

| | |
|-------------------------|---|
| 1. Record Nr. | UNINA9910219983203321 |
| Autore | Libicki Martin C |
| Titolo | Cyberdeterrence and cyberwar / / Martin C. Libicki |
| Pubbl/distr/stampa | Santa Monica, CA, : RAND, 2009 |
| ISBN | 1-282-39853-9 9786612398537 0-8330-4875-9 |
| Descrizione fisica | 1 online resource (239 p.) |
| Disciplina | 363.3250973 |
| Soggetti | Information warfare - United States Cyberterrorism - United States - Prevention Cyberspace - Security measures Computer networks - Security measures - United States Civil defense - United States |
| 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. |
| Nota di contenuto | Cover; Preface; Contents; Figures; Tables; Summary; Acknowledgements; Abbreviations; CHAPTER ONE - Introduction; CHAPTER TWO - A Conceptual Framework; CHAPTER THREE - Why Cyberdeterrence Is Different; CHAPTER FOUR - Why the Purpose of the Original Cyberattack Matters; CHAPTER FIVE - A Strategy of Response; CHAPTER SIX - Strategic Cyberwar; CHAPTER SEVEN - Operational Cyberwar; CHAPTER EIGHT - Cyberdefense; CHAPTER NINE - Tricky Terrain; APPENDIX A - What Constitutes an Act of War in Cyberspace?; APPENDIX B - The Calculus of Explicit Versus Implicit Deterrence APPENDIX C - The Dim Prospects for Cyber Arms ControlReferences |
| Sommario/riassunto | Cyberspace, where information--and hence serious value--is stored and manipulated, is a tempting target. An attacker could be a person, group, or state and may disrupt or corrupt the systems from which cyberspace is built. When states are involved, it is tempting to compare fights to warfare, but there are important differences. The author addresses these differences and ways the United States protect itself in the face of attack. |

