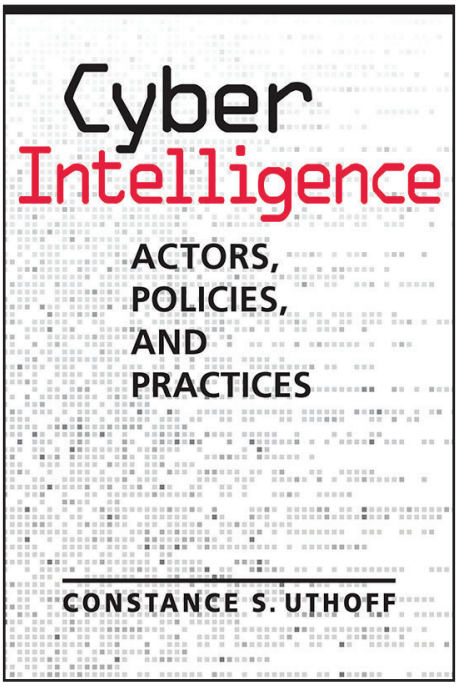
8-29-2023

Book Review: Cyber Intelligence: Actors, Policies, and Practices

Robert J. Bunker



Reviewed by Dr. Robert J. Bunker, director of research and analysis,
managing partner, C/O Futures LLC

Constance S. Uthoff, the author of this introductory book on cyber intelligence, serves as an associate program director of the Cybersecurity and Information Management Program at George Washington University. A cybersecurity consultant and practitioner, she holds a master's degree in intelligence studies from American Military University and has an affiliation with the Cyber Security Forum Initiative. Her applied rather than theoretical background suits the subject matter well and provides the work a straightforward and practical element. At the same time, it removes expectations for this major effort to break new ground concerning early warning and futures related to threat identification and emergent technologies and processes beyond what others have already identified.

The book's subtitle, *Actors, Policies, and Practices*, is a bit of a misnomer in that the work "examines the role of cyber intelligence in identifying, preventing, and countering current and emerging threats" (3). Hence, it goes beyond just the means—such as the cyber intelligence process, policy mandates, and agency structures behind cyber intelligence—and delves into the end states and outcomes stemming from our interactions and increasing conflict with a range of state and nonstate threats, actual cyber operations and sustained campaigns, and resultant successes and failures.

Cyber Intelligence is composed of 15 chapters, an acronym list, a well-developed bibliography, an index, and a short "about the book" synopsis. Although well-structured and edited, the work is almost solely text-based and devoid of imagery, with few figures or tables. The introductory first two chapters of the book provide context and the upfront matter. Chapter 1, "The Cyber Domain," offers key terms and concepts—such as "operationalizations"—and explains the book's structure and "connect-the-dots" approach. Chapter 2, "The Threat Landscape," explores US target sets, including the supply chain, the emerging Internet of Things, the economy, intellectual property, critical infrastructure, US government websites and systems, satellites, and the impact of cyberspace on warfighting domains.

The foundational chapters—3 through 9—focus on evolving processes, policies, and agency bureaucracies and are painful to read at times, given the dry foci. Chapter 3, "The Cyber Intelligence Cycle and Process," pertains to an overview of iterated intelligence activities (fig. 3.1, p. 43) and resources, such as *Cyberspace Operations,* Joint Publication 3-12. Chapter 4, "National Security Strategies and Policies," discusses various strategic documents (such as acts, strategies, directives, and such) used primarily after the Clinton administration. Chapter 5, "The Office of the Director of National Intelligence," details the various director terms from 2004–2021 (table 5.1, p. 117). Chapter 6, "The National Security Agency," spotlights NSA activities related to information operations, Trailblazer, Prism 2007, various documented cyber tools, and such. Chapter 7, "The Central Intelligence Agency," addresses the CIA's Cold War and post–Cold War technology use, policies, activities, structures (such as the Open Source and Information Operations Centers), and capabilities. Chapter 8, "The Federal Bureau of Investigation," provides insights into FBI activities and capabilities directed against online sexual predators and other cyber criminals (such as organized crime participants, terrorists, and state proxies). Chapter 9, "Intelligence Sharing," offers insights into ongoing mandated legislation and a proliferation of coordinating centers attempting to break down governmental institutional silos, and Uthoff recognizes much work needs to be done concerning public-private information-sharing activities.

Chapters 10 through 15 cover more dynamic and interesting topics. Chapter 10, "Counterintelligence Efforts," looks at Presidential Decision Directive 75, additional structures and strategies, and counterresponses and operations directed at US adversaries. Chapter 11, "Cyber Operations in International Conflicts," reviews activities from the Gulf War through fighting the Islamic State in Iraq and the Levant (1991–2019) and highlights Chinese, North Korean, and Russian cyber campaigns. Chapter 12, "Cyber Threats and Nonstate Actors," concerns "hacktivists," organized crime, the dark web, terrorist use of cyberspace, and insider threats. Chapter 13, "Emerging Cybersecurity Challenges," looks at SolarWinds and its four gaps in public-private collaboration, supply-chain vulnerabilities, overwhelming volume of data produced, workforce needs, and insider-threat issues. Chapter 14, "Three Case Studies of Cyber Espionage," details the Stuxnet attack on Iranian centrifuges, Chinese espionage and Mandiant Advanced Persistent Threat 1, and the Democratic National Committee breach and Russian intelligence activity. Chapter 15, "The Future of Cyber Intelligence," covers augmented intelligence, artificial intelligence and machine learning, 5G communications, and quantum computing.

This reviewer cannot fault the book's logical structure, approach, content, or even flow. Other than some tedious agency bureaucracy and policy discussions in the foundational chapters—which are to be expected given the subject matter—and a lack of figures or tables (which the reviewer recognizes allows for more informational understanding and retention), *Cyber Intelligence* delivers on what it advertises, from a technical viewpoint. At times, it does have a soulless, textbook feel, which is amplified by a lack of shout-outs to those who helped make the book a success.

In summation, this veteran practitioner's solid work covers a lot of ground at a reasonable price. As intended, it will serve as a useful introductory text on the subject matter. Selections from later chapters could be used for war college–level studies and student research. Although not theoretically inspiring, it should be considered a practical tool in our understanding of the cyber intelligence and conflict discipline. Kudos to the author and the publisher for producing a useful and readable cyber-related and national security-focused work.

Boulder, CO: Lynne Rienner Publishers, 2022 ▪ 441 pages ▪ $45.00

Keywords: cyber intelligence, cyber operations, Internet of Things, critical infrastructure, cyberspace, dark web