

1. Record Nr.	UNINA9910138856703321
Autore	Ventre Daniel
Titolo	Cyber conflict [[electronic resource]] : competing national perspectives // edited by Daniel Ventre
Pubbl/distr/stampa	London, : Iste Hoboken, N.J., : Wiley, 2012
ISBN	1-118-56266-6 1-118-56274-7 1-118-56296-8 1-299-18890-7
Edizione	[1st edition]
Descrizione fisica	1 online resource (345 p.)
Collana	ISTE
Altri autori (Persone)	VentreDaniel
Disciplina	363.325/6004678
Soggetti	Internet - Security measures Cyberspace - Security measures Computer networks - Security measures
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; Title Page; Copyright Page; Table of Contents; Introduction; Chapter 1. Canada's Cyber Security Policy: a Tortuous Path Toward a Cyber Security Strategy; 1.1. Introduction; 1.2. Canada in North America: sovereign but subordinate?; 1.3. Counter-terrorism for the improvement of national security; 1.4. The long path to a national CI protection strategy and nationalcyber security strategy; 1.5. The adoption of the current strategies for CI protection and cyber security; 1.6. Conclusion; 1.7. Bibliography; 1.7.1. Scientific and media articles; 1.7.2. Primary Data; 1.7.3. Websites Chapter 2. Cuba: Towards an Active Cyber-defense2.1. Cyberspace: statistics and history; 2.1.1. The marginalization of Cuba; 2.1.2. Cuban cyberspace as the target of attacks; 2.2. Theoretical and practical considerations on information warfareand cyber-warfare; 2.2.1. Development of capabilities; 2.3. Cyber-warfare theories and practices; 2.3.1. Fidel Castro's discourse; 2.3.2. The concept of active cyber- defense; 2.4. Regulations and ways around them; 2.4.1. The State's influence over cyberspace; 2.4.2. Getting around the restrictions

2.5. Capabilities of control, surveillance and interception
2.6. Enemies;
2.7. Conclusion; 2.8. Bibliography; Chapter 3. French Perspectives on Cyber-conflict; 3.1. Cyberspace; 3.2. Assessments, view on the world and awakening; 3.2.1. Attacks; 3.2.2. The feeling of insecurity, the threat; 3.2.3. Potential vulnerabilities of States; 3.2.4. Evolution of the international environment; 3.3. Reaction, position of France and choice: theories, political strategies and military doctrines; 3.3.1. Information: a powerful weapon for those controlling it; 3.3.2. Media information: beneficial if controlled
3.3.3. Economic information as power, if controlled
3.3.4. Information warfare; 3.3.5. Information warfare or information control; 3.3.6. The ANSSI; 3.3.7. Cyber-security and cyber-defense; 3.3.8. Army: Information operations, NEB (numerisation de l'espace de bataille/digitization of battlespace), info-development; 3.3.9. Cyber-war and other modalities of the cyber-conflict; 3.4. Conclusion; 3.5. Bibliography; Chapter 4. Digital Sparta: Information Operations and Cyber-warfare in Greece; 4.1. Geopolitical significance; 4.2. Strategic concerns and internal balancing
4.3. Formative experiences in information operations: the Ergenekon conspiracy
4.4. Formative experiences in information operations: intensifying cyber-attacks; 4.5. Formative experiences in information operations: the Ocalan affair; 4.6. Formative experiences in information operations: the Greek wiretapping case of 2004-2005; 4.7. Emerging civilian information operations strategies; 4.8. Emerging military information operations strategies; 4.9. The European Union dimension in Greek information operations; 4.10. Conclusion; 4.11. Bibliography
Chapter 5. Moving Toward an Italian Cyber Defense and Security Strategy

Sommario/riassunto

Today, cyber security, cyber defense, information warfare and cyber warfare issues are among the most relevant topics both at the national and international level. All the major states of the world are facing cyber threats and trying to understand how cyberspace could be used to increase power. Through an empirical, conceptual and theoretical approach, Cyber Conflict has been written by researchers and experts in the fields of cyber security, cyber defense and information warfare. It aims to analyze the processes of information warfare and cyber warfare through historical, operational
