Counterintelligence in a cyber world

Type de contenu : Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : Counterintelligence in a cyber world / Paul A. Watters

Auteur(s) : Watters, Paul A. (19..-....)

Publication : Cham : Springer

Date de copyright : C 2023

Description matérielle : 1 vol. (XIX-145 p.) ; 24 cm

ISBN : 978-3-031-35286-7

EAN : 9783031352867 rel.

Classification décimale Dewey : 364.168 2

Note sur les bibliographies et les index : Notes bibliogr. Index

Note sur le contenu : Chapter. 1. Counterintelligence Theory Chapter. 2. The Cyber Operational Environment Chapter. 3. Cyber Threats (and Opportunities) Chapter. 4. Psychology and Criminal Profiling Chapter. 5. Counterespionage Chapter. 6. Technical Surveillance Chapter. 7. Physical Surveillance Chapter. 8. Data Analysis Chapter. 9. Attack Attribution Chapter. 10. Practical Deception Chapter. 11. Legal Issues in Cyber Counterintelligence Chapter. 12. Ethical Issues in Cyber Counterintelligence

Résumé ou extrait : This book provides an outline of the major challenges and methodologies for applying classic counterintelligence theory into the cybersecurity domain. This book also covers operational security approaches to cyber, alongside detailed descriptions of contemporary cybersecurity threats, in the context of psychological and criminal profiling of cybercriminals. Following an analysis of the plethora of counterespionage techniques that can be mapped to the cyber realm, the mechanics of undertaking technical surveillance are reviewed. A range of approaches to web and forum surveillance are outlined as a virtual addition to traditional video and audio surveillance captured regarding targets. This includes a description of the advances in Artificial Intelligence, predictive analysis, support for the disciplines of digital forensics, behavioural analysis and Open Source Intelligence (OSINT). The rise of disinformation and misinformation and the veracity of widespread false flag claims are discussed at length, within the broader context of legal and ethical issues in cyber counterintelligence. This book is

designed for professionals working in the intelligence, law enforcement or cybersecurity domains to further explore and examine the contemporary intersection of these disciplines. Students studying cybersecurity, justice, law, intelligence, criminology or related fields may also find the book useful as a reference volume, while instructors could utilise the whole volume or individual chapters as a secondary textbook or required reading.

Sujet - Nom commun : Services de renseignements
Cyberterrorisme
Cybercriminalité