1.

Record Nr.	UNINA9910338231303321
Autore	Oakley Jacob G
Titolo	Waging cyber war : technical challenges and operational constraints / / Jacob G. Oakley
Pubbl/distr/stampa	Berkeley, California : , : Apress, , [2019] 2019
ISBN	1-5231-5043-2 1-4842-4950-X
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (xvii, 192 pages) : illustrations (some color)
Collana	Gale eBooks
Disciplina	355.4
Soggetti	Cyberspace operations (Military science) Cyberterrorism Computer networks - Security measures Cyberterrorism - Prevention
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Chapter 1: Cyber and Warfare -- Chapter 2: Legal Authority -- Chapter 3: Cyber Exploitation -- Chapter 4: Cyber-Attack -- Chapter 5: Cyber Collection -- Chapter 6: Enemy Attribution -- Chapter 7: Targeting -- Chapter 8: Access -- Chapter 9: Self-Attribution -- Chapter 10: Association -- Chapter 11: Resource Resilience -- Chapter 12: Control and Ownership -- Chapter 13: Challenges -- Chapter 14: Contemplation.
Sommario/riassunto	Understand the challenges of implementing a cyber warfare strategy and conducting cyber warfare. This book addresses the knowledge gaps and misconceptions of what it takes to wage cyber warfare from the technical standpoint of those with their hands on the keyboard. You will quickly appreciate the difficulty and complexity of executing warfare within the cyber domain. Included is a detailed illustration of cyber warfare against the backdrop of national and international policy, laws, and conventions relating to war. Waging Cyber War details technical resources and activities required by the cyber war fighter. Even non-technical readers will gain an understanding of how the obstacles encountered are not easily mitigated and the irreplaceable

nature of many cyber resources. You will walk away more informed on how war is conducted from a cyber perspective, and perhaps why it shouldn’t be waged. And you will come to know how cyber warfare has been covered unrealistically, technically misrepresented, and misunderstood by many. What You’ll Learn: Understand the concept of warfare and how cyber fits into the war-fighting domain Be aware of what constitutes and is involved in defining war and warfare as well as how cyber fits in that paradigm and vice versa Discover how the policies being put in place to plan and conduct cyber warfare reflect a lack of understanding regarding the technical means and resources necessary to perform such actions Know what it means to do cyber exploitation, attack, and intelligence gathering; when one is preferred over the other; and their specific values and impacts on each other Be familiar with the need for, and challenges of, enemy attribution Realize how to develop and scope a target in cyber warfare Grasp the concept of self-attribution: what it is, the need to avoid it, and its impact See what goes into establishing the access from which you will conduct cyber warfare against an identified target Appreciate how association affects cyber warfare Recognize the need for resource resilience, control, and ownership Walk through the misconceptions and an illustrative analogy of why cyber warfare doesn't always work as it is prescribed.