

## **Research handbook on cyberwarfare**

Type de contenu : Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : Research handbook on cyberwarfare / edited by Tim Stevens,...., Joe Devanny,...

Auteur(s) : Stevens, Tim (1973-....) politiste

Autre(s) auteur(s) : Devanny, Joe (19..-....)

Publication : Cheltenham Northampton (Mass.) : Edward Elgar publishing

Date de copyright : C 2024

Description matérielle : 1 vol. (XVII-410 p.) ; 25 cm

ISBN : 978-1-8039-2484-7  
1-80392-484-5

EAN : 9781803924847 rel.

Classification décimale Dewey : 364.168 2

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

Note sur le contenu : 1. Introduction to the research handbook on cyberwarfare / Tim Stevens and Joe Devanny Part I: Conceptualizing and investigating cyberwarfare 2. War by any other name: A short history of the idea of cyberwarfare in the United States / Sean Lawson 3. Conceptualizing cyberwarfare / Stéphane Taillat Cyberwarfare research methods / Miguel Albert Gomez, Grace B. Mueller, Ryan Shandler, Brandon Valeriano and Christopher Whyte 5. Reporting on cyberwarfare: A conversation / Alexander Martin, Joe Tidy, Kim Zetter, Joe Devanny and Tim Stevens Part II: Cyberwarfare actors and institutions 6. Military cybercapacity: Measures, drivers and effects / Nadiya Kostyuk and Evgenia Sidorova 7. Cyber intelligence: Method or target? / Aaron Brantly 8. The meaning of cyberwarfare in Brazil / Luiz Rogério Franco Goldoni, Karina Furtado Rodrigues, Breno Pauli Medeiros and Joe Devanny 9. Cyber proxies: Covert state-non-state interactions in cyberwarfare / Janine Schmoldt 10. Private authority and the political economy of private companies in cybersecurity crises and conflicts / Louise Marie Hurel 11. Civil society in cyberwarfare: Hack-and-leaks, attribution and mobilization / James Shires Part III: Cyberwarfare operations and strategy 12. Offensive cyber capabilities / J.D. Work 13. Do we need an effects-based approach for cyber operations? / Paul Withers 14. Deception in cyberwarfare / Simon Henderson 15. Cyber coercion as a tool of statecraft: How often, how effective? / Quentin E.

Hodgson 16. Understanding cyber escalation: Amplifiers and dampeners of conflict / Jason Healey and Virpratap Vikram Singh 17. Countering non-state actors in cyberspace / Jamie MacColl and Tim Stevens 18. Territory, sovereignty and boundaries in digital battlespace / Jordan Branch Part IV: Cyberwarfare governance 19. Cyberwarfare and international law / Russell Buchan and Nicholas Tsagourias 20. Cyber arms control and counter proliferation: The limits of the possible / Joe Devanny and Grant Christopher 21. Moral maze: Ethics for cyber weapon systems / Elke Schwarz 22. Cyberwarfare norms and the attribution imperative: Shaping responsible state behaviour in cyberspace / Gil Baram and Noya Peer 23. Postscript: Reflections and future directions for research and practice on cyber in competition, crisis and armed conflict / Emily O. Goldman

Résumé ou extrait : "This Research Handbook provides a rigorous analysis of cyberwarfare, a widely misunderstood field of contemporary conflict and geopolitical competition. Gathering insights from leading scholars and practitioners, it examines the actors involved in cyberwarfare, their objectives and strategies, and scrutinises the impact of cyberwarfare in a world dependent on connectivity. The Research Handbook on Cyberwarfare interrogates cyberwarfare as a form of military intelligence statecraft that seeks to exploit digital systems for operational and strategic advantage. Chapter authors address cyberwarfare in its conceptual, historical, operational and strategic dimensions, and explore the application of international law, norms, ethics and arms control to this area of conflict. They pose crucial questions about the utility of cyberwarfare and its effects on society and citizens, establishing foundations for future research on the topic as a fact of international life. Providing rich detail in an accessible and understandable manner, this Research Handbook is a vital resource for scholars and researchers of cyber conflict, international relations, and security studies. Its practical elements will also appeal to military and intelligence practitioners, as well as those interested in how cyberwarfare can be regulated to ameliorate its effects on society." (4e de couv.)

Sujet - Nom commun : Cyberguerre  
Cyberterrorisme