1. Record Nr. UNINA9910459909103321

| | |
|---|---|
| Titolo | Cyber blockades |
| Pubbl/distr/stampa | Washington, District of Columbia, : Georgetown University Press, 2014 |
| ISBN | 1-62616-113-5 |
| Descrizione fisica | 1 online resource (190 p.) |
| Classificazione | 355.424 |
| Altri autori (Persone) | RussellAlison Lawlor |
| Soggetti | Cyberterrorism<br>Cyberterrorism - Prevention<br>Cyberspace - Security measures<br>Computer security<br>Cyberkrig<br>Computer sikkerhed<br>Electronic books. |
| 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 | Contents -- List of tables and figures -- Acknowledgments -- List of abbreviations and acronyms -- Networks of power in the information society -- Theorizing about cyberspace -- Evolution of blockades in different domains -- Cyber attacks on estonia -- The Georgia-Russia war -- Comparing cyber blockades -- Conclusion -- Glossary -- Bibliography -- Index. |
| Sommario/riassunto | This is the first book to examine cyber blockades, which are large-scale attacks on infrastructure or systems that prevent a state from accessing cyberspace, thus preventing the transmission (ingress/egress) of data. The attack can take place through digital, physical, and/or electromagnetic means, and it can be conducted by another state or a sub-state group. The purpose of this book is to understand how cyber blockades can shut down or otherwise render cyberspace useless for an entire country, and Russell also seeks to understand the implications of cyber blockades for international relations. A cyber blockade can be either a legitimate or illegitimate tool depending on the circumstances. What is certain is that the state on the receiving end faces a serious threat to its political, military, economic, and social stability. The book |

| | | |
|---|---|---|
| | | includes two in-depth case studies of cyber blockades, Estonia in 2007 and Georgia in 2008, both of which suffered cyber attacks from Russia. Russell compares cyber blockades with those in other domains (sea, land, air, and space) and offers recommendations for policymakers and for further academic study. |

| | | |
|---|---|---|
| 2. | Record Nr. | UNINA9910829852403321 |
| | Autore | Jackson John (Cybersecurity professional) |
| | Titolo | Corporate cybersecurity : identifying risks and the bug bounty program / / John Jackson |
| | Pubbl/distr/stampa | Hoboken, New Jersey ; ; Chichester, England : , : John Wiley & Sons, Ltd., , [2022]<br>©2022 |
| | ISBN | 1-119-78253-8<br>1-119-78256-2<br>1-119-78254-6 |
| | Descrizione fisica | 1 online resource (273 pages) |
| | Disciplina | 658.478 |
| | Soggetti | Business enterprises - Computer networks - Security measures<br>Penetration testing (Computer security)<br>Cyberspace - Security measures |
| | Lingua di pubblicazione | Inglese |
| | Formato | Materiale a stampa |
| | Livello bibliografico | Monografia |
| | Note generali | Includes index. |
| | Sommario/riassunto | "Understanding the evolution of bug bounty programs first requires familiarity with the hacking landscape, or as many in the information security field know it, penetration testing. Security researchers haven't always been respected nor given the opportunity to shine. Throughout history, hacking has been a word that scares the public and creates waves of fear inside of a company when rumors of a 'hack' spread. The first bounty paid for breaking into something (in recorded history) was in 1851. Charles Alfred Hobbs was paid roughly the equivalent of $20,000 US Dollars to pick a physical lock. (https://www.itspmagazine. |

com/itsp-chronicles/history-and-interesting-facts-about-bug-bounties-an-appsec-usa-2017-panel-recap)."--