Cyber strategy

Type de contenu : Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : Cyber strategy : the evolving character of power and coercion / Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness

A pour autre édition sur un support différent : Cyber Strategy The Evolving Character of Power and Coercion Brandon Valeriano, Benjamin Jensen, Ryan C. Maness 2018 Oxford Oxford University Press 978-0-19-061812-4

Auteur(s) : Valeriano, Brandon

Autre(s) auteur(s) : Jensen, Benjamin M. (19..-....)
Maness, Ryan C.

Publication : New York : Oxford University Press

Date de copyright : C 2018

Description matérielle : 1 volume (XII-305 pages) : graphiques, tableaux, couverture avec illustrations en couleurs ; 25 cm

ISBN : 978-0-19-061809-4

EAN : 9780190618094 rel.

Classification décimale Dewey : 364.168 2

Note sur les bibliographies et les index : Bibliographie pages 257-290. Index

Résumé ou extrait : In 2011, the United States government declared a cyber attack as equal to an act of war, punishable with conventional military means. Cyber operations, cyber crime, and other forms of cyber activities directed by one state against another are now considered part of the normal relations range of combat and conflict, and the rising fear of cyber conflict has brought about a reorientation of military affairs. Despite the alarmist discussion surrounding the threat of cyber attack, the authors of this book (in a vein similar to Thomas Rid) argue that there is very little evidence that cyber war is, or is likely to become, a serious threat. What Valeriano and Maness provide in this manuscript is an empirically-grounded discussion of the reality of cyber conflict, based on an analysis of cyber incidents and disputes experienced by international states since 2001. They delineate patterns of cyber conflict to

develop a larger theory of cyber war that gets at the processes leading to cyber conflict. They find that, in addition to being a little-used tactic, cyber incidents thus far have been of a rather low-level intensity and with few to no long-term effects. Interestingly, they also find that many cyber incidents are motivated by regional conflict. They argue that restraint is the norm in cyberspace and suggest there is evidence this norm can influence how the tactic is used in the future. In conclusion, the authors lay out a set of policy recommendations for proper defense against cyber threats that is built on restraint and regionalism

Sujet - Nom commun : Cyberstratégie
Cyberterrorisme
Cyberdéfense