Introduction to cyber-warfare

Type de contenu : Texte

Type de médiation : sans médiation

Titre(s) : Introduction to cyber-warfare : a multidisciplinary approach / Paulo Shakarian, Jana Shakarian, Andrew Ruef ; foreword by Sushil Jajodia

Auteur(s) : Shakarian, Paulo

Autre(s) auteur(s) : Shakarian, Jana
Ruef, Andrew

Editeur, producteur : Amsterdam : Boston (Mass.) : Paris [etc.] : Syngress, cop. 2013

Description matérielle : 1 vol. (XVII-318 p.) : ill. ; 24 cm

ISBN : 978-0-12-407814-7
0-12-407814-1

EAN : 9780124078147 br.

Classification décimale Dewey : 364.168 2

Note sur les bibliographies et les index : Bibliogr. en fin de chapitres. Notes bibliogr. Glossaire. Index

Résumé ou extrait : La 4e de couv. indique : "Cyber Warfare has become a global problem threatening governments, corporations and individuals. This new domain of warfare is not only inhabited by governments such as China, Russia, Iran, and the United States, but a variety of other actors including insurgent groups like Hezbollah and Hamas as well as hacking groups such as Anonymous, LulzSec, and others. According to a recent analysis the global market for Cyber Warfare consulting, product development and protective services will reach a value of $15.9 billion in 2012. This in-depth text on cyber warfare, written by experts on the front lines, explores the cutting edge world of cyber-warfare including the following: Provides a multi-disciplinary approach to Cyber Warfare analyzing the information technology, military, policy, social, and scientific issues that are in play, Presents detailed case studies of cyber-attack including inter-state cyber-conflict (Russia-Estonia), cyber-attack as an element of an information operations strategy (Israel-Hezbollah,) cyber-attack as a tool against dissidents within a state (Russia, Iran); cyber-attack conducted by large, powerful, non-state hacking organizations such as Anonymous and LulzSec, and attacks directed against infrastructure such including water treatment plants, the power-grid and a detailed account on the Stuxent worm, Explores acts of cyber-warfare against industry including those against Aramco, Google, and others as well as the state-of-the-art in intelligence-gathering malware platforms including Duqu, Flame, and Gauss as well as how social media such as Facebook and Linkedln are also leveraged for this purpose."

Sujet - Nom commun : Guerre de l'information -- Études de cas
Cyberterrorisme
Cyberespace -- Mesures de sûreté
Criminalité informatique
Protection de l'information (informatique)
Cyber-espionnage