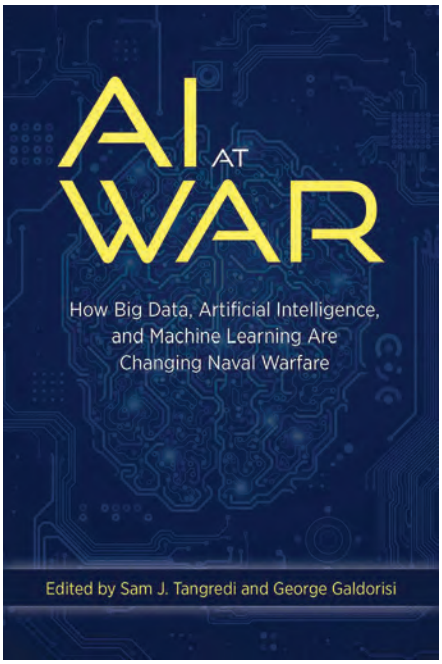


AI at War: How Big Data, Artificial Intelligence, and Machine Learning Are Changing Naval Warfare

Edited by Sam J. Tangredi and George Galdorisi
Naval Institute Press, 2020
461 pp. $49.95
ISBN: 978-1682476062

Reviewed by Frank Hoffman

There are many books and TED Talks about artificial intelligence (AI) these days, and most assert that this technology will revolutionize our politics, economy, and way of life. Futurists including Martin Ford, author of *Rise of the Robots: Technology and the Threat of a Jobless Future* (Basic Books, 2016), claim that AI and the various technologies that constitute both it and robotics will transform industries and rival the impact of electricity in our lives. A decade ago, one could be doubtful about the hype associated with AI, automation, and autonomous systems. Today, however, AI systems are increasingly used commercially and generate tangible advantages for those who master its applications and alter their operating methods appropriately.

AI at War examines how well the presumptions about AI can be applied to military missions. A carefully curated anthology developed by two military veterans with solid research and academic credentials, Sam Tangredi and George Galdorisi, *AI at War* does not offer a roadmap, but it clearly identifies barriers to embracing AI and maximizing its potential in naval warfare. There are both obstacles and opportunities in applying such powerful tools, and the conceptual, organizational, and cultural ramifications are spelled out in the book's various chapters. There is cause for concern about rushing precipitously into new fields with emergent technologies, but there is also risk in being complacent—and outpaced by the competition.

AI at War has 19 chapters, plus a foreword by Admiral James G. Stavridis (Ret.), former commander of U.S. European Command, and an epilogue by Admiral Michael S. Rogers (Ret.), former commander of the National Security Agency and U.S. Cyber Command. There are chapters devoted to specific naval functions, including command and control; intelligence, surveillance, and reconnaissance; and integrated fires. Each chapter has merit, but three stand out.

Paul Scharre, director of studies at the Center for New American Security, addresses the U.S. Navy's mixed progress with unmanned systems. He is unsparing in his criticism of the Navy's failure to press forward with a carrier-based unmanned strike system:

> *Even in a zero-sum budget environment, it would be far more sensible for the Navy to cut one or more carriers to fund development of an uninhabited combat aircraft than continue building $13 billion carriers that will lack the necessary aircraft to adequately project power against sophisticated competitors.*

Scharre, a former Soldier, appreciates the influence of Service culture and identity in impeding progress in the naval aviation community. He is sensitive to how strongly pilots embrace their function of flying and notes that unmanned systems "strike at the very core of their identity." But he remains convinced that the risks the Navy is taking by relegating the MQ-25 Stingray to merely a refueler platform are unacceptable, putting the Service decades behind in advancing U.S. power projection capabilities against formidable competitors.

In her incisive chapter, Nina Kollars, a professor at the Naval War College, identifies a major limitation of AI. She is concerned that a centralized, top-down approach to AI or its employment as a closed system will deprive the fleet of the kind of bottom-up innovations that come from the edge of an organization in wartime. Such innovations have been a unique advantage of some military cultures and can be a force multiplier when Sailors and Marines improvise under fire and rapidly share their user-generated solutions. Kollars's chapter stresses that instead of displacing human creativity, the design of AI capabilities should "support 'in stride' adaptation at the tactical/operational level as applied by practitioners as they apply the tip of the spear to the problems of combat." She may be discounting the potential for creativity from AI programs, but her reminder about the value of human intuition and inspiration should be heeded.

In another chapter, Adam Aycock and William Glenney relate their efforts to develop an operational-level AI-enabled system for naval commanders. This effort, which they facetiously call "putting Mahan in a box," derived over a dozen observations from past uses of AI products in beating humans in competitive games. Many advocates think that AI victories in chess, Go, and poker games apply equally to the complexity of warfare. Their study finds that existing AI-supported gaming is woefully inadequate for the demands of the military operating environment:

> *In war, timely big data can be very hard to obtain and is often obfuscated by the adversary, the rules are not clear and are subject to change by all side of the conflict, the uncertainty for all aspects is huge; feedback loops are few and slow, there is often an absence of clear, direct cause and effect*

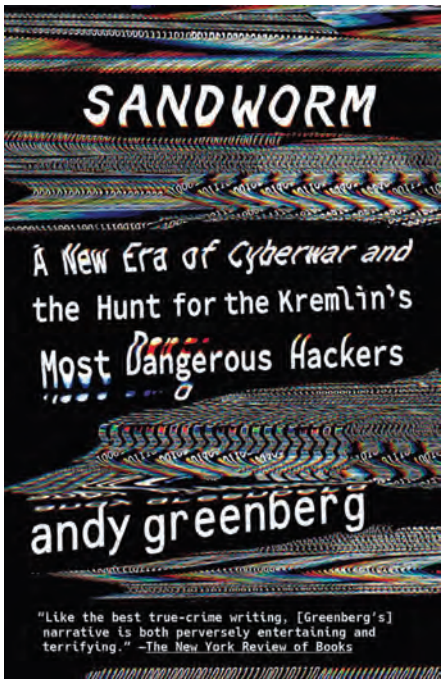
with divergent behaviors . . . the risk is significant; and the definition of success is cloudy at best.

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

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