1. Record Nr. UNINA9911019820603321

Titolo	Cyberwar and information warfare / / edited by Daniel Ventre
Pubbl/distr/stampa	London, : ISTE Hoboken, N.J., : John Wiley, 2011
ISBN	9781118603482 1118603486 9781299187894 1299187897 9781118603390 1118603397 9781118603512 1118603516
Edizione	[1st edition]
Descrizione fisica	1 online resource (434 p.)
Collana	ISTE
Altri autori (Persone)	VentreDaniel
Disciplina	355.3/43
Soggetti	Information warfare Psychological warfare Computer crimes
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover; Cyberwar and Information Warfare; Title Page; Copyright Page; Table of Contents; Introduction; List of Acronyms; Chapter 1. Cyberwar and its Borders; 1.1. The seduction of cyberwar; 1.2. Desirable, vulnerable and frightening information; 1.3. Conflict and its dimensions; 1.4. The Helm and space; 1.5. Between knowledge and violence; 1.6. Space, distance and paths; 1.7. The permanency of war; 1.8. No war without borders; 1.9. The enemy and the sovereign; 1.10. Strengths and weaknesses; 1.11. Bibliography; Chapter 2. War of Meaning, Cyberwar and Democracies; 2.1. Introduction 2.2. Informational environment, a new operating space for strategy2. 2.1. War and information: stakes for the West; 2.2.2. Strategy in the information environment; 2.2.3. Winning the battle of legitimacies; 2.3. Influence strategy: defeating and limiting armed force physical

involvement; 2.3.1. Describing the aggressor; 2.3.2. Armed forces and the information environment; 2.3.3. The need for moral force; 2.4. Conclusion; 2.5. Bibliography; Chapter 3. Intelligence, the First Defense? Information Warfare and Strategic Surprise; 3.1. Information warfare, information and war
3.2. Intelligence and strategic surprise3.2.1. Strategic surprise; 3.2.2. Perception of surprise; 3.2.3. Perception of the possibility of surprise; 3.3. Strategic surprise and information warfare; 3.4. Concluding remarks: surprise in strategic studies; 3.5. Bibliography; Chapter 4. Cyberconflict: Stakes of Power; 4.1. Stakes of power; 4.1.1. Power relations; 4.1.2. Expression of sovereignty; 4.1.3. Cyberpower; 4.1.4. Measuring and locating power; 4.1.5. Limits of exercising power; 4.1.6. The Monroe doctrine; 4.1.7. Globalization; 4.1.8. Shock theories; 4.1.9. Naval and maritime power strategy
4.1.10. Air/space and cybernetic power: analogies4.1.11. Cyberconflict/cyber weapons, chemical/biological weapons: comparisons; 4.1.12. Cyberconflict/cyber weapons, Cold War, nuclear weapons: comparisons; 4.1.13. Cyberconflict and new wars; 4.2. The Stuxnet affair; 4.3. Bibliography; Chapter 5. Operational Aspects of a Cyberattack: Intelligence, Planning and Conduct; 5.1. Introduction; 5.2. Towards a broader concept of cyberwar; 5.2.1. War and cyberwar: common ground; 5.2.2. New orders in cyberwar; 5.2.3. Who are cyberwarriors?; 5.2.4. Is formalization possible?
5.3. Concept of critical infrastructure5.3.1. Generalized definition of the notion of critical infrastructure; 5.3.2. System interdependence; 5.4. Different phases of a cyberattack; 5.4.1. Intelligence phase; 5.4.2. Planning phase; 5.4.3. Conduct phase; 5.5. A few "elementary building blocks"; 5.5.1. General tactical framework; 5.5.2. Attacks on people; 5.5.3. Opinion manipulation and area control; 5.5.4. Military computer attack in a conventional operation; 5.6. Example scenario; 5.6.1. Tactical scenario; 5.6.2. The order of events; 5.6.3. Analysis; 5.7. Conclusion; 5.8. Bibliography
Chapter 6. Riots in Xinjiang and Chinese Information Warfare

Sommario/riassunto

Integrating empirical, conceptual, and theoretical approaches, this book presents the thinking of researchers and experts in the fields of cybersecurity, cyberdefense, and information warfare.The aim of this book is to analyze the processes of information warfare and cyberwarfare through the historical, operational and strategic perspectives of cyberattacks.Cyberwar and Information Warfare is of extreme use to experts in security studies and intelligence studies, defense universities, ministries of defense and security, and anyone studying political sciences, international relations, g