Association of Former Intelligence Officers
Representing U.S. Intelligence Community
Service, Education, Interest, and Support
ASSOCIATION OF FORMER INTELLIGENCE OFFICERS AFIO

Weekly Intelligence Notes
Exclusive Book Review
(January 2025)

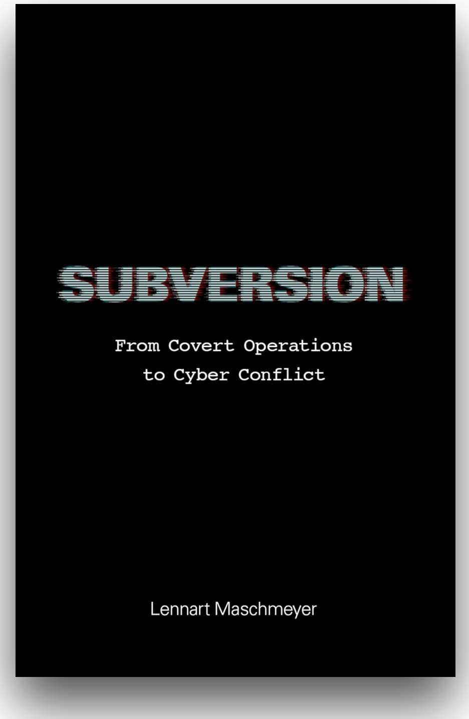
Subversion: From Covert Operations to Cyber Conflicts

by Lennart Maschmeyer
Oxford University Press
04 March 2024

Review by **Jennifer Ewbank***
Former Deputy Director of CIA
for Digital Innovation

What if one of the most feared weapons of modern conflict—cyberwarfare—is not as revolutionary as we think? In Subversion: From Covert Operations to Cyber Conflict, Dr. Lennart Maschmeyer challenges prevailing assumptions about the transformative potential of cyber operations, exploring subversion as a strategic tool. By connecting historical covert operations to contemporary cyber campaigns, Maschmeyer highlights their limitations and implications for global security.

At its core, Subversion examines the promises and pitfalls of subversive strategies, from Cold War-era covert action to modern cyberattacks. Maschmeyer introduces the "subversive trilemma," a framework that underscores the trade-offs between speed, intensity, and control in subversive operations. Through detailed case studies, he argues that while subversion is appealing as a low-cost, high-impact strategy, it often falls short in practice. Cyber operations, in particular, face even greater constraints than traditional methods, diminishing their strategic value.



SUBVERSION

From Covert Operations
to Cyber Conflict

Lennart Maschmeyer

Order Book Here

Maschmeyer's expertise as a senior researcher at ETH Zurich's Center for Security Studies and his academic credentials lend intellectual rigor to his analysis. The book is filled with theoretical insights and empirical evidence, making it a valuable resource for academics and policymakers seeking to understand the evolving dynamics of conflict in the digital age.

However, the book’s academic tone and dense theoretical focus may deter some readers. Lengthy introductions to each section often reiterate key points, slowing both pace and reader engagement. This approach caters to scholarly audiences and others seeking a more theoretical grounding in the material, but may leave intelligence practitioners seeking actionable insights somewhat underwhelmed.

One notable example of this academic-practitioner divide is Maschmeyer’s assessment of Russia’s cyber campaigns against Ukraine. He argues that their limited visibility during the ongoing war exposes the inherent weaknesses of cyber operations compared to traditional forms of subversion. While compelling, this conclusion gives insufficient weight to two significant challenges.

First, Maschmeyer describes cyber operations as relatively inexpensive tools of statecraft. In practice, however, they require substantial investments in talent, time, and resources. Developing sophisticated tools and exploiting vulnerabilities is neither cheap nor easy, particularly as global defensive measures improve. Second, he underestimates the strategic trade-offs in deploying cyber capabilities during wartime. Intelligence collection offers long-term strategic value, while destructive attacks may yield immediate impacts, compromise critical access points, and potentially trigger escalation. This tension between intelligence and operational objectives significantly complicates decisions about using cyber tools. To his credit, Maschmeyer does mention these trade-offs, but a deeper exploration of the issues could have enriched his analysis.

Despite these critiques, Subversion is a significant contribution to the field. Maschmeyer challenges conventional wisdom, offering new perspectives on the intersection of modern technology and age-old strategies of influence and coercion. For academics and policymakers, this work will undoubtedly shape discussions on subversion and cybersecurity for years to come.

While it may not be a light read for all audiences, Subversion delivers depth and ambition. Readers willing to engage with its academic approach will gain a deeper understanding of today’s pressing security challenges—and perhaps a more skeptical view of cyberwarfare’s revolutionary promise.

Jennifer Ewbank served as Deputy Director of CIA for Digital Innovation from 2019 - early 2024. In that role, she led transformation of one of the world's most sophisticated and secure digital technology ecosystems and leveraged its capabilities to ensure U.S. competitive advantage against its adversaries. Among other duties, she oversaw the CIA's offices delivering cyber intelligence, artificial intelligence, data strategy, information technology, global secure communications, cyber security, and open-source intelligence. She also served for a decade on the Editorial Board for the US Intelligence Community's professional journal, *Studies in Intelligence*.