Cyber warfare

Type de contenu : Texte

Type de médiation : sans médiation

Titre(s) : Cyber warfare : a multidisciplinary analysis / edited by James A. Green

Autre(s) responsabilité(s) : Green, James A. (1981-....) (Éditeur scientifique)

Editeur, producteur : London : New York (N.Y.) : Routledge, cop. 2015

Description matérielle : 1 vol. (XIV-182 p.) : ill. ; 24 cm

Collection : Routledge studies in conflict, security and technology

ISBN : 978-1-13-879307-1
1-13-879307-8

EAN : 9781138793071 rel.

Appartient à la collection : Routledge studies in conflict, security and technology

Classification décimale Dewey : 364.168 2

Note sur les bibliographies et les index : Bibliogr. en fin de chapitres. Notes bibliogr. Index

Note sur le contenu : A short history of cyber warfare / Richard Stiennon Understanding cyber-attacks / Duncan Hodges and Sadie Creese The attribution of cyber warfare / Neil C. Rowe The strategic implications of cyber warfare / Danny Steed The regulation of cyber warfare under the jus ad bellum / James A. Green The regulation of cyber warfare under the jus in bello / Heather A. Harrison Dinniss The relevance of the just war tradition to cyber warfare / David Whetham and George R. Lucas, Jr

Résumé ou extrait : Présentation de l'éditeur : "This book is a multi-disciplinary analysis of cyber warfare, featuring contributions by leading experts from a mixture of academic and professional backgrounds. Cyber warfare, meaning inter-state cyber aggression, is an increasingly important emerging phenomenon in international relations, with state-orchestrated (or apparently state-orchestrated) computer network attacks occurring in Estonia (2007), Georgia (2008) and Iran (2010). This method of waging warfare - given its potential to, for example, make planes fall from the sky or cause nuclear power plants to melt down - has the capacity to be as devastating as any conventional means of conducting armed conflict. Every state in the world now has a cyber-defence programme and over 120 states also have a cyber-attack programme. While the amount of literature on cyber warfare is growing within disciplines, our understanding of the subject has been limited by a lack of cross-disciplinary approaches. In response, this book, drawn from the fields of computer science, military strategy, international law, political science and

military ethics, provides a critical overview of cyber warfare for those approaching the topic from whatever angle. Chapters consider the emergence of the phenomena of cyber warfare in international affairs; what cyber-attacks are from a technological standpoint; the extent to which cyber-attacks can be attributed to state actors; the strategic value and danger posed by cyber conflict; the legal regulation of cyber-attacks as part of an on-going armed conflict and the ethical implications of cyber warfare. This book will be of great interest to students of cyber war, cyber security, military ethics, international law, security studies and IR in general."

Sujet - Nom commun : Guerre de l'information (droit international)
Guerre juste