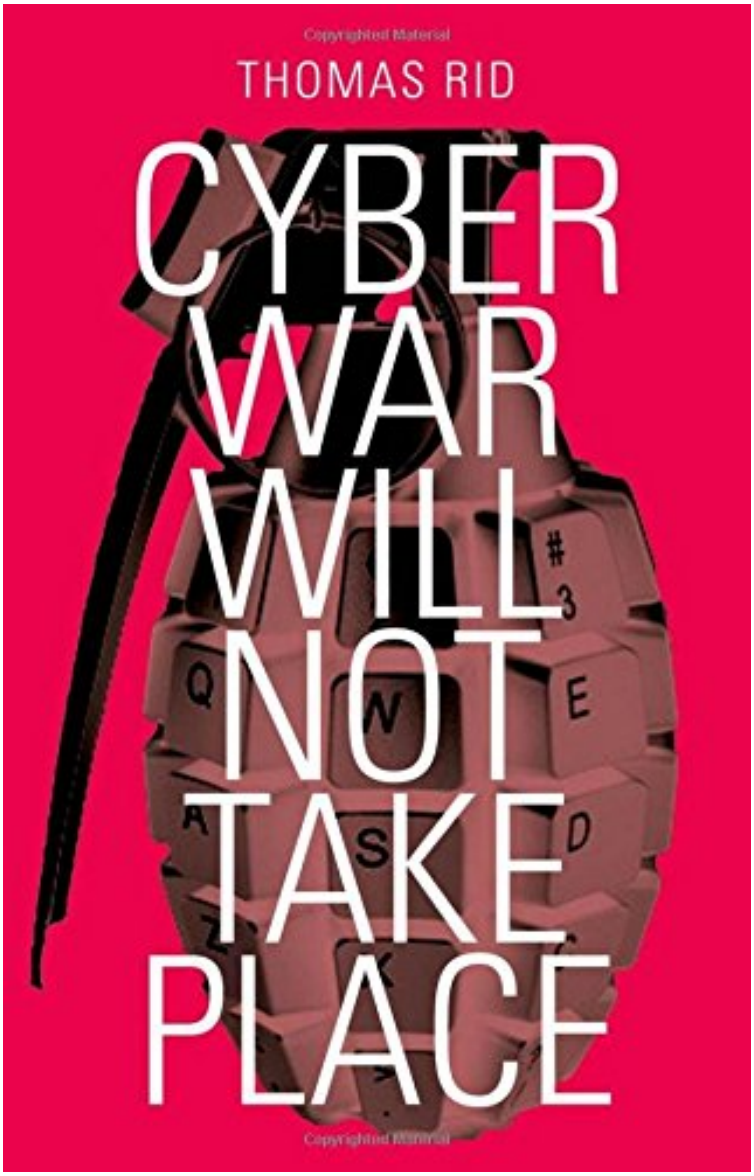
Cyber War Will Not Take Place

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



#711595 in Books Thomas Rid 2013-09-01Original language:EnglishPDF # 1 5.90 x 1.00 x 8.60l, 1.04 #File Name: 0199330638218 pagesCyber War Will Not Take Place | File size: 36.Mb

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:

13 of 16 people found the following review helpful. Not a book for the serious bookshelfBy LeRoy LuginbillThis book gives me hope. I will follow the example, do a lot of research on a topic with which I have no experience, publish it, and hopefully make enough money to pay off my wife’s Sears card. The interest rate is killing me!Dr. Rid’s

book provides many interesting stories about computer attacks and provides a slant on them that supports his thesis that a Cyber 9/11 will not happen. He also writes for pages and pages about topics unrelated to Cyber and though his command of the English language is impressive, more correctly, magniloquent, those pages still do not relate to Cyber.Why does everybody have to pick on the U.S. Air Force? It's because we mock what we don't understand. A lack of understanding and misguided assertions are common themes for this book. Dr. Rid cites over 200 sources in this 174 page thesis making me wonder if he had any original thought based on his experience, so I did a little research. Dr. Rid is a Professor who teaches wartime studies though I could not find evidence of him ever serving his country. I could also find no information on his Cyber or even IT background (yes, there is a difference), making it clear that he lacks the credentials to write on this topic.Dr. Rid asserts that Cyber is non-lethal, therefore Cyber war will not take place. His assertion can be discredited with three letters: UAV. Here we have a flying computer with weapons that is flown through the Internet. I would say that UAVs are most certainly lethal and they are flown from thousands of miles away through Cyberspace. Yes, the U.S. Air Force was right: Cyberspace is actually a fifth domain.I retired from the U.S. Air Force and also the U.S. Civil Service, working in Cybersecurity for the past eleven years, and IT for sixteen years before that, so I found this book to be doubly offensive. This book is certainly not one that should be taught in schools even if only for Dr. Rid's lack of credentials on the subject of Cyber. He did a lot of research and found books and articles freely available on the Internet, but only those that supported his assertion. In one case, he could not find a definition for "weapon" that supported his thesis so he made one up! How cheesy is that?Dr. Rid is highly educated in wartime studies but he avoided any tie that would discredit his assertion. In his book he talks about how the Israeli's used cyber to neutralize a Syrian radar site so they could safely fly past and bomb a nuclear reactor construction site. He states that this cyber intrusion helped the physical battle but because it was not lethal then it was not cyber warfare. The objective of war is not to kill people, it is to achieve a goal. In this case the goal was to bomb a construction site and the Israeli's did it without the loss of life – bonus, and goal achieved! Dr. Rid should know this tenet of warfare.My notes in the columns of the book say many times that Dr. Rid is stuck in the physical world and needs to open his mind. He cites people from centuries ago and falsely relates their thoughts to the cyber world. He even talked about Adam and Eve…really? To prepare for and win a Cyber war we need people who can think beyond the past and the physical and into the virtual, studying the "what if". Dr. Rid is not one of those people. I will put the pages of this book to good use and level my uneven dining table – they are both equally annoying.3 of 4 people found the following review helpful. Don't waste your time.By MikeA bunch of news clippings supporting a theory that doesn't mean anything. I strongly suggest you find a different book if you are interested in cyber.1 of 3 people found the following review helpful. Indispensable for Strategist and Security Practitioner AlikeBy The Desert FlyDr. Rid's book is a breath - nay, a desperate gasp - of fresh air in an overwhelming sea of blather from self-professed experts who all too often lack expertise in warfare and strategy, information security, or both.I hold a master's degree in Strategy, and have worked in information ("cyber") security for a number of years. I first heard Dr. Rid interviewed for King's College London's War Studies Podcast, had been eager to read his book, and finally invested the time to do. I was not disappointed. His arguments are many and varied, but from my perspective they boiled down to two main concepts. First: the definitions of war and warfare defined by Carl von Clausewitz are still the best framework for understanding either concept, and because "cyberwar"/information security lacks a number of key commonalities with either, the resulting martial language used to discuss the security of information technology is imprecise and counter-productive. Second: "cyber security" is more productively considered through the conceptual frameworks of sabotage, espionage, and subversion than through the conceptual frameworks of war and warfare in which it is commonly discussed.At no point does Dr. Rid argue against the dangers posed by vulnerabilities in international data networks - in fact, his case studies and observations make precisely the opposite case. However, he very adeptly disassembles the common martial rhetoric used to discuss the topic, and provides cogent arguments, observations, and case studies to wrap it all up. The book will be more accessible to those who are familiar with either military topics, information security, or both, but Dr. Rid does a reasonably good job of staying out of the realm of technobabble in order to make the book comprehensible to most readers.If there's one flaw to Dr. Rid's argument, it may be a lack of imagination: it's dangerous to presume what technology will or won't be able to do in ten, fifteen, twenty, fifty years. However, even this criticism is muted by his careful discussion of what is or isn't likely to happen, rather than what will absolutely happen; and his skepticism is still more credible than many of the alarmist predictions from others. Given the continuing debate over the attribution of the recent Sony hack, Dr. Rid's book (and particularly its penultimate chapter) seem prescient.For anyone interested in the future of warfare, or in information security, Dr. Rid's book is a must-read.

"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?

"Cyber War Will Not Take Place throws a well-timed bucket of cold water on an increasingly alarmist debate. EL What Rid does, with great skill, is to pivot the discussion away from cyber war and towards cyber weapons." -- Financial Times "Thomas Rid 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. Rid agrees that these present urgent security problems but he dislikes talk of 'warfare' and the militarization of the debate about dangers in cyberspace. Computer code can do lots of things, but it is not a weapon of war.' -- The Economist "This book provides a thorough and timely analysis of cyber conflict and makes a reasonable case to temper the dialogue around cyber war." -- International Affairs "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 the new technologies." -- Sir Lawrence Freedman, Professor of War Studies, King's College London and author of Strategy: A History 'Rid stands as a useful voice among the Cassandras and Chicken Littles who warn of the impending cyber apocalypse. He bridges the divide between law and technology, and serves as the standard bearer for those hoping to lead the cyber-war debate out of what he calls the 'realm of myth and fairytale' into rational, empirical discussion." -- Sydney Morning Herald "A stimulating read for anyone interested in the field of security studies, EL Cyber War Will Not Take Place has the tech language that academics from the field would expect it to have, but the author also manages to explain the background knowledge to lay readers in an understandable and often humorous fashion. Each of his points is accompanied by several real-life cybercrime examples, ranging from the infamous Stuxnet attack to operation Titan rain in 2003, when Chinese hackers attacked US military and governmental computer systems.' -- Journal for Intelligence, Propaganda and Security Studies About the AuthorThomas Rid is Reader in War Studies at King's College London. He is also a non-resident fellow at the Center for Transatlantic Relations in the School for Advanced International Studies, Johns Hopkins University, Washington, DC.