

Cyberterrorisme - menace, réalité et riposte - : Quel intérêt pour les forces armées ?

Titre(s) : Cyberterrorisme - menace, réalité et riposte - : Quel intérêt pour les forces armées ? / Alain KERBOULL

Auteur(s) : KERBOULL, Alain

Editeur, producteur : 2001 COLLEGE INTERARMEES DE DEFENSE

Autres classifications : TRAV

Note(s) : Groupe : C2

Numéro promotion : Promotion 2000-2001

Note sur la description bibliographique : I: 8è promo/ 07 Menaces non militaires

Note de thèses et écrits académiques : Géopolitique

Résumé ou extrait : Les ordinateurs participent aujourd'hui au fonctionnement de nombreuses infrastructures vitales. Dans ce contexte, de nombreuses failles existent et menacent la sécurité des Etats modernes. Certains Etats ont déjà ajouté aux menaces terroristes conventionnelles, le terrorisme informatique ou cyberterrorisme, en particulier les Etats-Unis. Des scénarios catastrophes sont établis et laissent à penser qu'une organisation terroriste pourrait utiliser l'informatique soit comme arme, soit comme cible, dans le but de poursuivre son combat, habituellement mené par des attentats à la bombe ou des enlèvements. Jusqu'à présent, aucune action d'envergure n'a été révélée et revendiquée par une organisation terroriste connue, mais la multiplicité des attaques informatiques attribuées à des groupes de pirates ne sont-elles pas les prémices de ce cyberterrorisme ? Face au cyberterrorisme, les pays les plus avancés technologiquement se préparent, cherchent à renforcer leur sécurité et envisagent déjà les ripostes à travers une lutte informatique offensive. Cette dernière pourrait fournir un nouveau type d'armes, intéressant les armées qui pourraient l'utiliser dans la gestion des conflits armés en phase préparatoire à une intervention.

Sujet(s) : INTERNET
TERRORISME

Adresse électronique et mode d'accès : <https://bibliotheques-numeriques.defense.gouv.fr/koha/documents/cdem/D2564.pdf>