# Defensive information warfare

Type de contenu : Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : Defensive information warfare / David S. Alberts

Auteur(s) : Alberts, David Stephen (1942-....)

Autre(s) auteur(s) : National defense university Washington, D.C.

Publication : Washington : National defense University, 1996

Description matérielle : 1 vol. (XIII-80 p.) : ill. ; 23 cm

Classification décimale Dewey : 355.343

Note(s) : La p. de titre porte en plus : "ACT, the Center for advanced concepts and technology, Directorate of advanced concepts, technologies, and information strategies, Institute for national strategic studies."
G.P.O. sales statement incorrect in publication

Note sur le contenu : Defensive information warfare Analogies and realities Current situation Digital war Formulating the problem Threat topology Threat characteristics Proposed IW-D strategy Managing the solution Framework for progress Allocation of responsibilities IW-D challenges IWS awareness and understanding IW deterrence Building a defense-in-depth Organizational action plan

Résumé ou extrait : The problem of defending against information warfare is real. Our citizens and the organizations that provide them with the vital services they need can find no sanctuary from these attacks. The low cost of mounting these attacks has enlarged the field of potential adversaries and complicated efforts to collect intelligence and array our defenses. The consequences of a well-planned and coordinated attack by a relatively sophisticated foe could be serious. Even the threat of such an attack or digital blackmail is a distinct possibility. How the public will respond to the threat of 1W infrastructure attacks or to actual attacks is unclear, but is a major determinant of future policy and actions. This situation is getting worse with the rapid proliferation of information technology and know-how. We are becoming increasingly dependent on automation in every aspect of our lives. As information technology becomes an essential part of the way organizations and individuals create products and provide services, the need for interconnectivity and interoperability increases. With this increased need for exchanges of information (and products), vulnerabilities increase. Finally, the increased reliance on commercial-off-the-shelf products or commercial services makes it more and more difficult for organizations and individuals to control their own security environment. Given this situation we need to focus on two goals. First, we need

to find a way to protect ourselves against catastrophic events. Second, we need to build a firm foundation upon which we can make steady progress by continually raising the cost of mounting an attack and mitigating the expected damage.

Sujet - Nom commun : Guerre de l'information
Défensive (science militaire)