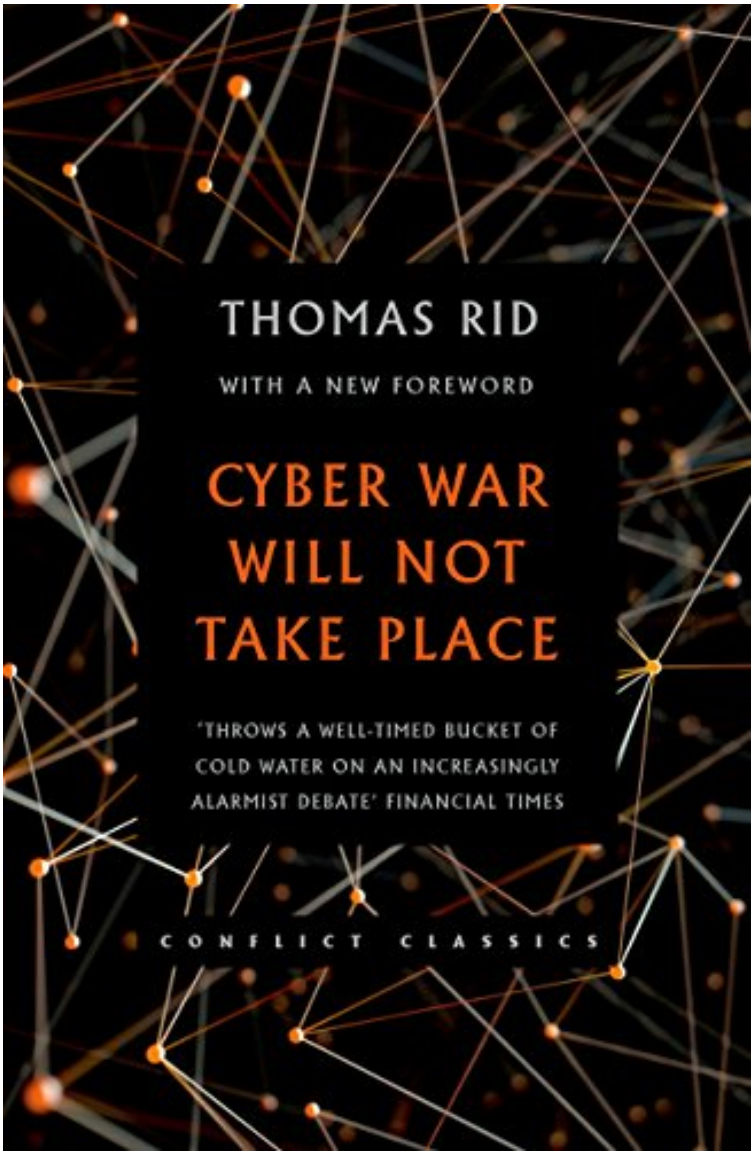
(Read free ebook) Cyber War Will Not Take Place

Cyber War Will Not Take Place

Von Thomas Rid
*ebooks | Download PDF | *ePub | DOC | audiobook*



DOWNLOAD READ ONLINE

Produktinformation -Verkaufsrang: #490877 in eBooksVerffentlicht am: 2013-09-01Erscheinungsdatum: 2013-09-01File Name: B00ET38G9G | File size: 71.Mb

Von Thomas Rid : Cyber War Will Not Take Place before purchasing it in order to gage whether or not it would be worth my time, and all praised Cyber War Will Not Take Place:

KundenrezensionenHilfreichste Kundenrezensionen0 von 0 Kunden fanden die folgende Rezension hilfreich. good analysis, but beyond the pointVon Dirk HeinenThis book is very very good in terms of determining a terminology of cyber, war, aggresion etc. and thus giving a solid framework within which to conduct the professional discussion about the topic.However, I think this is a bit beyond the point of such popular literature. In reality, this solid framework is

not used. Day to day speak is somewhat neglectful in terms of correct terminology and this fact is completely disregarded in this book.So all the conclusions that Rid takes are correct only within this framework, but not within the popular discussion, which does not base is arguments about cyber "war" on the categorization of a german military theoretician of the 19th century.In other words: Cyber war according to Rid's definition will most probably not take place. But this is not the cyber war of the popular discussion, which is already well under way.

Kurzbeschreibung"Cyber war is coming," announced a land-mark RAND report in 1993. In 2005, the U.S. Air Force boasted it would now fly, fight, and win in cyberspace, the "fifth domain" of warfare. This book takes stock, twenty years on: is cyber war really coming? Has war indeed entered the fifth domain?Cyber War Will Not Take Place cuts through the hype and takes a fresh look at cyber security. Thomas Rid argues that the focus on war and winning distracts from the real challenge of cyberspace: non-violent confrontation that may rival or even replace violence in surprising ways.The threat consists of three different vectors: espionage, sabotage, and subversion. The author traces the most significant hacks and attacks, exploring the full spectrum of case studies from the shadowy world of computer espionage and weaponised code. With a mix of technical detail and rigorous political analysis, the book explores some key questions: What are cyber weapons? How have they changed the meaning of violence? How likely and how dangerous is crowd-sourced subversive activity? Why has there never been a lethal cyber attack against a country's critical infrastructure? How serious is the threat of "pure" cyber espionage, of exfiltrating data without infiltrating humans first? And who is most vulnerable: which countries, industries, individuals?Pressestimmen'In a new book, provocatively titled "Cyber War Will Not Take Place," Rid argues that what we have seen so far in the cyber realm can't properly be classified as war at all. And, he and his allies suggest, in thinking of it that way, we're creating new international hazards and diverting attention from changes that might actually keep us safe. Rid represents one pole of an emerging debate, as the world's policy establishment grapples with how to think about virtual attacks. One side believes that to downplay them is dangerously naive - that this latest weapon of war has to be treated with the same seriousness as conventional arms, even nuclear weapons. An international effort is now underway to codify international rules of war as they apply to cyberattacks, placing them on a continuum with conventional warfare. Rid's side of this debate, which includes both experts on cybersecurity and those given the task of designing the new "weapons" for cyberspace, argues that although the threat is real, in overstating it we're helping create a new kind of global risk. Framing cyberattacks as acts of war has already fueled escalation, as countries like Iran and China invest in their own offensive cyberwarfare capabilities. And the military's enthusiastic embrace of this new theater of war, stoked by public fear, could have dangerous consequences.'--Boston Globe 'Thomas Rid is a German-born academic, now at King's College London. He is one of Britain's leading authorities on, and sceptics about, cyber-warfare. His provocatively titled book attacks the hype and mystique about sabotage, espionage, subversion and other mischief on the internet. He agrees that these present urgent security problems. But he dislikes talk of "warfare" and the militarisation of the debate about dangers in cyberspace. Computer code can do lots of things, but it is not a weapon of war. He criticises the American air force for using a "lobbying gimmick" with talk of "cyber" as a fifth domain of warfare, after land, sea, air and space.'--The Economist 'In Cyber War Will Not Take Place, Thomas Rid throws a well-timed bucket of cold water on an increasingly alarmist debate. Just as strategic bombing never fulfilled its promise, and even air power at its apogee - Kosovo in 1999, or Libya two years ago - only worked with old-fashioned boots on the ground, Rid argues that the promise of cyber war is equally illusory... What Rid does, with great skill, is to pivot the discussion away from cyber war and towards cyber weapons.'--Financial Times 'This book will be welcomed by all those who have struggled to get the measure of the "cyber war" threat. As Thomas Rid takes on the digital doomsters he also provides a comprehensive, authoritative and sophisticated analysis of the strategic quandaries created by new technologies.' Sir Lawrence Freedman, Professor of War Studies, King's College London and author of Strategy: A History 'Thomas Rid provides an unusually level-headed view of where we are in the cyber arms race. This book nips in the bud the loose talk of cyber war and illustrates what's really happening. Anyone involved in building defences against future attacks should read this book first.' Mikko Hypponen, virus analyst and Chief Research Officer, F-Secure 'We're in the early years of a cyber war arms race, one fuelled both by fear and ignorance. This book is a cogent counterpoint to both the doomsayers and profiteers, and should be required reading for anyone concerned about our national security policy in cyberspace.' Bruce Schneier, security guru and author of Liars and Outliers: Enabling the Trust Society Needs to Thrive 'With news of cyber war, terrorism and espionage seemingly everywhere, separating hype from reality is not always easy. Many agencies and companies stand to gain by inflating cyber security fears. Thomas Rid takes a razor to the evidence and carefully dissects the evolution of conflict and espionage in the cyber age. The result is a compelling and authoritative take on war and strategy in cyberspace, one that will surely be seminal in this area for years to come.' Ronald J. Deibert, Citizen Lab Director, Professor of Political Science, University of Toronto and author of Black Code: Inside the Battle for CyberspaceKurzbeschreibung"Cyber war is coming," announced a land-mark RAND report in 1993. In 2005, the U.S.

Air Force boasted it would now fly, fight, and win in cyberspace, the "fifth domain" of warfare. This book takes stock, twenty years on: is cyber war really coming? Has war indeed entered the fifth domain?Cyber War Will Not Take Place cuts through the hype and takes a fresh look at cyber security. Thomas Rid argues that the focus on war and winning distracts from the real challenge of cyberspace: non-violent confrontation that may rival or even replace violence in surprising ways.The threat consists of three different vectors: espionage, sabotage, and subversion. The author traces the most significant hacks and attacks, exploring the full spectrum of case studies from the shadowy world of computer espionage and weaponised code. With a mix of technical detail and rigorous political analysis, the book explores some key questions: What are cyber weapons? How have they changed the meaning of violence? How likely and how dangerous is crowd-sourced subversive activity? Why has there never been a lethal cyber attack against a country's critical infrastructure? How serious is the threat of "pure" cyber espionage, of exfiltrating data without infiltrating humans first? And who is most vulnerable: which countries, industries, individuals?