

## **Binary bullets**

Type de contenu : Texte  
Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : Binary bullets : the ethics of cyberwarfare / edited by Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser [Texte imprimé]

Autre(s) responsabilité(s) : Allhoff, Fritz (1947-....) (Éditeur scientifique)  
Henschke, Adam (Éditeur scientifique)  
Strawser, Bradley Jay (Éditeur scientifique)

Editeur, producteur : Oxford : New York (N.Y.) : Oxford university press, cop. 2016

Description matérielle : 1 vol. (XVIII-296 p.) ; 24 cm

ISBN : 9780190221089  
0190221089  
9780190221072  
0190221070

EAN : 9780190221072 rel.

Autre variante du titre : [Ethics of cyberwarfare.]

Classification décimale Dewey : 172.42 23

Note(s) : Textes en partie issus de colloques

Note sur la description bibliographique : Publisher description

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

Note sur le contenu : Foundational norms for cyberwarfare Emerging norms for cyberwarfare / George R. Lucas, Jr The emergence of international legal norms for cyber-conflict / Michael N. Schmitt and Liis Vihul Distinctive ethical issues of cyberwarfare / Randall R. Dipert Cyberwarfare and the just war tradition Cyber chevauchées : cyber war can happen / David Whetham Cyberwarfare as ideal war / Ryan Jenkins Post-cyber: dealing with the aftermath of cyber-attacks / Brian Orend Ethos of cyberwarfare Beyond Tallinn: the code of the cyber-warrior ? / Matthew Beard Immune from cyber-fire ? The psychological & physiological effects of cyberwarfare / Daphna Canetti, Michael L. Gross, & Israel

Waismel-Manor Beyond machines : humans in cyber operations, espionage, and conflict / David Danks and Joseph H. Danks Cyberwarfare, deception, and privacy Cyber perfidy, ruse, and deception / Heather M. Roff Cyber-attacks and "dirty hands" : cyberwar, cyber-crimes or covert political action ? / Seumas Miller Moral concerns with cyber espionage : automated key-word searches and data-mining / Michael Skerker

Résumé ou extrait : Philosophical and ethical discussions of warfare are often tied to emerging technologies and techniques. Today we are presented with what many believe is a radical shift in the nature of war-the realization of conflict in the cyber-realm, the so-called "fifth domain" of warfare. Does an aggressive act in the cyber-realm constitute an act of war? If so, what rules should govern such warfare? Are the standard theories of just war capable of analyzing and assessing this mode of conflict? These changing circumstances present us with a series of questions demanding serious attention. Is there such a thing as cyberwarfare? How do the existing rules of engagement and theories from the just war tradition apply to cyberwarfare? How should we assess a cyber-attack conducted by a state agency against private enterprise and vice versa? Furthermore, how should actors behave in the cyber-realm? Are there ethical norms that can be applied to the cyber-realm? Are the classic just war constraints of non-combatant immunity and proportionality possible in this realm? Especially given the idea that events that are constrained within the cyber-realm do not directly physically harm anyone, what do traditional ethics of war conventions say about this new space? These questions strike at the very center of contemporary intellectual discussion over the ethics of war. In twelve original essays, plus a foreword from John Arquilla and an introduction, Binary Bullets: The Ethics of Cyberwarfare, engages these questions head on with contributions from the top scholars working in this field today.

Sujet - Nom commun : Cyberspace operations (Military science) -- Moral and ethical aspects  
Cyberstratégie -- Aspect moral  
Cyberterrorisme -- Aspect moral  
Cyberspace  
Guerre de l'information (droit international)  
Éthique militaire

Classification de la Bibliothèque du Congrès : U163 .B5525 2016