BOOK REVIEW: CYBER POWER AND NATIONAL SECURITY EDITED BY FRANKLIN D. KRAMER, STUART H. STARR, & LARRY K. WENTZ, 2009, PP. 664 (1ST ED.).

Washing, D.C. National Defense University Press.

Francis Otiato*

The cyber realm is experiencing remarkable developments that give both extraordinary opportunities to and significant threats for users of cyberspace. The threats stem from the malicious individuals who use cyberspace and the numerous security vulnerabilities that trouble this field. Capitalize On suitable circumstance and overcoming challenges will need a well-balanced foundation of information on the cyber security. Cyber power and National Security brings together a team of specialists, including; Franklin D. Kramer; Struart H. Starr, and Larry Wentz both outstanding research scholars at the Center for Technology and National Security Policy,and outlines the core arguments and identifies the critical issues involved in developing the human capability to address cyber concerns, balancing civil rights with national safety concerns, and promoting the global cooperation required to address cyber threats.

With more than two dozen contributors, Cyber power and National Security wrap it totally. The opening three chapters form the comprehensive framework section that strives to provide a general outlook of the text by identifying and addressing significant policy concerns, building basic vocabularies, and formulating a preliminary theory of cyber power. Chapter 1 examines the key policy concerns, classifying them into structural and geopolitical. Chapter 2 establishes a standard vocabulary for the cyber domain, with explanations for essential ideas of cyberspace, cyber power, and cyber strategy. Chapter 3 introduces the primary theory of cyber power.

* **Texas Southern University**

The second section "Cyberspace" identifies and examines potential developments in cyberspace over the following fifteen years by evaluating cyber infrastructure and security problems. Chapter 4 examines at structural components that form cyberspace, whilst chapter 5 names vulnerabilities affecting the crucial national infrastructure of the United States, including power grids, communication systems, and cyberspace infrastructure. In chapter 6, the writers examine the trends in cyberspace: generation of broadband, the progress to Internet protocol, version 6 (IPv6), improve software complexity, the growth of online communities, and so on. Chapter 7 studies the information security concerns affecting the Internet world. Chapter 8 suggests various policy discussions that the writers believe are linked to the future of cyberspace, including safety, identity, and location-aware computing, whilst chapter 9 examines the biotech revolution and the shading of boundaries between humans and technology.

The third section analyzes the feasible impact of developments in cyberspace on the military and informational levers of power, "Military Use and Deterrence," consist of four chapters. Chapter 10 examines the environmental power theories, relates them to cyber power, and explains common components. Chapter 11 examines the topic of whether networking engineers do actually enhance operational effectiveness. Chapter 12 presents a summary of the cyberspace and cyber power initiatives offered by the military, and chapter 13 looks at the controversial issue of the deterrence of cyber crimes.

The fourth section discusses the degree at which developments in cyberspace help to enable important entities such as transnational criminals, terrorists, and nation-states. Chapter 14 explores the strategic impacts of cyberspace information on global security. Chapter 15 explores the difficulties linked with influence developments at the tactical level, while chapter 16 looks at the relevant issue of how information and communication technology and policies can affect security maintenance. This topic is further continued in chapter 17, which analyzes different policy and institutional activities.

Section 5, comprise of three chapters, which looks at the extent at which cyber power can empower nations, terrorists, and criminals. Chapter 18 examines the way crime has improved in cyberspace, particularly the use of cyberspace by organized criminals to advance their agenda. Chapter 19 attempts to scope the term "cyber terrorism," and considers the debated issue of

whether it exists or is merely a myth. Chapter 20 examines the application of cyberspace by China and Russia.

In the concluding section, chapter 21 studies the complicated and delicate issue of Internet governance and how the United States can realize "Internet influence" in the face of demand from other countries. Chapter 22 discusses legal matters associated with cyber counterinsurgency, especially two types of problems: legitimate recourse to force and use of violence in wartime. Chapter 23 presents a crucial evaluation of the United States federal attempts to protect important infrastructure. The last chapter pushes for the establishment of a Cyber Policy Council to give a structured answer to any of the vexing problems in the domain.

Contrasted to different publications on the subject, this work is incredibly comprehensive and logical in its coverage. Given its extensive coverage, it should be studied and considered by those who have more than a passing interest in cyber power and cyber policies but with a desire for a more erudite approach of the problem.