the preservation and the defense of U.S. military advantage and U.S. interests. **JFQ**

Major Janine Lafortune, USA, is a Space Operations Officer (FA40) serving in the Joint Information Operations Warfare Center at the Pentagon.



This is Not Propaganda: Adventures in the War Against Reality

By Peter Pomerantsev
PublicAffairs, 2020
256 pp. $16.99
ISBN-13: 9781541762121

Reviewed by Jeffrey Mankoff

In the Jewish mystical tradition of Kabbalah, the concept of *tsimtsum* represents an alternative, essentially deistic vision of creation—with God stepping back from the universe He created, leaving behind a vacant space for humanity to impart its own meaning. From this concept, the critic Boris Groys coined the phrase *Big Tsimtsum* to describe the void created by the collapse of the intellectual, ideological, and moral certainties embodied (or at least claimed) by the Soviet Union. For journalist Peter Pomerantsev, Groys's Big Tsimtsum, the absence of meaning left behind when the certainties of the past evaporated, was the necessary condition for the emergence of a new, more cynical brand of politics—and not only in post-Soviet Russia. Unlike the seemingly existential, ideologically infused