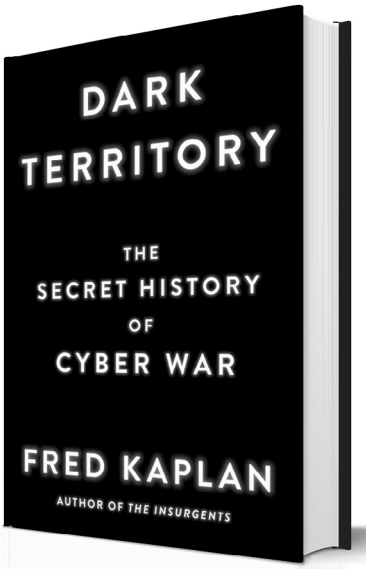
Dark Territory: The Secret History of Cyber War by Fred Kaplan

Reviewed by Dr. David V. Gioe



Writing a history of anything without clear or accepted chronological boundaries, such as cyber war, is a challenging undertaking. Even with a definite start and stop points, Winston Churchill still felt that he needed six enormous volumes, eight years, and a team of contributing authors to tell his history of the easily demarcated Second World War. British wartime code-breaker turned Cambridge historian, F.H. "Harry" Hinsley, in some respects had a more modest task than Churchill—to write a history of World War II examining only the intelligence aspect. Like Churchill, however, Professor Hinsley found that he required several research and writing assistants, many years of work, and four volumes to tell his history of World War II secrets, not to mention the benefit of over a quarter century of time—much-needed hindsight and cooling off of intelligence sources and methods—to place intelligence and code-breaking operations into their wartime context. Even Hinsley's abridged version of *British Intelligence in the Second World War* (1993) spanned a dense 628 pages. Thus, broad histories are exceptionally challenging to write—much more so in their own time—and compounded by the fact that any "secret history" is bound to be a historiographical challenge for even the most veteran researchers.

In *Dark Territory: The Secret History of Cyber War,* Fred Kaplan has undertaken this daunting task and produced a well-researched book with a lively narrative. Kaplan, the national security columnist for Slate, is no novice to writing on opaque subjects, especially ones still in the headlines and shrouded in governmental secrecy. His

former works on a diverse range of topics from nuclear weapons to military operations demonstrate a malware-like ability to penetrate seemingly sealed systems which appears to offer nothing but a frustrating carapace to those that lack Kaplan's knack for investigative reporting. In some ways, Kaplan is the ideal author to attempt a secret history of cyber war: He is undaunted by technical complexity as evidenced not only by *Dark Territory,* but also his previous work on the nuclear arms race. Although technical enough to understand more than the basics of how cyber operations work, Kaplan keeps the narrative progressing and stays above the minutiae of coding and network integration. He never loses his intended generalist audience, and places cyber vulnerabilities into a larger political and international context. Kaplan reminds the reader that cyber operations are about technology and innovation, but equally, they're about people. It would be difficult to read *Dark Territory* and not find oneself rooting for Kaplan's protagonists—those cyber pioneers laboring in Pentagon basements, scientific labs, or at forgotten airbases, seeking to warn their Luddite leadership of danger ahead.

In the main, Kaplan adroitly navigates the problematic historiographical issues in intelligence history, relying overwhelmingly on off-the-record oral interviews, secondary sources and publicly available official policy announcements, directives, and strategies, such as those issued by the White House on certain national security topics. The closer Kaplan gets to present-day cyber operations, the more challenging reliable sourcing becomes due to classification issues (or some may say, "over-classification" issues). That Kaplan is forced to rely on interviews and anecdotes more than primary sources for his anecdotes and conclusions is yet another reminder of the challenges facing historians dealing with classified materials. The remedy, of course, is faster declassification review of relevant cyber-related materials, but that is a very long shot indeed. Edward Snowden likely felt this way, and thus took it upon himself to ensure that perhaps a million classified documents found their way into the public sphere through his devastating mass leaks, and historians are still grappling with the implications of mass leaks as primary source documents. Kaplan relies on remarkably little of Snowden's haul, perhaps because of their illegitimate provenance, but perhaps also because they lacked context, rendering them less reliable for authors.

The authoritative source material is a challenge for any secret history, and Kaplan's *Secret History* is no exception. Secret histories are often supplemented with oral interviews and secondary sources, but the best ones have primary sources at their core. Richard J. Aldrich's book, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* is the best example of primary source mastery which, instead of bogging it down, actually drives and enhances a narrative on technical topics such as signals intelligence and cyber history. This usually requires either a sizeable number of Freedom of Information Act requests (Kaplan cites a few), or tedious digging in the archives. Although written for a popular audience, Kaplan's work would have benefitted from further

exploration of salient declassified primary sources, such as the National Security Agency's significant "United Kingdom–United States of America Agreement", the formerly highly classified secret treaty which governed signals intelligence (SIGINT) relationships between the US and the UK.[1] The UK-USA agreement is arguably the mustard seed of today's cyber operations, given that it is this agreement from 1946 (solidifying earlier wartime US-UK signals intelligence cooperation) that laid the groundwork for Anglo-American and "Five Eyes" partnership in cyberspace up to the present day. Given the enduring, secret–and occasionally controversial–reciprocal agreements between the NSA and Great Britain's Government Communications Headquarters (GCHQ), any history of cyber war could be given additional context and reliability with such newly accessible declassified source material.

The fact that a journalist of Kaplan's stature has logged into the cyber realm is itself a notable and promising development in cyber studies. To wit, no longer are cyber specialists the only ones with the technical credentials to write an authoritative book on cyber operations; non-specialist journalists, even a Pulitzer Prize winner such as Kaplan (who holds a Ph.D. from MIT in Political Science), are now interested in contributing to cyber studies as another window into international relations, national security studies, and organizational history, to name but a few. And in that sense, literature on cyber issues has become more relevant and accessible to humanities and social science generalists than ever before. This is a promising development for cyber studies in as much as cyber issues have successfully transitioned from specialist literature to a fair game topic for an author like Kaplan.

Kaplan's *Dark Territory* is far from comprehensive, but then a comprehensive cyber history is likely impossible, especially considering classification issues, but also given the blurred lines between code-breaking, communications and signals intelligence, electronic warfare, and even electronic or cyber operations enabled or supported by other intelligence types, such as Human Intelligence. Further, the geopolitical impact of these operations would take many more volumes to assess. As an example, Kim Zetter's *Countdown to Zero Day,* a single case study about the Stuxnet virus, is substantially longer and more detailed than Kaplan's *Dark Territory.* Therefore, Kaplan's book must be read as a complement or supplement to other works in the burgeoning cyber history canon, such as Jason Healey's *A Fierce Domain: Conflict in Cyber Space,* 1986-2012. As a historical primer on cyber operations, Kaplan's book does a great service opening other doors of intellectual inquiry regarding the relevance of cyber operations to current events, identifying the main actors and turning points, and critically, putting them in their own historical context.

Dark Territory: The Secret History of Cyber War by Fred Kaplan

Paperback edition of *Dark Territory,* with a new Afterword, will be published in March 2017.

Author: Fred Kaplan
Publisher: Simon & Schuster, 2016
e-book: 353 pages
Language: English
ISBN: 978-1476763255

David V. Gioe is Assistant Professor of History at the United States Military Academy at West Point and History Fellow for the Army Cyber Institute. Dr. Gioe spent over a decade working in the U.S. intelligence community, both in the FBI National Security Division and in the CIA Counterterrorist Center (CTC). He retains his commission as a Naval Reserve Intelligence Officer. Dr. Goie earned his Ph.D. in Politics and International Studies at Corpus Christi College, University of Cambridge. He holds a BA in History and Social Science from Wheaton College, an MA from the Georgetown University School of Foreign Service, and is a graduate of the U.S. Naval War College Command and Staff program.

NOTES

1. The National Archives (UK), Newly Released GCHQ Files: The UKUSA Agreement, http://www.nationalarchives.gov.uk/ukusa/, accessed 8 November 2016. See also https://www.nsa.gov/news-features/declassified-documents/ukusa/.