Cyberwar

Type de contenu : Texte

Type de médiation : sans médiation

Titre(s) : Cyberwar : law and ethics for virtual conflicts / édité par Jens David Ohlin, Kevin Govern, Claire Finkelstein

Autre(s) responsabilité(s) : Ohlin, Jens David (Éditeur scientifique)
Govern, Kevin (Éditeur scientifique)
Finkelstein, Claire (19..-....) philosophe (Éditeur scientifique)

Editeur, producteur : Oxford : Oxford university press, 2015, cop. 2015

Description matérielle : 1 vol. (XXXII-274 p.) ; 25 cm

ISBN : 978-0-19-871749-2
978-0-19-871750-8

EAN : 9780198717508 br.

Classification décimale Dewey : 364.168 2

Note sur les bibliographies et les index : Notes bibliogr. Index

Résumé ou extrait : Présentation de l'éditeur : "Cyber weapons and cyber warfare have become one of the most dangerous innovations of recent years, and a significant threat to national security. Cyber weapons can imperil economic, political, and military systems by a single act, or by multifaceted orders of effect, with wide-ranging potential consequences. Unlike past forms of warfare circumscribed by centuries of just war tradition and Law of Armed Conflict prohibitions, cyber warfare occupies a particularly ambiguous status in the conventions of the laws of war. Furthermore, cyber attacks put immense pressure on conventional notions of sovereignty, and the moral and legal doctrines that were developed to regulate them. This book, written by an unrivalled set of experts, assists in proactively addressing the ethical and legal issues that surround cyber warfare by considering, first, whether the Laws of Armed Conflict apply to cyberspace just as they do to traditional warfare, and second, the ethical position of cyber warfare against the background of our generally recognized moral traditions in armed conflict. The book explores these moral and legal issues in three categories. First, it addresses foundational questions regarding cyber attacks. What are they and what does it mean to talk about a cyber war? The book presents alternative views concerning whether the laws of war should apply, or whether transnational criminal law or some other peacetime framework is more appropriate, or if there is a tipping point that enables the laws of war to be used. Secondly, it examines the key principles of jus in bello to determine how they might be applied to cyber-conflicts, in particular those of proportionality and necessity. It also investigates the distinction between civilian and combatant in this context, and studies the level of causation necessary to

elicit a response, looking at the notion of a 'proximate cause'. Finally, it analyses the specific operational realities implicated by particular regulatory regimes. This book is unmissable reading for anyone interested in the impact of cyber warfare on international law and the laws of war."

Sujet - Nom commun : Cyberguerre (droit international)
Cyberespace -- Droit
Cyberterrorisme