Cyber war versus cyber realities

Type de contenu : Texte

Type de médiation : sans médiation

Titre(s) : Cyber war versus cyber realities : cyber conflict in the international system / Brandon Valeriano, Ryan C. Maness

Auteur(s) : Valeriano, Brandon

Autre(s) auteur(s) : Maness, Ryan C.

Editeur, producteur : Oxford : New York (N.Y.) : Auckland [etc.] : Oxford university press, cop. 2015

Description matérielle : 1 vol. (XIV-266 p.) : ill., cartes, graph., tabl. ; 25 cm

ISBN : 978-0-19-020479-2
0-19-020479-6

EAN : 9780190204792 rel.

Classification décimale Dewey : 364.168 2

Note sur les bibliographies et les index : Bibliogr. p. [249]-257. Notes bibliogr. Index

Résumé ou extrait : La jaquette indique : "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. What is the reality of this threat? Is it actual or inflated, fear or fact-based? Taking a bold stand against the mainstream wisdom, Valeriano and Maness argue that there is very little evidence that cyber war is, or is likely to become, a serious threat. Their claim is empirically grounded, involving a careful analysis of cyber incidents and disputes experienced by international states since 2001, and an examination of the processes leading to cyber conflict. As the authors convincingly show, cyber incidents are a little-used tactic, with low-level intensity and few to no long-term effects. As well, cyber incidents are motivated by the same dynamics that prompt regional conflicts. Based on this evidence, Valeriano and Maness lay out a set of policy recommendations for proper defense against cyber threats that is built on restraint and regionalism."
Présentation de l'éditeur : "What Valeriano and Maness provide in this book 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 : Cyberterrorisme
Technologie et relations internationales
Relations internationales -- Ressources Internet