Waging cyber war

Type de contenu : Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : Waging cyber war : technical challenges and operational constraints / Jacob G. Oakley

Auteur(s) : Oakley, Jacob G.

Publication : [Berkeley (Calif.)] : Apress

Date de copyright : C 2019

Description matérielle : 1 vol. (XVII-192 p.) : ill. ; 26 cm

ISBN : 1-4842-4949-6
978-1-4842-4949-9

EAN : 9781484249499

Classification décimale Dewey : 364.168 2

Note(s) : "For professionals by professionals" (4e de couv.)
Index

Note sur le contenu : Cyber and warfare Legal authority Cyber exploitation Cyber-attack Cyber collection Enemy attribution Targeting Access Self-attribution Association Resource resilience Control and ownership Challenges Contemplation

Résumé ou extrait : La 4e de couv. indique : "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, what one is preferred over the other, and their specific values and impacts on each other ; Be familiar with the needs 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."

Sujet - Nom commun : Cyberterrorisme
Cyberdéfense
Cyberterrorisme -- Mesures de sûreté
Cyberdéfense